

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
CURSO DE SISTEMAS DE INFORMAÇÃO**

ASPECTOS DE SEGURANÇA NO PROTOCOLO INTERNET VERSÃO 6 – IPv6

ASPECTOS DE SEGURANÇA NO PROTOCOLO INTERNET VERSÃO 6 – IPv6

Monografia apresentada ao Curso de Graduação em
Sistemas de Informação da Faculdade Natalense
para o Desenvolvimento do Rio Grande do Norte
como curso regular parcial para obtenção do grau
de Bacharel em Sistemas de Informação

André Felipe Carvalho de Oliveira

Orientador:

Ricardo Eudes Martins Galvão, MSc

ANDRÉ FELIPE CARVALHO DE OLIVEIRA

FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
CURSO DE SISTEMAS DE INFORMAÇÃO

ASPECTOS DE SEGURANÇA NO PROTOCOLO INTERNET VERSÃO 6 – IPv6

André Felipe Carvalho De Oliveira

Monografia apresentada e aprovada em 15 de 12 de 2004
pela banca examinadora composta pelos seguintes membros:

Monografia apresentada ao Curso de Graduação em
Sistemas de Informação da Faculdade Natalense
para o Desenvolvimento do Rio Grande do Norte
como requisito parcial para obtenção do grau
de Bacharel em Sistemas de Informação.

Ricardo Kléber Martins Galvão, Msc.
Orientador:

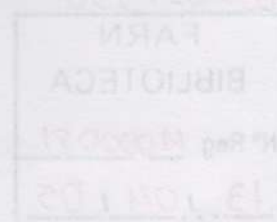
Orientador:

Ricardo Kléber Martins Galvão, Msc.

Alcides Pereira de Souza Neto, Msc.
Membro Examinador

Felipe Augusto Silva
Membro Examinador

**NATAL/RN
2004**



ANDRÉ FELIPE CARVALHO DE OLIVEIRA

ASPECTOS DE SEGURANÇA NO PROTOCOLO INTERNET VERSÃO 6 - IPv6

Monografia apresentada ao Curso de Graduação em
Sistemas de Informação da Faculdade Natalense
para o Desenvolvimento do Rio Grande do Norte
como requisito parcial para obtenção do grau
de Bacharel em Sistemas de Informação.

Orientador:

Ricardo Kleber Martins Galvão, Msc.

RB-21.350

FARN

BIBLIOTECA

Nº Reg. M000081

13.104.05

M
004.738.5

045a

2004

NATALIA
1005

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
CURSO DE SISTEMAS DE INFORMAÇÃO**

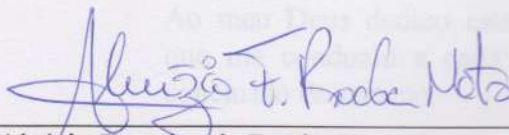
ASPECTOS DE SEGURANÇA NO PROTOCOLO INTERNET VERSÃO 6 – IPv6

André Felipe Carvalho De Oliveira

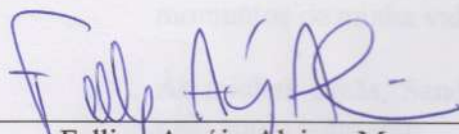
Monografia apresentada e aprovada em 15 de 12 de 2004,
pela banca examinadora composta pelos seguintes membros.



Ricardo Kleber Martins Galvão, Msc.
Orientador



Aluizio Ferreira da Rocha Neto, Msc.
Membro examinador



Felipe Araújo Aleixo, Msc.
Membro examinador

Natal, 15 de DEZEMBRO de 2004.

Cada etapa deste trabalho foi cumprida com o apoio de pessoas pelas quais tenho muito apreço e aqui, agradeço a todos com sinceridade.

Aos professores das disciplinas as quais ao longo do tempo foram minhas colaboradoras e cumpriram o seu papel no sentido de auxiliá-las no desenvolvimento necessário para que eu pudesse atingir o meu objetivo.

Aos professores orientadores, em especial, o Prof. Ricardo Kötter, pelo apoio e dedicação para a conclusão deste trabalho.

Aos meus colegas de curso, pelo companheirismo desenvolvido ao longo da jornada.

A Instituição, Faculdade Noroeste para o Desenvolvimento do Rio Grande do Norte, sob o comando de seus Diretores, Professores e Corpo Funcional, pelo suporte estrutural que nos ofereceram para a realização e conclusão deste instrumento de conhecimento.

E a todos que direta ou indiretamente, contribuíram na construção deste instrumento.

Ao meu Deus dedico este trabalho, pela sua força que me conduziu a cada passo que trilhei para a conclusão do mesmo.

Ao meu pai, José de Oliveira (*in memoriam*) e minha mãe, Nelita, pelo apoio recebido em todos os momentos de minha vida.

Às minhas irmãs, Sandra e Ana Angélica, também pelo apoio constante.

À minha noiva, Manaíra pela compreensão e o carinho nos momentos difíceis ao longo dessa jornada.

AGRADECIMENTOS

Cada etapa deste trabalho foi construído com o apoio de pessoas pelas quais tenho muito apreço e assim, agradeço a todos com sinceridade.

Aos professores das disciplinas os quais ao longo do curso foram sinceros colaboradores e cumpriram o seu papel no sentido de aprofundar os conhecimentos necessários para que eu pudesse atingir o meu objetivo.

Aos professores orientadores, em especial, o Prof. Ricardo Kléber, pelo apoio e dedicação para a conclusão deste trabalho.

Aos caros colegas de curso, pelo companheirismo demonstrado ao longo do percurso.

À Instituição, Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte, nas pessoas de seus Diretores, Professores e Corpo Funcional, pelo suporte estrutural que me ofereceram para a realização e conclusão deste instrumento de conhecimento.

E a todos que direta ou indiretamente, contribuíram na construção deste instrumento.

SUMÁRIO

LISTA DE FIGURAS	
LISTA DE SIGLAS	
RESUMO	
ABSTRACT	
1 INTRODUÇÃO	11
1.1 Objetivos	12
1.1.1 Objetivo Geral	12
1.1.2 Objetivos Específicos	12
1.2 Justificativa	13
2 REFERENCIAL TEÓRICO	14
2.1 Protocolos de Interligação em Redes.....	14
2.1.1 O Funcionamento do TCP/IP	15
2.2 O Protocolo IPv4	16
2.2.1 Motivação Para Mudar o IPv4	18
2.3 O Futuro IP (IPv6)	19
2.3.1 As Principais Vantagens do IPv6	20
2.3.2 Segurança no IPv6	21
2.4 Arquitetura Básica do IPSec	23
2.4.1 Protocolos AH e ESP	24
2.4.2 Gerenciamento de Chaves	25
2.4.3 Funcionamento do IPSec	25
2.4.4 Implementação do IPSec	26
2.4.5 Associação de Segurança	27
2.5 Considerações sobre a Mudança para o IPV6	30
2.6 Definição de Segurança em Redes de Computadores	31

2.6.1 Aspectos de Segurança de Redes	32
2.7 Considerações sobre Segurança de Rede de Informação	32
3 METODOLOGIA	34
3.1 Tipo de Pesquisa	34
3.2 Técnicas e Procedimentos da Pesquisa	34
3.2.1 Coleta dos Dados	34
3.2.2 Interpretação dos Dados	35
4 ANÁLISE DOS RESULTADOS	36
4.1 Quanto as Desvantagens do Protocolo IPv4 em Termos de Segurança das Informações	36
4.2 Quanto as Vantagens do Protocolo IPv6 em Termos de Segurança das Informações	37
4.3 Os Protocolos IPv4 e IPv6 na Segurança das Informações	39
4.4 Considerações sobre as Vantagens e Desvantagens da Migração para a Versão IPv6	40
5 CONCLUSÃO	41
BIBLIOGRAFIA	42

LISTA DE FIGURAS

FIGURA 1 – Arquitetura do IPsec	24
FIGURA 2 – Túneis IPsec entre Sistemas.....	26
FIGURA 3 – Cabeçalho do Protocolo AH (<i>Authentication Header</i>)	27
FIGURA 4 – Cabeçalho do Protocolo ESP (<i>Encapsulation Security Payload</i>)	28
FIGURA 5 – Protocolo AH e ESP	29
FIGURA 6 – Os Protocolos IPv4 e IPv6 na Segurança das Informações	39

ESP – *Encapsulated Security Payload (Segurança do Encapsulamento)*

ICV – *Integrity Check Value*

IEFP – *Internet Engineering Task Force (Força Tarefa de Engenharia da Internet)*

IESG – *Internet Engineering Steering Group*

IPsec – *Internet Protocol Security (Protocolo de Segurança da Internet)*

IPv4 – *Internet Protocol versão 4*

IPv6 – *Internet Protocol versão 6*

NAT – *Network Address Translation*

P2P – *Peer to Peer*

QoS – *Quality of Service (Qualidade de Serviço)*

RSVP – *Resource Reservation Protocol*

SPI – *Security Parameter Index*

SPD – *Security Policy Database*

TCP/IP – *Transmission Control Protocol (Controle de Transmissão de Protocolo)*

VPN – *Virtual Private Network (Rede Virtual Privada)*

LISTA DE SIGLAS

AH	<i>Authentication Header (Autenticação de Cabeçalho)</i>
ARPA	<i>Advanced Research Projects Agency (Agência de Projetos de Pesquisa Avançada)</i>
AS	<i>Security Association (Associação de Segurança)</i>
BITS	<i>Bump-in-the-stack</i>
BITW	<i>Bump-in-the-wire</i>
ESP	<i>Encrypted Security Payload (Segurança do Encapsulamento)</i>
ICV	<i>Integrity Check Value</i>
IETF	<i>Internet Engineering Task Force (Força Tarefa de Engenharia da Internet)</i>
IESG	<i>Internet Engineering Steering Group</i>
IPSec	<i>Internet Protocol Security (Protocolo de Segurança da Internet)</i>
Ipv4	<i>Internet Protocol versão 4</i>
IPv6	<i>Internet Protocol versão 6</i>
NAT	<i>Network Address Translation</i>
P2P	<i>Peer to Peer</i>
Qos	<i>Quality of Service (Qualidade de Serviço)</i>
RSVP	<i>Resource Reservation Protocol</i>
SPI	<i>Security Parameter Index</i>
SPD	<i>Security Policy Database</i>
TCP/IP	<i>Transmission Control Protocol (Controle de Transmissão de Protocolo)</i>
VPN	<i>Virtual Private Network (Rede Virtual Privada)</i>

RESUMO

Este estudo está inserido na área de sistemas de informação e contempla a “análise dos mecanismos e impactos na segurança das informações com a migração para o Protocolo IPv6”. Isto posto, a título de esclarecimento, o IPv6, é a nova versão do Internet Protocol, projetado para ser o sucessor do IPv4. O IPv4, versão atualmente utilizada, não vem correspondendo por uma série de fatores à questão da segurança no tráfego das informações na rede, sendo uma das motivações à migração para o IPv6. Assim, para o delineamento do estudo realizou-se um levantamento bibliográfico através de referências normatizadas, artigos, meio eletrônico (Internet) e estudos acadêmicos já realizados sobre a temática, os quais se caracterizaram como conteúdo cognitivo que se julgou necessário para o suporte teórico da pesquisa. Num segundo momento, o estudo interpreta e analisa o conteúdo de dados coletados de uma forma discussiva e progressiva à medida da ordem dos guias operacionais da pesquisa, apresentando as desvantagens do IPv4 em termos de segurança das informações, expondo as vantagens do Protocolo IPv6 no que se refere à segurança das informações, de forma que, analisa comparativamente os Protocolos sob os aspectos de segurança, para finalmente, tecer considerações sobre as vantagens e desvantagens da migração, visto que, constatou-se como resultado da pesquisa, que a migração e implementação do IPv6 é uma tendência, à medida que o IPv6 oferece melhores condições para a implementação de uma infra-estrutura de segurança em redes de computadores contemplando aspectos de segurança requeridos na rede, quais sejam: confidencialidade, integridade e privacidade das informações trafegadas.

Palavras-chave: Segurança de redes – IPv6 – IPv4

ABSTRACT

This study is inserted in the area of information systems and it contemplates the "analysis of the mechanisms and impacts in the security of information with the migration to the Protocol IPv6". The IPv6 is a new version of the Internet Protocol, projected to be the successor of IPv4. The IPv4, version now used, has not presented positive results related to the security of information traffic due to a number of factors, which motivates the migration to the IPv6. To carry out this study, bibliographical research, electronic (Internet) and academic studies already accomplished on the thematic were used. In a second moment, the study interprets and analyzes the content of collected data in a progressive form, presenting the disadvantages of IPv4 in terms of information security, exposing the IPv6 Protocol advantages referring to the security of the information, so that, it analyzes the Protocols comparatively when it comes to safety's aspects, to finally, take into consideration the advantages and disadvantages of the migration, since it was verified as a result of the research, that the migration and implementation of IPv6 is a tendency, as IPv6 offers better conditions for the implementation of an infrastructure of security in nets of computers contemplating aspects of security requested in the net, which are: confidentiality, integrity and privacy of the information traffic.

Key words: Internet Protocol – IPv6 – Security Aspects

1 INTRODUÇÃO

O presente trabalho abordou o estudo e a análise dos mecanismos relacionados à segurança de redes promovida pelo Protocolo Internet versão 6 (Ipv6), modelo proposto para substituir a versão 4 do protocolo (Ipv4), atualmente utilizado na Internet e nas Intranets.

No início da década de 80 com surgimento da rede mundial "Internet" foi desenvolvido para tal, a primeira versão do protocolo IP (*Internet Protocol*), que se caracterizou como Protocolo Internet versão 4 (Ipv4), e se configura como um conjunto de protocolos que estabelecem a comunicação entre redes. Nesse sentido, essa especificação foi publicada com o objetivo de colocar computadores em rede sendo o padrão atualmente utilizado.

Em princípio, a versão 4 (Ipv4) foi proposta e implementada para colocar computadores em rede tendo como base as comunidades acadêmicas e aplicações simples de pesquisa e troca rápida de informações entre usuários das redes interligadas, e, nesse sentido, pouco se pensou na questão da segurança dos dados, condição justificada pela confiança entre usuários, baixo número de máquinas interligadas e pouca criticidade dos dados transmitidos.

Entretanto, embora não tenha sido projetado para dar suporte a uma rede de escala universal o IP versão 4 conseguiu se ajustar as mudanças decorrentes do crescimento do número de máquinas conectadas à rede, como também, do potencial de processamento das máquinas.

Contudo, uma década depois, em 1991, membros do IETF - *Internet Engineering Task Force* (*Força Tarefa de Engenharia da Internet*) chegaram à conclusão de que esse crescimento exponencial da rede levaria certamente ao esgotamento dos endereços IP até o final do ano de 1994.

Nesse sentido, o iminente esgotamento de endereços Ipv4 válidos para utilização na Internet, além das limitações do próprio protocolo entre elas a questão da segurança no tráfego das informações, aceleraram os esforços de proposição de um novo padrão mais adequado ao quadro atual.

Assim sendo, em 1993, o IESG (*Internet Engineering Steering Group*) criou um grupo de trabalho para uma nova versão do protocolo IP e, nesse sentido, várias equipes com propostas diferentes começaram a pesquisar em paralelo e numa combinação de aspectos positivos do que foi desenvolvido pelas equipes, gerou-se então, a recomendação para a versão 6 do IP em novembro de 1994 que se configura como a nova geração do protocolo IP.

Dessa forma, surgiu o Ipv6 como um conjunto de especificações e padronizações proposto como solução no atendimento às necessidades surgidas devido ao crescimento dos pontos de acesso à Internet, além do avanço de novas tecnologias baseadas no protocolo IP.

Além do iminente esgotamento de endereços IPv4 e o avanço de novas tecnologias baseadas no protocolo IP, um dos aspectos que fortemente influenciam a evolução IPv6 é a questão da segurança no tráfego das informações que neste contexto, se constitui como objeto de estudo deste trabalho de pesquisa, mediante que, com o crescimento da rede, muitas são as vulnerabilidades existentes no que concerne a integridade e confidencialidade das informações.

É evidente que a versão IPv4 apresenta falhas em relação a capacidade de endereço, como também, em relação à segurança no tráfego das informações em função da mesma não ter sido desenvolvida para dar suporte a uma rede de escala universal.

Desta forma, surge a necessidade de utilização de uma nova versão do Protocolo IP, e assim, quais as vantagens promovidas pela nova versão em termos de segurança das informações? Que mecanismos garantem a questão da segurança das informações na rede? Quais seriam os impactos com a migração para essa nova versão?

Assim sendo, este estudo analisa os mecanismos e impactos na segurança das informações com a migração para o Protocolo IPv6.

1.1 Objetivos

1.1.1 Objetivo Geral

Analisar os mecanismos e impactos de utilização na segurança das informações com a migração para o Protocolo IPv6.

1.1.2 Objetivos Específicos

- Apresentar em termos de segurança as desvantagens do Protocolo IPv4;
- Expor as vantagens do Protocolo IPv6 em termos de segurança das informações;
- Analisar comparativamente os Protocolos IPv4 e IPv6 na segurança das informações;
- Tecer considerações sobre as vantagens e desvantagens da migração para a versão IPv6;
- Contribuir com a pesquisa científica na área de segurança da informação.

1.2 Justificativa

É evidente que nos dias atuais a Internet é uma ferramenta imprescindível para o ambiente científico, acadêmico, corporativo e popular, de forma que, a sua utilização é vasta tanto para fins comerciais, financeiros e pessoais e a rede enfrenta inúmeros problemas de segurança devido a ausência de um mecanismo que garanta a segurança no tráfego das informações. Neste sentido, a preocupação com segurança em redes torna-se cada vez maior demandando soluções que concorram para a transmissão das informações de forma autêntica, íntegra e segura.

Desta forma, o estudo permite uma análise do que se caracterizou como o novo padrão do protocolo internet versão seis (IPv6), enfatizando a questão da segurança em rede no tráfego das informações e acredita-se que, esse trabalho contribuirá de forma relevante para o meio acadêmico, à medida que reúne informações técnicas necessárias para um conhecimento mais complexo dos aspectos e mecanismos relativos à segurança das informações em rede e suas aplicações, haja visto, a realidade crescente, ou seja, o aumento da utilização dos sistemas onde as bases de dados estão distribuídas que demandam a implementação de mecanismos que possibilitem o processamento e transmissão de dados seguros.

2 REFERENCIAL TEÓRICO

Sendo o objetivo geral deste estudo analisar os mecanismos e impactos de utilização na segurança das informações com a migração para o Protocolo IPv6, buscou-se para tal, inteirar-se de estudos já realizados sobre a temática, perfazendo assim, um levantamento bibliográfico que, neste capítulo, se caracteriza como conteúdo cognitivo que se tomou por referência para a análise do objeto de estudo.

Nesse sentido, apresenta-se na sequência a fundamentação teórica que se julgou necessária para o desenvolvimento da temática de estudo.

2.1 Protocolos de Interligação em Redes

De uma forma geral, pode-se dizer que em computação, protocolos é um conjunto de normas e padrões que definem como computadores se comunicam entre si. Em outras palavras, protocolos significa “línguas computacionais” que definem como os computadores devem falar, de forma que, ao se comunicarem, troquem dados dentro de uma padronização conhecida por ambos.

Parafraseando com Comer (1998), a tecnologia de interligação de redes inclui um conjunto de padrões que especificam os detalhes do sistema pelo qual os computadores se comunicam, como também, um conjunto de convenções para interconexão em redes e roteamento. Oficialmente, o TCP/IP (*Transmission Control Protocol*), constitui a tecnologia de base, através de uma Pilha de Protocolos, para uma interligação em redes global que conecta domicílios, campus universitários, organismos de governo, empresas privadas, etc.

Em outras palavras, o autor afirma que protocolos como TCP e IP fornecem as regras para a comunicação, ou seja, neles estão contidos os detalhes de formatos de mensagens, de modo que, descrevem o que um computador faz ao receber uma mensagem e especificam como um computador trata os erros ou outras condições anormais. Esses protocolos permitem a comunicação através do computador, independentemente do hardware da rede de qualquer fornecedor em particular.

Os protocolos estão para a comunicação assim como os algoritmos estão para a computação. Se um algoritmo permite que uma pessoa especifique ou compreenda a computação sem conhecer os detalhes de um conjunto de instruções de uma CPU em especial, da mesma

forma, um protocolo de comunicação permite que alguém especifique ou entenda uma comunicação de dados sem depender de conhecimentos minuciosos de hardware da rede de um fornecedor específico.

2.1.1 O Funcionamento do TCP/IP

O TCP/IP, é definido como um grupo de protocolos que trabalham conjuntamente, com o objetivo de estabelecer a comunicação e a transferência de dados entre dois ou mais computadores ligados em rede. Essa definição encontra-se inserida em material de estudo sobre IPv6 disponível em http://www.w2k.com.br/images/SID/IPV6_ATM/ipv6atm.htm.

O TCP (*Transmission Control Protocol*), controla a transmissão dos dados, cuidando para que os dados enviados por um computador cheguem integralmente ao destino correto. Esse controle se dá através de uma biblioteca de rotinas instaladas nos computadores origem e destino (ou seja, em todos os computadores que utilizem o protocolo TCP/IP para se comunicar). O TCP é capaz de verificar, se os datagramas (mensagens/pacotes) chegam ao destino correto ou se não houve perda de dados durante a transmissão, retransmitindo o datagrama se necessário. Faz também o processo inverso ao juntar os datagramas no computador (host) destino para a reconstituição dos dados originais.

O IP é o protocolo responsável por definir o caminho que um pacote de dados deverá percorrer do computador (host) de origem ao computador (host) de destino, passando por várias redes. Ao contrário do TCP, o protocolo IP é chamado de Protocolo não-orientado a conexão, o que significa que não há nenhuma verificação de erro na transferência, ele apenas roteia os pacotes pela rede. Dessa forma, o TCP cuida da segurança do envio e recebimento dos datagramas, ao passo que, o IP é responsável pela transmissão propriamente dita, fazendo o serviço de roteamento, ou seja, conduzindo os dados para os endereços corretos.

Os protocolos TCP/IP, promovem a condição para duas importantes definições de serviços, sendo que uma delas define a unidade básica de transferência de dados chamada *datagrama IP* e a outra define a função de *roteamento* (caminho) o qual os *pacotes* (informações) são endereçados, de forma que, preocupa-se com os caminhos que as informações terão que seguir para atingirem o seu destino. Na verdade os dois protocolos se completam: enquanto o IP identifica os endereços e cuida para que os dados sejam enviados pelo meio físico, o TCP verifica se estes dados enviados foram transmitidos corretamente. Assim sendo, o fluxo de dados

é realizado como se existisse um duto, onde uma vez feito a conexão inicial, os dados são colocados neste, garantindo assim uma entrega dos dados.

2.2 O Protocolo IPv4

De acordo com Comer (1998), a Internet global teve seu início mais ou menos em 1980, quando a ARPA (*Advanced Research Projects Agency – Agência de Projetos de Pesquisa Avançada*), órgão do governo norte-americano, passou a adotar os protocolos TCP/IP nas máquinas ligadas as suas redes de pesquisa. Assim sendo, para o desenvolvimento da rede mundial, novos protocolos foram desenvolvidos perfazendo assim, um conjunto de normas para se colocar computadores em rede mundial, sendo a primeira versão o IPv4.

Em artigo¹ publicado pelo Centro Federal de Educação Tecnológica do Rio Grande do Norte (CEFET-RN), consta que, a especificação IPv4 foi publicada em setembro de 1981, sob o RFC 791, com o auxílio do *Information Sciences Institute – University of Southern California* (Instituto de Ciências da Informação da Universidade do Sul da Califórnia), com o intuito de utilizar o protocolo para colocar computadores em rede. Nesse sentido, ele é considerado como o elemento integrador da Internet e através do mesmo torna-se possível a conexão de diversas sub-redes.

A rede Internet é composta de diversos *backbones* que, traduzido, se trata de portas construídas através de linhas de alta velocidade de diversos tipos de tecnologia. A cada um desses *backbone* estão conectados varias redes locais de muitas instituições cada uma com suas características de sub-rede. Nesse sentido, empresas se utilizam do IP e outros protocolos de sua família, para interligar computadores. De acordo com Silva e Teixeira (1999), no princípio do desenvolvimento do conjunto de protocolos TCP/IP, pouco ou quase nada se falava ou se desenvolvia em relação à segurança de redes. Com o surgimento de várias aplicações e o rápido crescimento da Internet, passou-se a perceber que as questões relativas à segurança de redes e sistemas tornaram-se demandas cada vez mais crescente.

No material disponível em http://www.w2k.com.br/images/SID/IPV6_ATM/ipv6atm.htm consta que, embora os protocolos do TCP/IP viabilizem a Internet e ofereçam valiosos serviços, existem algumas imperfeições, como por exemplo a questão da segurança.

¹ SILVA, C. E. et al. *IPv6 – Protocolo Internet Versão 6*. Natal: Centro Federal de Educação Tecnológica-RN, 2004.

Quando uma empresa conecta sua rede na Internet sem as defesas, qualquer computador na rede interna com TCP/IP pode (teoricamente) ser acessado por qualquer usuário da Internet, o que representa um risco altíssimo para a segurança das informações e até mesmo para a continuidade dos serviços. Muitos problemas atuais de segurança da transmissão de dados pela Internet estão relacionados com o fato de que o protocolo TCP/IP na sua forma atual (IPv4) não foi projetado para ser seguro, e é sujeito a uma série de ataques.

Para Comer (2001), embora o IPv4 tenha sido definido antes das tecnologias de Rede Local se tornarem populares, o projeto original continuou a funcionar bem através de várias gerações de tecnologias de hardware. Já para Lima (2004), a versão 4 tinha o simples objetivo de facilitar a interconexão de diferentes tecnologias físicas de rede e, essa rede era relativamente pequena, com um número de *hosts*, confiáveis entre si, honrando todos os detalhes previstos nos padrões dos protocolos.

Devido ao crescimento da rede, padrões foram desrespeitados e brechas de segurança nos protocolos começaram a ser exploradas. No que concerne ao aspecto segurança os principais problemas existentes no IPv4 são:

- Facilidade de personificar máquinas da rede (*IP Spoofing*);
- Facilidade de obter informações confidenciais na rede, fazendo *eavesdropping*, caso o meio físico permita; e,
- Nenhuma garantia da integridade dos dados que trafegam na rede.

Neste sentido Sousa Jr. e Puttinni (2004), vem enfatizar a questão de segurança de redes quando comenta que o relatório anual do “*Computer Emergency Response Team*”, uma entidade pertencente ao governo Norte Americano que pesquisa sobre segurança na Internet, listou aproximadamente 2.500 (dois mil e quinhentos) acidentes de segurança os quais atingiram 12.000 (doze mil) “redes” em 1995.

Os ataques relatados de consequências mais graves incluíam “*Ipspoofing*” (ataque que se utilizam de pacotes IP com endereços falsos), “*eavesdropping*” (análise não autorizada dos pacotes que trafegam na rede) e “*packet sniffing*” (ataque no qual um intruso pode diretamente ler as informações transmitidas mesmo as de “*log on*” e conteúdo de base de dados).

Os fatos ocorridos deixaram claro a vulnerabilidade e a necessidade de implementação de mecanismos de segurança que sejam eficazes os quais necessariamente devem cobrir áreas tais como proteção da infra-estrutura contra monitoramento não autorizado e controle de tráfego de

rede. Além disso, torna-se necessário defender o tráfego entre usuários finais usando mecanismos de autenticação e criptografia, sendo assim, a segurança implementada para o protocolo IP é apresentada como uma das soluções do problema.

2.2.1 Motivação para mudar o Ipv4

Conforme Comer (1998), a versão 4 do Internet Protocol (Ipv4) forneceu o mecanismo básico de comunicação da pilha TCP/IP (*Transmission Control Protocol*), para a comunicação através de uma grande variedade de tecnologias de redes básicas e da Internet global. Porém, o Ipv4 permaneceu quase inalterado desde seu início e a longevidade dessa versão mostra que o projeto é flexível e poderoso.

E nesse sentido, faz um breve histórico abordando que, desde quando o IPv4 foi projetado, o desempenho do processador aumentou mais de duas ordens de magnitude, os tamanhos típicos de memória aumentaram 32 vezes, a largura da banda de rede do backbone da Internet cresceu 800 vezes, tecnologias de rede local afloraram e o número de hosts na Internet cresceu de apenas um punhado para 4 milhões. Além disso, as mudanças não ocorreram simultaneamente e o IP conciliou mudanças em uma tecnologia, diante das mudanças em outras.

Contudo, apesar de seu projeto sólido, o Ipv4 deverá ser logo substituído e a motivação primária para a mudança advém do espaço de endereçamento limitado em função do crescimento exponencial da Internet. Em outras palavras, na taxa de crescimento atual, cada um dos atuais prefixos de rede possível será logo atribuído, e nenhum crescimento adicional será possível. Deste modo, a motivação primária para definir uma nova versão de IP surgiu da limitação de espaço de endereçamento – são necessários endereços maiores para acomodar o crescimento contínuo da Internet.

Porém, embora a necessidade de um espaço maior esteja forçando uma mudança imediata no IP, outros fatores estão também contribuindo para o projeto. Particularmente, muita atenção tem sido dispensada para ajudar a apoiar novos aplicativos. Por exemplo, áudio e vídeo em tempo real precisam entregar dados em intervalos regulares. Para manter tais informações circulando a Internet sem interrupção, o IP deve evitar variar freqüentemente as rotas.

Além disso, tem questão da segurança, já que muitos dos novos aplicativos da Internet requerem comunicações seguras, uma nova versão do IP deve incluir recursos que tornem possível validar o transmissor. Assim, o estímulo para a mudança ocorre à medida que aumentos

em volume e em tamanho forçam as melhorias necessárias para manter o serviço, uma vez que novos aplicativos exigem mais tecnologia dominada e já que novas tecnologias tornam possível fornecer outros serviços. Em tese, segundo o autor, os desenvolvimentos que estimulam a evolução e da arquitetura da Internet, recaem em quatro categorias:

- Novas tecnologias de computador e de comunicações – com a disponibilidade de computadores de alta velocidade, eles são usados como hosts* e roteadores**. Com o surgimento de novas tecnologias de rede fez com que eles fossem usados para transportar datagramas IP;
- Novos aplicativos – uma das mais notáveis fronteiras de pesquisa e desenvolvimento da internet, os novos aplicativos freqüentemente criam uma demanda por recursos ou serviços que os protocolos atuais não podem oferecer. Por exemplo, um surto de interesse de multimídia criou a demanda por protocolos que pudessem transferir som e imagens com eficácia. De modo semelhante, o interesse pela comunicação de áudio e vídeo em tempo real criou a demanda por protocolos que pudessem garantir a entrega das informações dentro de um retardo fixo de transmissão, bem como protocolos que pudessem sincronizar correntes de dados de vídeo e áudio;
- Aumentos em tamanho e da carga – a Internet global experimentou muitos anos de crescimento exponencial ininterrupto, duplicando em tamanho a cada nove meses, ou mais rápido ainda. Em princípios de 1994, um novo host aparecia em média, a cada 30 segundos e esse índice foi crescendo de forma drástica. Surpreendentemente, o volume de tráfego da Internet aumentou mais rápido do que o número de redes;
- Novas políticas – à medida que a Internet se expande dentro de novos mercados de trabalho e novos países, ela se transforma de uma maneira fundamental: ganha novas jurisdições administrativas. As mudanças de jurisdição produzem mudanças nas políticas administrativas e impõem novos mecanismos para executar essas políticas.

2.3 O Futuro IP (IPv6)

O IP versão 6 (IPv6) é a nova versão do Internet Protocol, projetado para ser o sucessor do IPv4, nesse sentido, Silva et al. (2004), afirma que a nova versão foi projetada e desenvolvida para atender as necessidades técnicas e mercadológicas atuais e futuras, à medida que o mercado atual tem exigido soluções cada vez mais robustas, integradas e seguras.

* Qualquer sistema de computador de usuário final que se conecta a uma rede

** Computador dedicado de finalidade específica que liga duas ou mais redes e encaminha pacotes de uma para outra.

O autor insere ainda que mediante o iminente esgotamento de endereços e as limitações do IPv4, sendo uma delas, a questão da segurança no tráfego das informações, impulsionaram o desenvolvimento do IPv6.

Entretanto, apesar das limitações pertinentes na versão corrente, o protocolo IPv6 foi desenhado como uma evolução do IPv4, de modo que, as características que se consideram estar na base do sucesso do protocolo, foram mantidas. Da mesma forma, as funcionalidades que não dispensavam um bom desempenho ou que não são de uso freqüente foram removidas ou tornadas opcionais, sendo adicionadas algumas funcionalidades que foram demandadas, sem no entanto, alterar os conceitos de base. Assim sendo, de acordo com o que está inserido em Silva et al. (2004), as principais mudanças no Ipv6 são:

- Capacidade de endereço expandida: no IPv6, cada endereço é determinado por 128 bits, isto é, 4 vezes maior que no IPv4, onde são reservados 32 bits para endereçamento;
- Simplificação do formato do cabeçalho: alguns campos do cabeçalho do IPv4 foram descartados ou tornados opcionais, para simplificar o processamento dos pacotes mais comuns e diminuir o *overhead* do IPv6, que possui um cabeçalho maior;
- Maior suporte para campos opcionais e extensões: os campos opcionais possuem agora menos restrições quanto ao seu tamanho, há maior flexibilidade para a introdução de extensões futuras, o encaminhamento de pacotes fica mais simplificado e pode ser diferenciado a cada *hop*;
- Capacidade para identificação de fluxo: o originador dos pacotes tem como identificar um fluxo de pacotes para um determinado destino e pedir tratamento especial desse fluxo por parte do roteador, como QoS (*Quality of Service – Qualidade de Serviço*) diferenciado e serviço de tempo real. No IPv4, esse tipo de funcionalidade é implementado por roteadores e switches de camadas 3 ou 4, sobrecarregando seu processamento.

2.3.1 As principais Vantagens do IPv6

Além de maior capacidade de endereçamento, Silva et al. (2004), explica que o IPv6 oferece as seguintes vantagens:

- Suporte a multiprotocolos e mobilidade – uma grande parte do espaço de endereçamento IPv6 foi reservada para uso futuro e essa parte poderá ser alocada para outros protocolos. O suporte para comunicações móveis também é um dos direcionamentos do IPv6, constituindo este, um fator determinante nas funcionalidades e crescimento na telefonia móvel de 3ª geração;

- QoS (*Quality of Service – Qualidade de Serviço*) para transmissões de dados mais críticos com priorização de tráfego - os campos “*Traffic Class*” (*Tráfego de Classes*) “*Flow Label*” (*Fluxo*) foram criados especialmente para facilitar o desenvolvimento de protocolos para controle de tráfego em tempo real, como o RSVP (*Resource Reservation Protocol*), de forma a permitir a implementação na Internet de aplicações multimídia e com a integração de serviços de dados, voz e vídeo em tempo real;

- Segurança nativa nas informações contidas nos pacotes – as especificações do IPv6 definiram dois mecanismos de segurança inclusos no IPSec (*Internet Protocol Security*): autenticação de cabeçalho (*Authentication Header*) e segurança do encapsulamento IP (*Encrypted Security Payload*).

- Sistema de autoconfiguração – quando se instala um host (servidor/cliente) numa rede, automaticamente será atribuído um endereço composto pelas componentes AG:TLA:NLA:SLA:EU164. Esta característica de autoconfiguração, denominada “*stateless autoconfiguration*”, estará presente no IPv6 eliminando a necessidade de se configurar manualmente este tipo de equipamentos.

2.3.2 Segurança no IPv6

Em várias publicações de estudo sobre segurança de redes encontram-se afirmações em comum que o IPv4 apresenta uma série de falhas de segurança, que não garante a autenticidade e privacidade no tráfego das informações, ao passo que, o IPv6 foi desenvolvido, para oferecer características de segurança aos datagramas e que essa segurança já é incorporada ao protocolo.

Conforme Lima (2004), neste novo protocolo, todas as máquinas na rede trazem uma implementação nativa de segurança que oferece recursos para garantir confidencialidade, integridade e autenticidade de dados de rede. Essa implementação de segurança é o IPSec (*IP SEcurity - Segurança do Protocolo Internet*) que inclusos estão dois mecanismos de segurança, quais sejam: autenticação de cabeçalho (*authentication header*) e segurança do encapsulamento IP (*encrypted security payload*).

- Autenticação de Cabeçalho (*Authentication Header - AH*) – com esse método, o cabeçalho é autenticado, garantindo assim a identidade do remetente, e que o pacote não foi alterado em tráfego. A informação pertinente é armazenada em um *Authentication Header*, que é um dos possíveis cabeçalhos de extensão.

- Segurança do Encapsulamento (*Encrypted Security Payload - ESP*) – esse método criptografa os dados enviados e armazena as informações pertinentes em um ESP (outro tipo de cabeçalho de extensão). Assim, é possível garantir que caso a informação transmitida seja interceptada por pessoas não autorizadas, estas serão incapazes de compreendê-las, garantindo assim a privacidade.

De acordo com Sousa Jr e Puttinni (2004), consideram que um conceito chave que aparece em ambos os mecanismos de autenticação e privacidade para o protocolo IP é a associação de segurança – conjunto de directivas que permite negociar algoritmos de cifra a utilizar. Dessa forma, uma associação é uma relação de sentido único entre um emissor e um receptor que descreve quais os mecanismos de segurança a utilizar para estabelecer uma comunicação segura.

Assim sendo, explicam os autores, para uma relação que se processa em dois sentidos (origem/destino) é necessário, então, duas associações de segurança. Essa associação é unicamente identificada por um endereço Internet e um índice de parâmetro de segurança (*Security Parameter Index - SPI*). Reiterando, em qualquer pacote (informações) IP, a associação de segurança é unicamente identificada pelo endereço de destino e pelo SPI.

Na visão dos autores, a aplicação de segurança em nível IP engloba áreas funcionais quais sejam: autenticação e privacidade sendo que a primeira assegura que um pacote recebido foi realmente transmitido pela origem identificado no cabeçalho do pacote, e, a segunda, permite que sejam criptografados os dados transmitidos de modo a prevenir interceptação de terceiros. Em outras palavras, mesmo que a mensagem seja interceptada, seu conteúdo não poderia ser lido.

Em ambos os casos as características de segurança são implementadas como cabeçalhos de extensão que seguem o cabeçalho IP principal (no IPv6), ou, no caso do IPv4, no campo “options”. O cabeçalho de extensão para autenticação é conhecido como *Cabeçalho de Autenticação (Authentication Header)* enquanto o correspondente à privacidade é conhecido como *Cabeçalho de Encapsulamento de Dados de Segurança (Encapsulating Security Payload)*. O suporte a essas características é opcional para a versão 4 (IPv4) e obrigatório para a versão 6 (IPv6).

Lima (2004), vem corroborar e afirma que, dentro desse cenário ideal, ataques clássicos possíveis no Protocolo IPv4, podem ser evitados em IPv6, como por exemplo, *IP Spoofing* pode ser eliminado completamente com a utilização do *Authentication Header - AH* com certificados digitais e/ou *preshared keys*. Pois, esse mecanismo usa algoritmos e assinatura digital para

autenticar todos os pacotes IP. Portanto, a grande maioria dos ataques, que usa técnica de personificação, seria eliminada dentro da rede IPv6.

A segurança do Encapsulamento (*Encrypted Security Payload - ESP*) garante a impossibilidade de *eavesdropping*, como também, pode ser usado para fins de autenticação. Todavia, AH é mais interessante pois, autentica o pacote inteiro, incluindo o cabeçalho IP (exceto aqueles campos do cabeçalho que precisam ser alterados em trânsito) enquanto ESP autentica apenas o *payload* do datagrama. Assim sendo, esses dois métodos podem ser utilizados em conjunto, a fim de fornecer tanto autenticidade quanto privacidade, garantindo segurança em três aspectos muito importantes, de modo que certifica:

- Quem enviou a determinada informação;
- Que a informação não está adulterada por terceiros;
- Que a informação não foi lida por terceiros, ou seja, correspondendo a informação realmente enviada.

Nesse sentido, o suporte IPsec é um conjunto de protocolos que permite a troca de pacotes de modo seguro na camada IP. Este conjunto é usado largamente na implementação de Redes Virtuais Privadas (VPN – *Virtual Private Network*). Fornece serviços de segurança na camada de rede IP, permitindo um sistema selecionar protocolos de segurança requeridos, determinar os algoritmos usados pelos serviços e chamar chaves criptográficas necessárias para algum serviço. Em IPv4, o suporte IPsec é opcional e, em geral, nenhuma plataforma de software ou hardware oferece IPsec nativamente em suas implementações. Sendo que, o IPv6 apresenta a vantagem de já possuí-lo e foi projetado para atender as necessidades técnicas e mercadológicas atuais e futuras à medida que o mercado exige soluções de segurança em termos de autenticidade e privacidade de dados ao passo que, permite uma maior flexibilidade e segurança, visto que, pode-se periodicamente evoluir para um método criptográfico mais seguro.

2.4 Arquitetura Básica do IPsec

De acordo com Silva e Teixeira (1999), a plataforma do IPsec foi desenvolvida para prover serviços de segurança da alta qualidade, baseados em criptografia, para o nível IP e/ou para as camadas superiores. No conjunto de serviços oferecidos pelo IPsec estão inclusos: controle de acesso, integridade não orientada à conexão, autenticação da origem dos dados e confidencialidade (criptografia).

Estes serviços são implementados através da utilização conjunta de protocolos de segurança de tráfego de dados, de autenticação de cabeçalho (AH – *Authentication Header*), de encapsulamento seguro do *payload* ou conteúdo dos dados (ESP – *Encapsulating Security Payload*) e de procedimentos e protocolos de gerência de chaves.

Ainda parafraseando com os autores, além de ser um padrão aberto pela IETF que está sendo adotado por todos os fabricantes de equipamentos de redes de computadores e desenvolvedores de sistemas, por definição o IPSec possui uma arquitetura aberta no sentido de possibilitar a inclusão de outros algoritmos de autenticação e criptografia. No que concerne a diretrizes para produção, organização e inter-relacionamento entre os diversos documentos que descrevem o conjunto de protocolos IPSec, são apresentados através da RFC 2411 – *IP Security Document Roadmap*.

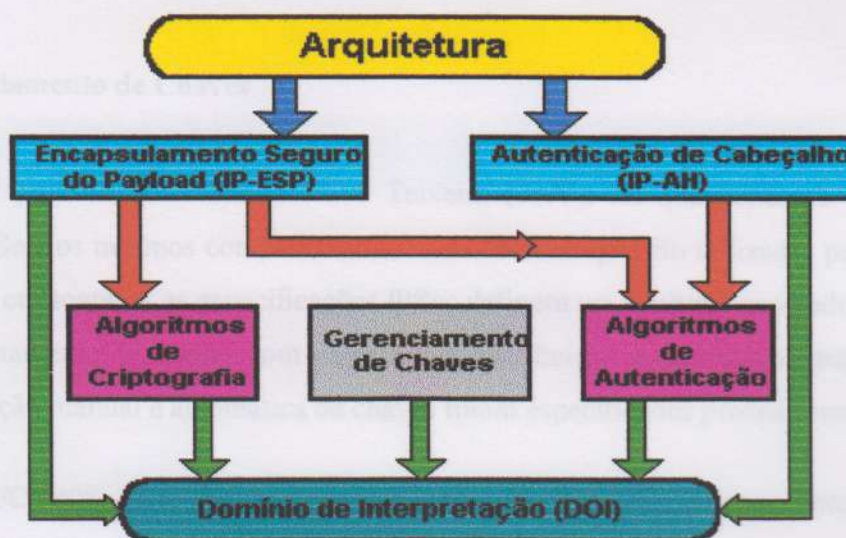


Figura 1 – Arquitetura do IPSec

Fonte: SILVA, Adailton J. S., TEIXEIRA, Renata Cicilini. News Generation: boletim bimestral sobre tecnologia de redes. Produzido e publicado pela RNP – Rede Nacional de Ensino Pesquisa – vol 3, número 4. ISSN 1518-597

A figura 1 apresenta a arquitetura IPSec e o roadmap para especificações que descrevem o uso de algoritmos de autenticação e criptografia definidas pelo protocolo ESP (RFC 2406 – *IP Encapsulating Security Payload*), e de autenticação definidas pelo protocolo AH (RFC 2402 – *IP Authentication Header*).

2.4.1 Protocolos AH e ESP

Os protocolos AH e ESP fazem parte da arquitetura básica IPSec e, conforme Silva e Teixeira (1999), por questões de garantia de interoperabilidade, estes protocolos estabelecem que

todas as implementações IPSec suportem alguns algoritmos pré-definidos. Para autenticação de cabeçalho os algoritmos obrigatórios são os seguintes:

- HMAC-MD5, RFC 2403 – *The Use of HMAC-MD5 within ESP and AH*;
- HMAC-SHA-1, RFC 2404 – *The Use of HMAC-SHA-1 within ESP and AH*.

Para o encapsulamento seguro do *payload*, além destes dois já citados os outros algoritmos são:

- DESC-CBC, RFC 2405 – *ESP DES-CBC Cipher Algorithm With Explicit IV*;
- Null Authentication Algorithm;
- Null Encryption Algorithm.

As especificações IPSec também suportam negociação de compressão IP definidas pela RFC 2393 – *IP Payload Compression Protocol*.

2.4.2 Gerenciamento de Chaves

Ainda parafraseando com Silva e Teixeira (1999), no que concerne aos serviços de segurança IPSec, os mesmos 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 de chaves foram especificados procedimentos RFCs:

- RFC 2408 – *Internet Security Association and Key Management Protocol (ISAKMP)*;
- RFC 2409 – *The Internet Key Exchange (IKE)*;
- RFC 2412 – *The OAKLEY Key Determination Protocol*.

Os autores afirmam, que mesmo com as definições desses padrões, as especificações IPSec permitem a inclusão de outros protocolos de gerência de chaves públicas como, por exemplo, SKIP.

2.4.3 Funcionamento do IPSec

No que concerne ao funcionamento do IPSec Silva e Teixeira (1999), explica que o protocolo IPSec opera num *gateway* ou num *host*, com os requisitos de segurança estabelecidos por um banco de dados de política de segurança (*SPD – Security Policy Database*) mantido pelo

usuário, pelo administrador da rede ou por uma aplicação operando dentro de limites pré-definidos. Pode ser utilizado para proteger uma ou mais conexões entre um par de *hosts*, entre dois *gateways* de segurança ou entre um *host* e um *gateway*. A figura 2 ilustra a afirmação.

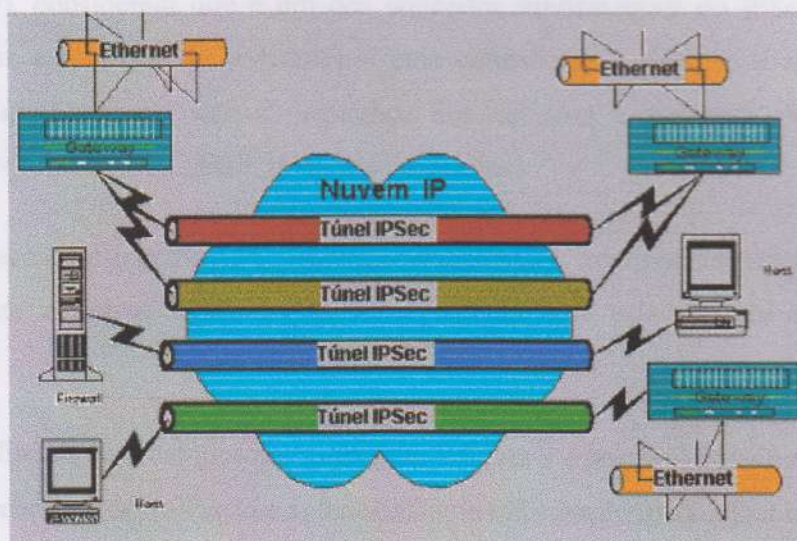


Figura 2 – Túneis IPsec entre Sistemas

Fonte: SILVA, Adailton J. S., TEIXEIRA, Renata Cicilini. News Generation: boletim bimestral sobre tecnologia de redes. Produzido e publicado pela RNP – Rede Nacional de Ensino Pesquisa – vol 3, número 4. ISSN 1518-597

Dessa forma, os pacotes IP são selecionados através de três formas de processamento definidas por seletores. Os seletores utilizam o pacote IP e as informações do cabeçalho da camada de transporte, comparando-as com as entradas do banco de dados SPD. Com base nas políticas aplicadas e identificadas pelos seletores, cada pacote ou é submetido aos serviços IPsec, ou é permitido desprezar tais serviços ou então é descartado.

2.4.4 Implementação do IPsec

Ao que se refere à implementação do IPsec conforme Silva e Teixeira (1999), o mesmo pode ser implementado de três formas:

A primeira refere-se à implementação IPsec na pilha nativa IP, aplicável tanto em *hosts* como em *gateways*. O pré-requisito para isso é o acesso ao código fonte do protocolo IP. A segunda forma de implementação é conhecida como *Bump-in-the-stack* (BITS) é usualmente utilizada em *hosts*, onde o IPsec é implementado sob o protocolo IP, entre este e o *driver* de rede local. Neste caso, o acesso ao código fonte IP não é necessário. *Bump-in-the-wire* (BITW) é a terceira forma de implementação IPsec, na qual é utilizada uma placa processadora de criptografia tanto em *hosts* como em *gateways*.

2.4.5 Associação de Segurança

Com relação a Associação de Segurança – AS, (*Security Association – AS*), Silva e Teixeira (1999), consideram que é um dos conceitos fundamentais do IPSec e nesse sentido, define que uma associação de segurança é uma conexão que viabiliza o tráfego de serviços seguros. Afirmam também, que a segurança dos serviços é garantida pela utilização dos protocolos de segurança (AH, ESP, ou ainda por ambos).

- No caso do protocolo AH, *Authentication Header*, adiciona autenticação e integridade, ou seja, garante a autenticidade do pacote e também que este não foi alterado durante a transmissão.

Na definição dos campos que compõem a figura 3 é possível compreender o mecanismo AH no que concerne a identificação e autenticação da informação (pacote) na rede.

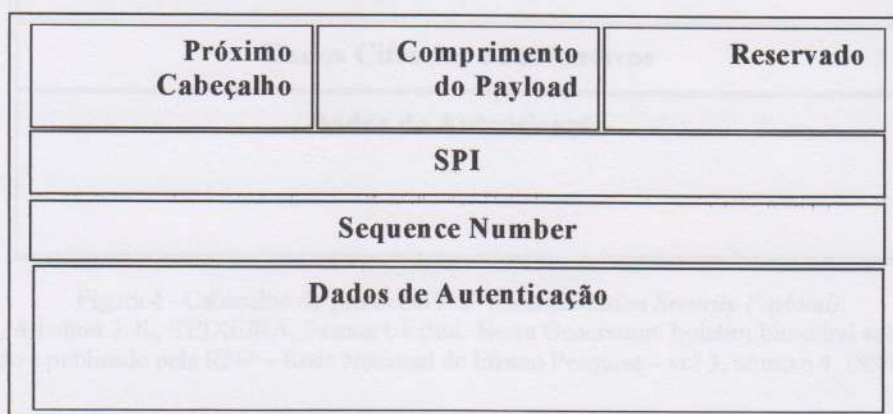


Figura 3 –Cabeçalho do protocolo AH (*Authentication Header*)

Fonte: SILVA, Adailton J. S., TEIXEIRA, Renata Cicilini. News Generation: boletim bimestral sobre tecnologia de redes. Produzido e publicado pela RNP – Rede Nacional de Ensino Pesquisa – vol 3, número 4. ISSN 1518-597

Definindo os campos que compõe o cabeçalho do protocolo de segurança AH tem-se:

- Próximo Cabeçalho: contém o identificador do protocolo próximo cabeçalho;
- Comprimento do Payload: comprimento do *payload* (conteúdo);
- Reservado: 16 bits reservado para extensão do protocolo;
- SPI (*Security Parameter Index*): este índice, em conjunto com o protocolo AH e o endereço fonte, identifica unicamente uma AS para um determinado pacote;
- Sequence Number: contador que identifica os pacotes pertencentes a uma determinada AS (usado como mecanismo anti-replay).

- **Dados de Autenticação:** campo de comprimento variável que contém o ICV (*Integrity Check Value*) para este pacote, que é calculado seguindo o algoritmo de autenticação usado, definido pela AS.

O AH adiciona autenticação, porém os dados continuam trafegando na rede intactos, e podem ser capturados através de *sniffers*, por exemplo. Assim, a confidencialidade é tratada por outro protocolo, o ESP. E, nesse sentido, de acordo com Silva e Teixeira (1999), o protocolo ESP (*Encapsulating Security Payload*), adiciona autenticação e confidencialidade, garantindo que somente os destinatários autorizados terão acesso ao conteúdo do pacote.

Na definição dos campos que compõem a figura 4 compreende-se o mecanismo da confidencialidade.

<i>SPI</i>
<i>Sequence Number</i>
Dados Cifrados e Parâmetros
Dados de Autenticação

Figura 4 –Cabeçalho do protocolo ESP (*Encapsulation Security Payload*)

Fonte: SILVA, Adailton J. S., TEIXEIRA, Renata Cicilini. News Generation: boletim bimestral sobre tecnologia de redes. Produzido e publicado pela RNP – Rede Nacional de Ensino Pesquisa – vol 3, número 4. ISSN 1518-597

Os campos que compõem o cabeçalho ESP são assim definidos:

- **SPI (*Security Parameter Index*):** este índice, em conjunto com o protocolo AH e o endereço fonte, identifica unicamente uma AS para um determinado pacote;
- ***Sequence Number*:** contador que identifica os pacotes pertencentes a uma determinada AS (usado como mecanismo anti-replay);
- **Dados Cifrados e Parâmetros:** contêm os dados cifrados e os parâmetros utilizados pelo algoritmo de criptografia usado, definido pela AS;
- **Dados de Autenticação:** campo de comprimento variável que contém ICV (*Integrity Check Value*) para este pacote, calculado seguindo o algoritmo de autenticação usado, definido pela AS.

Para os casos em que se exige apenas a autenticação, ou ainda, onde a confidencialidade não deve ser usada, Silva e Teixeira (1999), explica que é recomendada a utilização do AH.

No entanto, enfatizam que a situação ideal é a utilização de autenticação e confidencialidade, ou seja, a utilização do AH e ESP em conjunto. Nesse sentido, especificam que é recomendado o uso do ESP “dentro” do AH, permitindo que o destino verifique a autenticidade e decifre o pacote em paralelo. A figura 5 apresenta os dois mecanismos utilizados em conjunto.

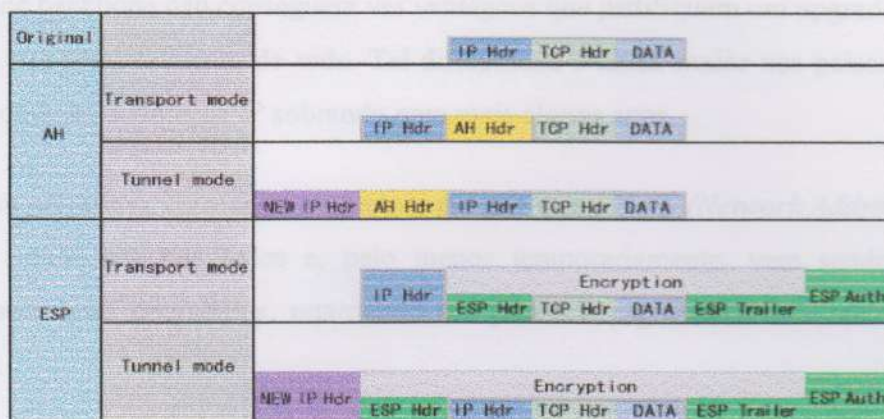


Figura 5 – Protocolos AH e ESP

Fonte: http://www.nri-aitd.com/tips/image/ipsec_pic.gif

Qualificando a utilização conjunta dos dois mecanismos para a segurança no tráfego das informações, conforme o que está inserido em Silva e Teixeira (1999), o uso do AH previne ataques do tipo:

- *Replay*, ou seja, quando o atacante intercepta um pacote válido e autenticado pertencente a conexão, replica-o e o reenvia, “entrando na conversa”.
- *Spoofing*, ou seja, quando um atacante assume o papel de uma máquina confiável para o destino e, dessa forma, ganha privilégios na comunicação. A utilização de mecanismos de autenticação previne este tipo de ataque;
- “Roubo de conexões” (*connection hijacking*), ou seja, quando o atacante intercepta um pacote no contexto de uma conexão e passa a participar da comunicação. A utilização de mecanismos de autenticação previnem este tipo de ataque.

O uso do ESP previne 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 um 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 esse tipo de ataque.

2.5 Considerações sobre a Mudança para o IPv6

A questão da escassez de endereços IP, como também, a questão da segurança no tráfego das informações, são de fato alguns dos fatores que convergem à evolução IPv6. Contudo, Lima (2004), esclarece que existe uma resistência para a mudança, que reside no fato de que as operadoras de backbone não conseguem ver vantagens que justifiquem um upgrade imediato para o IPv6, em sua atual estrutura de rede. Tal dificuldade é ainda maior nos países do continente americano, onde há endereços IP sobrando para mais alguns anos.

Outro ponto a se considerar segundo o autor, é que o NAT (*Network Address Translation*) vem sendo usado em tais redes e, pelo menos temporariamente, vem sendo uma solução suficiente para estas operadoras, retardando um pouco o esgotamento dos seus endereços IP disponíveis.

Entretanto, o NAT é uma solução que oferece grandes problemas: roteadores e *firewalls* devem oferecer tal mecanismo, ampliando a complexidade de desenvolvimento e administração dos mesmos, pode não oferecer suporte a certas aplicações P2P (*Peer to Peer*), podendo trazer problemas para a implementação de *Virtual Privat Networks*. Ainda, há de se considerar que muitas aplicações ainda não foram portadas para IPv6, alguns equipamentos não trazem IPv6 em sua pilha de protocolos e muitos recursos importantes não foram completamente padronizados pelo IETF.

Dessa forma, na tentativa de introduzir o protocolo IPv6 para o mercado várias possíveis vantagens, em relação ao antigo IPv4, são citadas e exploradas, gerando muita polêmica em torno dessas vantagens.

As polêmicas geradas em torno dessas vantagens está no fato de que, na prática, muitas soluções similares podem ser implementadas usando o protocolo IPv4 original com alguns protocolos, softwares e/ou hardwares adicionais, considerando ainda, que não existem aplicações que demonstrem que o modelo atual, usando o NAT, deva ser substituído imediatamente pelo protocolo IPv6 com o seu número maior de endereços.

Portanto, o resultado é uma forte resistência para a substituição do IPv4 para o IPv6, entretanto não se pode deixar de considerar que as vantagens existem, mas as operadoras ainda não são capazes de aproveitá-las integralmente por esses motivos. Na opinião do autor, o desenvolvimento de uma "*killer Application*" seria fundamental para uma mais rápida adoção do protocolo IPv6.

2.6 Definição de Segurança em Redes de Computadores

Conforme a visão de Comer (2001), embora o conceito de uma rede segura seja atraente para a maioria dos usuários, as redes não podem ser classificadas simplesmente como seguras ou não-seguras porque o termo não é absoluto. O autor explica que sob a questão segurança, cada organização define o nível de acesso que é permitido ou negado, mediante que, algumas organizações armazenam dados que são valiosos e essas definem uma rede segura como um sistema que impede que estranhos acessem seus computadores.

De outro modo, existem organizações que necessitam disponibilizar informações para estranhos, mas proibindo-os de modificar os dados. Em outras palavras, o autor deixa subentendido que é complexo a questão de definição de uma rede segura e neste sentido exemplifica:

- Há organizações que definem uma rede segura como uma rede que permite acesso arbitrário a dados, porém, inclui mecanismos que impedem mudanças sem autorização;
- Ainda outros grupos se concentram em manter a comunicação privada e definem uma rede segura como uma rede em que ninguém além do receptor pretendido possa interceptar e ler uma mensagem;
- Finalmente, muitas organizações de grande porte necessitam de uma definição complexa de segurança, que permite acesso a dados ou serviços selecionados que a organização decide tornar públicos, ao impedir acesso ou modificação de dados e serviços sensíveis que são mantidos privados.

Dessa forma, é complexa a definição de rede segura à medida que, não existe uma definição absoluta de rede segura, e sendo assim, o primeiro passo que uma organização deve tomar para obter um sistema seguro é definir uma política de segurança. A política não especifica como obter proteção, porém, deve afirmar claramente os itens que devem ser protegidos.

Assim, desenvolver uma política de segurança de rede pode ser complexo, mas é o primeiro passo para a organização, pois, uma política racional exige que a organização avalie o valor de suas informações e deve se aplicar a informações armazenadas em computadores e também a informações cruzando uma rede.

2.6.1 Aspectos de Segurança de Redes

Os aspectos de segurança de uma rede devem assumir um balanço entre segurança e facilidade de uso e nesse sentido, segundo Comer (2001, p. 444), uma organização pode considerar:

- Integridade dos Dados – que se refere a proteção contra mudança: os dados que chegam em um receptor são exatamente os mesmos que foram enviados?
- Disponibilidade dos Dados – que se refere à proteção contra a interrupção de serviço: os dados permanecem acessíveis para uso legítimo?
- Confidencialidade e Privacidade dos Dados – referem-se à proteção contra bisbilhotice ou grampo: os dados são protegidos contra acesso sem autorização?

Dessa forma, existem vários aspectos de segurança que precisam ser considerados pois, o problema de segurança da rede surge de um conflito fundamental: embora a comunicação requeira um nível de confiança mútua entre as partes que se comunicam, uma rede de computador pode estabelecer a comunicação entre os grupos que desenvolvem uma desconfiança mútua.

2.7 Considerações sobre Segurança de Rede e de Informação

Segundo Comer (1998, p. 524), “Os termos *segurança de rede e segurança de informação* referem-se, em geral, à certeza de que as informações e os serviços disponíveis em uma rede não podem ser acessados por usuários não-autorizados.” Insere ainda o autor, que segurança implica proteção inclusive garantia de integridade dos dados, proteção contra acesso não-autorizado dos recursos do computador, pessoas investigando ou fazendo ligações clandestinas de escuta, e contra a interrupção de serviços. Contudo, acrescenta que, assim como nenhuma propriedade particular mesmo com todo aparato de segurança está completamente protegida, assim também, nenhuma rede também está totalmente segura. Dessa forma, embora não se possa impedir totalmente um crime, medidas básicas de segurança deverão ser tomadas no intuito de tornar significativamente mais difícil de ser impetrado. Neste sentido, o autor enfatiza que fornecer segurança de informações requer proteção não apenas dos recursos físicos como também dos recursos abstratos.

Recursos físicos incluem dispositivos de armazenagem passiva, tais como fitas magnéticas e discos, e também dispositivos ativos como computadores de usuários. Em um

ambiente de rede, a segurança física estende-se a cabos, pontes e roteadores que constituem a infra-estrutura da rede. A segurança física pode impedir uma escuta telefônica, pode eliminar ataques que impliquem em sabotagem (exemplo: desativar um roteador para fazer com que os pacotes sejam roteados através de um trajeto e menos seguro). Assim, a segurança física desempenha um papel preponderante no plano de segurança geral.

Proteger um recurso abstrato como a informação via de regra é mais difícil do que fornecer segurança física, porque a informação é algo abstrato. A *integridade dos dados* (proteção contra mudanças não autorizadas) é crucial; também o é a *disponibilidade dos dados* (garantia de que pessoas de fora não tenham a capacidade de impedir o acesso legítimo aos dados através da saturação do tráfego de uma rede). Assim, como a informação pode ser copiada à medida que trafega por uma rede, a proteção deve também prevenir a escuta não-autorizada. Em outras palavras, a segurança da rede deve garantir a *privacidade*. Nesse sentido, sabendo-se que as informações podem ser acessadas e transferidas em alta velocidade, pode ser difícil perceber a diferença entre um acesso legítimo e um ilegítimo quando estiver ocorrendo uma transferência. Assim sendo, enquanto a segurança física geralmente classifica pessoas e recursos em categorias amplas (por exemplo, proibir o acesso privativo aos que não sejam funcionários), a segurança para a informação precisa ser ainda mais restritiva.

3.3 Técnicas e Procedimentos da Pesquisa

3.3.1 Leitura e Coleta de Dados

Para a coleta de dados a pesquisa se utilizou de fontes de dados primárias contidas em referências bibliográficas, artigos, livros, jornais (Jornal) e sites eletrônicos. A coleta de dados foi realizada através de uma pesquisa bibliográfica que foi o primeiro passo para a análise da temática objeto de estudo.

3 METODOLOGIA

3.1 Tipo de Pesquisa

Para classificar a tipologia da pesquisa, tomou-se como base os critérios adotados por Vergara (2000), os quais propõem a qualificação das pesquisas sob dois aspectos: quanto aos fins e quanto aos meios.

Quanto aos fins, a pesquisa se caracteriza como exploratória e explicativa. Exploratória à medida que avança através de leitura analítica buscando a compreensão e explicitando os pressupostos que fundamentam a temática objeto de estudo. Explicativa, porque esclarece os resultados à luz dos fundamentos teóricos que deram suporte à mesma.

Quanto aos meios, se caracteriza como bibliográfica à medida que, para a fundamentação teórico-metodológica do estudo, construiu-se um suporte teórico sobre assuntos relacionados à temática em questão.

3.2 Método de Pesquisa

O método de pesquisa se caracteriza como um estudo dialético histórico, e comparativo com o propósito de expor sob a perspectiva qualitativa, a análise dos mecanismos e impactos de utilização na segurança das informações com a migração para o Protocolo IPv6.

Dessa forma, a pesquisa buscou examinar o que se considera como uma nova geração do protocolo IP dentro de seu contexto, entretanto, se atendo mais especificamente na questão da segurança das informações, esclarecendo suas vantagens e desvantagens através de uma avaliação.

3.3 Técnicas e Procedimentos da Pesquisa

3.3.1 Leitura e Coleta de Dados

Para a coleta de dados a pesquisa se utilizou de fontes de dados primários contidos em referências normatizadas, artigos, meio eletrônico (Internet) e estudos acadêmicos já realizados sobre a temática, perfazendo assim, um levantamento bibliográfico que foi o conteúdo cognitivo que deu o suporte para a análise da temática objeto de estudo.

4 ANÁLISE DOS RESULTADOS

Este trabalho teve como objeto de estudo a análise dos mecanismos e impactos de utilização na segurança das informações com a migração para o Protocolo IPv6. Assim sendo, relata-se aqui neste capítulo, a interpretação e análise de conteúdo referente ao levantamento de dados resultante da coleta. Nesse sentido, conforme determinado na metodologia a interpretação e análise se dá discursivamente de forma progressiva, levando-se em conta a ordem determinada nos objetivos específicos, para posteriormente, se ater ao que se conclui como objetivo geral.

Assim, principiando a interpretação e análise do objeto de estudo e considerando a ordem das questões a serem respondidas, tem-se na seqüência os resultados decorrentes do que foi pesquisado através do levantamento bibliográfico.

4.1 Quanto as Desvantagens do Protocolo IPv4 em Termos de Segurança das Informações

Constata-se que os principais problemas de segurança no tráfego das informações existentes na versão 4 (IPv4) são:

- Facilidade de personificar máquinas da rede através de *IP Spoofing* que corresponde a um tipo de ataque em que se utilizam de pacotes IP com endereços falsos;
- Facilidade de obter informações confidenciais na rede, fazendo *eavesdropping* que corresponde a análise não autorizada dos pacotes que trafegam na rede;
- Nenhuma garantia de integridade dos dados que trafegam na rede.

Tomando por princípio que não há nenhuma garantia de integridade dos dados que trafegam na rede, pode-se afirmar conforme o que está inserido em Lima (2004), que em IPv4, esses ataques podem redirecionar todo o tráfego de uma rede para uma máquina maliciosa.

Em outras palavras, seria o mesmo que dizer que se uma empresa tem conectado sua rede na Internet sem as defesas, qualquer outro computador na rede interna pode ser acessado por qualquer usuário da Internet, o que significa um risco extremo para a segurança das informações e para a continuidade dos serviços. Nesse sentido, isso acontece porque não há nenhum mecanismo de proteção para autenticar as mensagens trocadas.

Dessa forma, fornecer segurança, conforme o que afirma Comer (2001, p. 444), requer proteção não apenas dos recursos físicos como também dos abstratos. Entendendo que recursos físicos incluem fitas, discos, computadores, ao passo que, recursos abstratos são as informações.

Assim, em um ambiente de rede, a segurança física que se estende a cabos, pontes, roteadores, constituem a infra-estrutura da rede, podendo essa segurança impedir uma escuta telefônica e/ou eliminar ataques que impliquem sabotagem. Já sendo mais difícil, fornecer segurança ao recurso abstrato (informação), à medida que este pode ser acessado e transferido em alta velocidade.

Nesse sentido, considera-se que os aspectos de segurança de uma rede e segurança de informação incluem integridade dos dados (proteção contra mudanças não autorizadas), disponibilidade dos dados (garantia de que pessoas de fora não tenham capacidade de impedir o acesso legítimo aos dados através da saturação do tráfego de uma rede), confidencialidade e privacidade dos dados (proteção contra bisbilhotice ou grampo).

Desta forma, caracterizando as desvantagens do Protocolo IPv4 em termos de segurança das informações, considerando os fundamentos acima abordados, pode-se afirmar que: o IPv4, apresenta falhas mostrando-se extremamente vulnerável à utilização propositalmente maliciosa por parte dos usuários interligados a grande rede contra outras máquinas conectadas a mesma rede, não dispondo de mecanismos de segurança à integridade, confidencialidade, privacidade e autenticidade das informações trafegadas, deixando evidente a necessidade da implementação de recursos que possam garantir uma infra-estrutura de segurança.

4.2 Quanto as Vantagens do Protocolo IPv6 em Termos de Segurança das Informações

Constatou-se que o IPv6 traz segurança nativa através do IPSec (*Internet Protocol Security*) que é um conjunto de protocolos desenvolvidos para prover serviços de segurança nos aspectos confidencialidade, integridade e autenticidade das informações contidas nos pacotes através de dois mecanismos de segurança quais sejam: autenticação de cabeçalho (*Authentication Header*) e segurança do encapsulamento IP (*Encrypted Security Payload*).

A afirmação acima é confirmada por Silva e Teixeira (1999), esclarecendo que a plataforma do IPSec foi desenvolvida para prover serviços de segurança de alta qualidade, baseados em criptografia, para o nível IP e/ou para as camadas superiores e que no conjunto de serviços oferecidos pelo IPSec estão inclusos: controle de acesso, integridade não orientada à conexão, autenticação da origem dos dados e confidencialidade (criptografia).

Nesse sentido, através do mecanismo de Autenticação de Cabeçalho (AH), é possível garantir a autenticidade e integridade da informação, ou seja, que o pacote não foi alterado no

tráfego, como também, a identidade do remetente, à medida que esse mecanismo usa algoritmos e assinatura digital para autenticar todos os pacotes.

Da mesma forma, a Segurança do Encapsulamento (ESP) através da criptografia, armazena as informações pertinentes, garantindo que, mesmo que a informação seja interceptada por pessoas não autorizadas, estas não serão capazes de compreendê-la, garantindo assim, a confidencialidade e privacidade dos dados.

Com a utilização do protocolo AH, pode-se prevenir ataques do tipo: "Replay", "Spoofing" e "Roubo de Conexões" (*connection hijacking*). Da mesma forma, o protocolo ESP previne ataques do tipo "Replay" de maneira análoga ao AH, "Particionamento de pacotes cifrados" e "Sniffer".

Constatou-se também, que o tráfego de serviços seguros promovidos pelo IPsec através dos protocolos AH e ESP, provém da utilização em conjunto dos mesmos. Em outras palavras, a utilização desses mecanismos em conjunto, formam uma associação de segurança (AS), que viabiliza o tráfego de serviços seguros. Essa associação é identificada unicamente por três parâmetros: o SPI (*Security Parameter Index*), o endereço IP de destino e o identificador do protocolo (AH ou ESP). Sendo o SPI, um número que identifica uma AS, que é definido durante a negociação que antecede o estabelecimento da mesma, e, dessa forma, todos os membros de uma AS devem conhecer o SPI correspondente e usá-lo durante a comunicação.

Assim, constatou-se em termos de vantagens no que concerne a questão da segurança baseado no que foi estudado, que esses mecanismos utilizados em conjunto formam uma plataforma para prover serviços de segurança de alta qualidade para o tráfego das informações certificando quem enviou a determinada informação, que a informação não se encontra adulterada, e ainda que, através da confidencialidade e privacidade garantida pela criptografia, que a informação não foi lida por terceiros, de modo que, o pacote de informação vai realmente corresponder ao que de fato foi enviado.

Assim, considera-se que o IPv6 possui como vantagens em termos de segurança das informações, funcionalidades que garantem serviços de segurança no tráfego das informações que permitem e garantem que a informação chegue ao seu destino sem alteração.

Contudo, há de considerar que essa estrutura de segurança pode ser adicionada ao IPv4, porém, o IPv6 apresenta a grande vantagem de possuí-la nativamente, suprimindo assim, as limitações da atual versão IPv4.

4.3 Os Protocolos IPv4 e IPv6 na Segurança das Informações

Considera-se com base no que foi pesquisado que o Protocolo IPv6 oferece melhores condições de uma infra-estrutura de segurança. Em outras palavras, pode-se afirmar que os recursos que podem garantir uma infra-estrutura de segurança à rede, estão incluídos no Protocolo IPv6, o qual se caracteriza como a nova geração de protocolos Internet, projetado para atender as necessidades e suprir as limitações da atual versão IPv4, sendo uma delas a questão da segurança no tráfego das informações.

Nesse sentido, a figura 5 apresenta uma comparação entre os protocolos IPv4 e IPv6 em termos de segurança das informações, que evidencia os recursos e aspectos que formam a estrutura de segurança oferecida pela nova versão.

Recursos de Segurança	Protocolo IPv6	Protocolo IPv4
Protocolos de Segurança AH e ESP	É mandatório, ou seja, faz parte nativamente.	É opcional e em geral nenhuma plataforma de software e hardware oferece nativamente.
Isso significa em IPv6 todas as máquinas na rede trazem a implementação nativa do IPSec, o que permite que tais máquinas possam estabelecer canais seguros de comunicação com qualquer outra máquina na rede, vindo promover as defesas necessárias aos ataques clássicos possíveis no IPv4 tais como: <i>IP Spoofing, Sniffers, Replay, Eavesdropping</i> etc.		
Aspectos de Segurança	Protocolo IPv6	Protocolo IPv4
Integridade, autenticidade, confidencialidade e privacidade	Esses aspectos são garantidos à medida que todas as mensagens trocadas na rede são autenticadas com AH e cifradas com ESP.	Poucas são as soluções que implementam esses aspectos à medida que, não foi projetado para ser seguro, estando sujeito a uma série de ataques.
Isso significa que em IPv4 é claro as vulnerabilidades em termos de segurança das informações, ao passo que, em IPv6 essas falhas são corrigidas através dos dois mecanismos de segurança nativos.		

Figura 6 – Os Protocolos IPv4 e IPv6 na Segurança das Informações
Fonte: Adaptação de Dados Primários (2004)

4.4 Considerações sobre as Vantagens e Desvantagens da Migração para a Versão IPv6

Na tentativa de introduzir o IPv6 no mercado, várias vantagens são exploradas em relação a versão corrente (IPv4). Nesse sentido, conforme constatou-se, há muita polêmica envolvendo cada uma das vantagens da nova versão, à medida que, muitas soluções são implementadas usando o protocolo IPv4 original com outros protocolos, softwares e/ou hardwares adicionais.

Dessa forma, a implementação do IPv6 no mercado encontra resistência e, nesse sentido, a grande dificuldade reside no fato de que as operadoras de *backbone* não conseguem ver vantagem que justifique um *upgrade* imediato para o IPv6, em sua infra-estrutura atual de rede. Essa infra-estrutura deverá ser única e global para ser usada como base para autenticação de todas as máquinas na rede, independente de sua localização na rede. Nesse sentido, uma atualização de sistemas e redes envolveria custos altos.

Assim, devido a ausência de uma infra-estrutura única e global, apesar de IPv6 oferecer recursos para o desenvolvimento de um nível maior de segurança na Internet, tais recursos deverão ser usados adequadamente sob pena de IPv6 apresentar as mesmas vulnerabilidades da versão corrente. Em outras palavras, seria o mesmo que dizer que nas atuais condições, todos os benefícios oferecidos pelo IPv6 em termos de segurança não podem ser explorados na Internet.

Como a implementação do IPv6 é considerada inevitável, porém, deverá ocorrer de maneira gradual, de forma que, permitam-se um período de transição entre as duas versões coexistindo simultaneamente por algum tempo, até que se complete o período de transição.

Nesse sentido, apesar das dificuldades e restrições existentes é possível que nos próximos anos muitas dessas barreiras sejam transpostas, permitindo assim, que a Internet seja um local relativamente seguro, tanto para as comunicações empresariais quanto para o público popular.

5 CONCLUSÃO

Em linhas gerais, o IPv6 foi desenvolvido com o objetivo de substituir a versão corrente (IPv4), no que diz respeito tanto à melhoria do desempenho, na questão da segurança e no suprimento da escassez de endereços IP.

Contudo, mais especificamente, há de se considerar que a nova versão parte de conceitos de base da versão anterior, à medida que as características do IPv4 que foram consideradas eficazes e necessárias, foram mantidas, como também, adicionadas novas capacidades. Nesse sentido, pode-se considerar que o IPv6 é uma evolução da versão IPv4.

Com relação a questão de segurança, considera-se que o conjunto de protocolos que formam a arquitetura do IPsec e que faz parte nativamente do IPv6, se constitui como a verdadeira tecnologia do IP seguro que veio suprir a demanda da segurança no tráfego das informações. Contudo, seu emprego imediato não depende somente da utilização do IPsec, pois, toda a segurança oferecida pelo protocolo depende de uma infra-estrutura global onde todas as máquinas possam compartilhar.

Isso significa dizer, que existem barreiras de ordem que não são tecnológicas e que se refletem como restrições ao seu pleno emprego. Nesse sentido, embora o Ipv4 tenha suas limitações, deve-se considerar, que ele ainda está muito presente e forte no mercado representando o investimento de muitas empresas, à medida que soluções são incorporadas ao IPv4 original na tentativa de suprir suas limitações, promovendo-se assim, uma resistência à substituição para o IPv6.

Contudo, a implementação do IPv6 é considerada inevitável. Porém, deverá ocorrer de maneira gradual, de forma que, pressupõem-se um período de transição onde as duas versões coexistirão simultaneamente por algum tempo, até que se complete o período de transição.

Nesse sentido, apesar das dificuldades e restrições existentes é possível que nos próximos anos muitas dessas barreiras sejam transpostas, permitindo assim, que a Internet seja um local relativamente seguro, tanto para as comunicações empresariais quanto para a esfera popular.

BIBLIOGRAFIA

ANDRADE, Sara; OLIVEIRA, Ana Katarina P. de. **Manual para apresentação de trabalhos acadêmicos, projetos de pesquisa, relatórios finais e artigos**. 1. ed. rev. e ampl. ____ Natal: FARN, 2003.

COMER, Douglas E. **Interligação em rede com TCP/IP: princípios, protocolos e arquitetura**. Vol 1. Rio de Janeiro: 1998.

_____. **Redes de computadores e Internet: abrange transmissão de dados, ligação inter-redes e web**. 2. ed. Porto Alegre: Bookman, 2001.

HISATUGU, Wiliam Hiroshi. **IPv6 (Internet Protocol version 6) IP Móvel: princípios fundamentais (03)**. Disponível em: <http://www.wirelessbrasil.org/wirelessbr/colaboradores/hisatugu/ipv6_03.html>. Acesso em: 05.mai.2004.

LIMA, Marcelo Barbosa. **Considerações sobre segurança em IPv6**. CISSP: Fevereiro de 2004. disponível em: <http://www.kcmelo.com/files/IPv6_seg.pdf>. Acesso em: 05.out.2004.

MATERIAL SOBRE IPV6 E ATM. Disponível em: <http://www.w2k.com.br/images/SID/IPV6_ATM/ipv6atm.ht>. Acesso em: 05.out.2004.

SILVA, Carlos Eduardo *et al.* **IPv6 – Protocolo Internet versão 6**. Artigo publicado pela Gerência de Informática do Centro Federal de Educação Tecnológica –RN. Natal: CEFET, 2004.

SILVA, Adailton J. S.; TEIXEIRA, Renata Cicilini. **Arquitetura IP Security – Parte 1**. NewsGeneration - Boletim bimestral sobre tecnologia de redes produzido e publicado pela RNP – Rede Nacional de Ensino e Pesquisa. ISSN 1518-597. Disponível em: <<http://www.rnp.br/newsgen/9907/ipsec3.html>>. Acesso em: 05.out.2004.

SOUSA JR, Rafael T. de; PUTTINI, Ricardo S. **Principais aspectos na segurança de redes de computadores: IPSEC – Internet Protocol Security**. UnB – Departamento de Engenharia Elétrica – Mestrado em Engenharia de Redes e Tecnologia da Informação. Disponível em: <<http://www.labredes.unb.br/security/firewall/ipsec.html>>. Acesso em 09.mai.2004.

OLIVEIRA, Robson. **IPv6 do Brasil – o que é IPv6: introdução ao IPv6**. Disponível em: <<file:///C:/Documents%20and%20Settings/p2837/Desktop/MSN%20Hotmail%20-%20...>> Acesso em: 16.mar.2004.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. **Protocolo IPv6: Segurança**. Disponível em: <http://www.gta.ufjf.br/grad/99_2/eric/seguranca.htm>. Acesso em: 16.mar.2004.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 3. ed. São Paulo: Atlas, 2000.