UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

HENRIQUE GONÇALVES BEIRA

MÉTODO E ANÁLISE DE DESEMPENHO E SEGURANÇA DE UMA REDE IPV6 UTILIZANDO IPSEC EM MODO TÚNEL

MONOGRAFIA

CURITIBA

2014

HENRIQUE GONÇALVES BEIRA

MÉTODO E ANÁLISE DE DESEMPENHO E SEGURANÇA DE UMA REDE IPV6 UTILIZANDO IPSEC EM MODO TÚNEL

Monografia apresentada à Unidade Curricular de Trabalho de Conclusão de Curso do CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO da UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ como requisito parcial de aprovação.

Orientador: Prof Me. Fabiano Scriptore de Carvalho

CURITIBA

2014

AGRADECIMENTOS

Registra-se aqui a manifestação de reconhecimento do autor deste presente trabalho de conclusão de curso para com as pessoas que contribuiriam, em algum momento, para o progresso do mesmo.

Reverências ao orientador deste trabalho, o Professor Mestre Fabiano Scriptore de Carvalho, com as suas valiosas contribuições ao trabalho feito.

Agradecimentos à Professora Doutora Mariângela de Oliveira Gomes Setti, que esteve a frente da disciplina de Trabalho de Conclusão de Curso 1, e à Professora Doutora Marília Abrahão Amaral, na disciplina de Trabalho de Conclusão de Curso 2, com as suas respectivas orientações na busca do êxito deste trabalho.

Por fim, gratidão à Professora Doutora Anelise Munaretto Fonseca e ao Professor Mestre Luiz Augusto Pelisson, por aceitarem comporem a banca de professores avaliadores deste presente trabalho.

RESUMO

BEIRA, Henrique Gonçalves. Método e Análise de Desempenho e Segurança de uma Rede IPv6 utilizando IPsec em Modo Túnel. 47 f. Monografia – CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO, UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ. Curitiba, 2014.

Este trabalho teve como tema o Internet Protocol version 6 (IPv6), mais especificamente sobre a utilização do modo túnel do Internet Protocol Security (IPsec) para IPV6, implantando em uma rede de computadores. O foco deste projeto foi a avaliação, assim como o método, de desempenho e segurança desta rede. O projeto visou a criação de uma topologia com duas redes locais, uma chamada de matriz e outra de filial, que usam o modo túnel do IPsec para se comunicarem. A utilização do IPsec em modo túnel forma uma conexão privada, entre os dois roteadores de borda que estão em cada lado desta comunicação. O problema constituiu em, a partir de uma rede completamente IPv6, avaliar o desempenho e a segurança desta rede, pois, para garantir as características de autenticidade e integridade do pacote de rede, assim como a confidencialidade dos dados, é necessário utilizar cabeçalhos específicos do IPsec. Os cabeçalhos analisados neste trabalho foram: o Autentication Header (AH), e o cabeçalho Encapsulating Security Payload (ESP). Os resultados apresentaram que o IPsec, com os cabeçalhos AH e ESP, são recomendados de serem utilizados, devido a diferença de desempenho em comparação ao não uso do IPsec ficar estabilizada em 7% (com 7 roteadores) e 9% (com 3 roteadores), segundo os experimentos realizados.

Palavras-chave: IPv6, modo túnel, IPsec

Áreas de Conhecimento: Protocolos de rede, Roteadores, Análise de desempenho de rede, Protocolos de segurança

ABSTRACT

BEIRA, Henrique Gonçalves. Method and Analysis of Security and Performance of a Network using IPv6 in IPsec Tunnel Mode. 47 f. Monografia – CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO, UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ. Curitiba, 2014.

This work has the focus on the Internet Protocol version 6 (IPv6), specifically on the use of tunnel mode in Internet Protocol Security (IPsec) for IPv6 , deploying a network of computers. The focus of this project was the evaluation, as well as the method, of performance and security of the network. The project aimed to create a topology with two local networks, one called as matriz and another as filial, using IPsec tunnel mode to communicate. The use of IPsec in tunnel mode forms a private connection between the two border routers that are on each side of this communication. The problem is, from a completely IPv6 network, evaluating the performance and security of the network, thus to ensure the authenticity and integrity characteristics of network packet, as well as data confidentiality, it is necessary to use specific headers of IPsec. Headers analyzed in this work were: Autentication Header (AH) and Encapsulating Security Payload Header (ESP). The results showed that the IPsec with AH and ESP headers are recommended to be used because the performance difference compared to not using IPsec get stabilized on 7 % (with 7 routers) and 9% (with 3 routers), according to the experiments.

Keywords: IPv6, tunnel mode, IPsec

Knowledge Areas: Network protocols, Routers, Network performance analysis, Security protocols

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Este trabalho teve como tema o *Internet Protocol version 6* (IPv6), mais especificamente sobre a utilização do modo túnel do *Internet Protocol Security* (IPsec) para IPv6, implantado em uma rede de computadores. O foco deste trabalho foi a avaliação, assim como o método, de desempenho e segurança desta rede.

O trabalho visou a criação de uma topologia com duas redes locais, uma chamada de matriz e outra de filial, que usam o modo túnel do IPsec para se comunicarem. A utilização do IPsec em modo túnel forma uma conexão privada, entre os dois roteadores de borda que estão em cada lado desta comunicação. Por padrão, todos os roteadores que suportam o protocolo IPv6 devem suportar também o IPsec, pois no *Internet Protocol version 4* (IPv4) é opcional este suporte (SILVA, 2006).

1.1 PROBLEMA

O problema constituiu em, a partir de uma rede completamente IPv6, avaliar o desempenho e a segurança desta rede, pois para garantir as características de autenticidade do pacote, assim como a confidencialidade dos dados, é necessário utilizar cabeçalhos específicos do IPsec. Os cabeçalhos analisados neste trabalho foram: o *Autentication Header* (AH), e o cabeçalho *Encapsulating Security Payload* (ESP).

O AH se refere à autenticação e garantia da integridade dos pacotes IP. Já o ESP se refere à criptografia dos dados dos pacotes IP. A utilização destes cabeçalhos poderia causar uma perda de desempenho em uma conexão, pois os pacotes IP iriam ter um tamanho maior do que os pacotes que não utilizariam tais cabeçalhos.

Sobre a segurança, o estudo indicou problemas que podem ocorrer caso não houverem a utilização dos cabeçalhos de segurança apresentados no parágrafo anterior. Por exemplo, como um pacote IP que não tem a sua parte de dados criptografada pelo ESP pode ser interceptada e lida.

A demanda deste trabalho veio da falta de experimentos com redes completamente IPv6, utilizando equipamentos como roteadores. A Figura 1 apresenta a simplificação da topologia que foi montada para efetuar os testes de desempenho e de segurança.

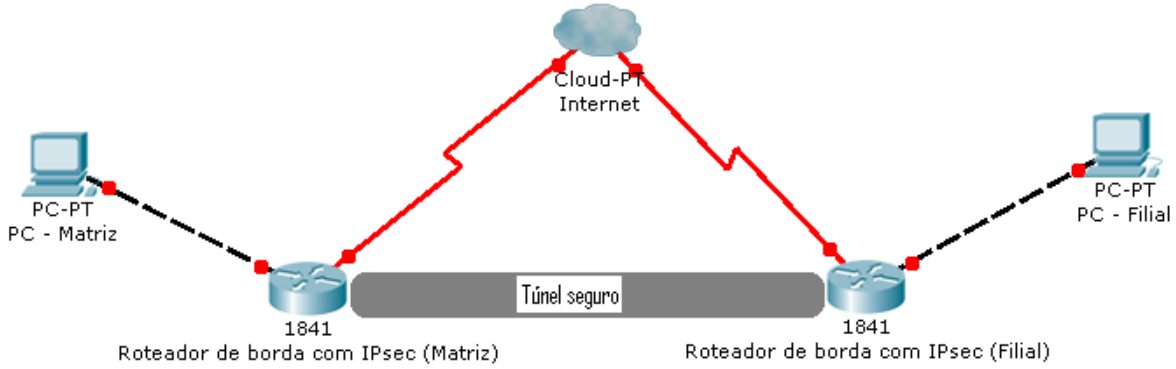

Figura 1: Topologia com 2 roteadores de borda em modo túnel

Fonte: Autoria Própria

1.2 JUSTIFICATIVA

O protocolo IPv6 precisa ser testado no que concerne a sua implantação em casos específicos, como a deste presente trabalho, que é o uso deste protocolo entre dois roteadores de borda[1], analisando os impactos de desempenho e segurança. As instituições de pesquisa, como as universidades, podem colaborar na análise dos impactos da implantação de novas tecnologias.

É importante a utilização do protocolo IPv6 nas redes públicas/privadas, devido ao esgotamento dos endereços do IPv4 (BASSO, 2011), assunto que é tratado mais adiante neste presente trabalho. A implantação de uma rede que faça o uso do IPsec para IPv6, em modo túnel, deve ser avaliada, para que se indique o seu uso efetivo em redes de computadores.

1.3 MOTIVAÇÃO

Ao realizar uma pesquisa inicial sobre o tema, não foram encontrados trabalhos que abordassem a implantação de topologias 100% em IPv6. Considerando que o IPv6 é um protocolo

[1]Roteadores da extremidade de uma rede local.

que substituirá o IPv4, estudos sobre ele são essenciais para a realização de experimentos que podem atestar ou não a viabilidade do uso efetivo do mesmo em redes de computadores.

1.4 OBJETO DE TRABALHO

O objeto de trabalho foi o protocolo IPv6, mais precisamente o IPsec para IPv6, utilizando o modo túnel.

1.5 OBJETIVOS

A seguir é descrito o objetivo geral deste trabalho e as suas partes específicas.

1.5.1 Objetivo geral

Avaliar o desempenho e a segurança de uma rede completamente IPv6, mais especificamente uma rede que utiliza o modo túnel do IPsec.

1.5.2 Objetivos específicos

- Estudar o estado da arte do protocolo IPv6;
- Estudar o estado da arte do protocolo IPsec;
- Explorar o uso do IPsec no IPv6, no que concerne aos cabeçalhos que garantem a integridade e criptografia dos pacotes IPv6, AH e ESP respectivamente;
- Prospectar equipamentos de rede, assim como ferramentas que permitem a simulação de redes;
- Estruturar uma rede completamente IPv6, constituída de duas redes locais, que estarão ligadas através do modo túnel do IPsec;
- Utilizar esta rede para realizar os testes de desempenho e segurança dos pacotes IPv6;
- Verificar a viabilidade da utilização dos cabeçalhos AH e ESP;
- Fornecer a metodologia adotada para a realização dos experimentos.

1.6 ESTRUTURA DO TRABALHO

No capítulo de introdução, foram descritos: o problema que a pesquisa abordou, a justificativa e a motivação deste trabalho ser feito, o objeto que foi estudado e, por fim, os objetivos.

Já no capítulo 2, são apresentados o protocolo IPv6 e o IPsec para esta versão, assim como uma análise de trabalhos correlatos a este, mais especificamente os que tiveram como objeto de trabalho o IPsec.

No capítulo 3, sobre a metodologia adotada, são mostrados os passos de como foi o desenvolvimento deste presente trabalho para a obtenção dos seus resultados. São apresentados os fundamentos e as tecnologias a serem empregadas. Há uma seção final que apresenta os resultados dos experimentos realizados.

Por fim, no capítulo de conclusões, é exposto as considerações finais deste presente trabalho, e também a indicação de trabalhos futuros que poderão ser realizados para dar continuidade ao mesmo.

2 REVISÃO BIBLIOGRÁFICA

Neste capítulo, antes de ser feita uma análise sobre os trabalhos que envolveram o uso do IPsec, são apresentados os conceitos para o entendimento dos assuntos que são vistos neste trabalho, como, por exemplo, o por quê do IPv6 ser desenvolvido, assim como quais são as suas características que o diferem do IPv4. Também são descritos os detalhes a respeito do IPsec, e o seu uso no IPv6.

2.1 REFERENCIAL TEÓRICO

Uma rede de computadores é formada por dois ou mais computadores interligados, por meio físico, e que usam regras definidas para se comunicarem. Estas regras funcionam como uma linguagem, e são chamadas de protocolo (ALMEIDA; INES, 2009).

A comunicação entre computadores em uma rede é feita através de uma pilha de protocolos. A pilha *Transmission Control Protocol/Internet Protocol* (TCP/IP) é a mais utilizada atualmente (BASSO, 2011). A Tabela 1 apresenta as camadas desta pilha, assim como alguns protocolos de cada uma delas.

Tabela 1: Pilha de protocolos TCP/IP

Camada	Protocolos
4. Aplicação	HTTP, SMTP, FTP, SSH, Telnet, POP3, BitTorrent, DNS
3. Transporte	TCP, UDP
2. Internet	IP (IPv4, IPv6), ARP, RARP, ICMP, IPsec
1. Acesso à rede	Ethernet, WiFi, HDLC, Token Ring, Frame Relay, PPP

Fonte: Autoria Própria

Para ocorrer a comunicação entre diversas redes de computadores, é necessário a utilização do Protocolo Internet, ou *Internet Protocol* (IP), localizada na camada Internet da pilha TCP/IP. A *Internet* constitui a chamada rede mundial de computadores, possibilitando que pessoas e organizações tenham uma nova forma de comunicação e acesso à informação (GODINHO, 2012).

O protocolo IP é utilizado na *Internet*, e define a regra que cada dispositivo conectado deve possuir um número único de identificação, que chama-se número IP, ou endereço IP.

A distribuição de números IP é controlada, de forma hierárquica, por diversas entidades, como a *Internet Assigned Numbers Authority* (IANA), que distribui faixas de números IP, por meio da *Internet Corporation for Assigned Names and Numbers* (ICANN), para as chamadas *Regional Internet Registry* (RIR).

Há um total de cinco RIRs: A **AfriNIC**, responsável pela África, a **ARIN**, responsável pelos EUA e o Canada, a **APNIC**, responsável pela Austrália, Ásia, Nova Zelândia e países vizinhos, **LACNIC**, responsável pela América Latina e Caribe, e a **RIPE NCC**, responsável pela Europa e todo o restante do mundo. A Figura 2 apresenta em forma gráfica a distribuição das RIR pelo planeta.

Figura 2: Abrangência das Regional Internet Registry (RIR)
Fonte: http://pleco-kingdom.jp/geekpage-cache/img/2011/02-ipv4/rir.png

Alguns países possuem um *National Internet Registry* (NIR), que faz a distribuição nacional de endereços IP. No Brasil, o Núcleo de Informação e Coordenação do Ponto BR[1] é quem cum-

[1] http://www.nic.br

pre esta função. Por fim, os Provedores de Internet são considerados *Local Internet Registries* (LIR), e distribuem endereços IP aos usuários finais.

2.1.1 O IPv4

A Internet não foi planejada para ser utilizada comercialmente, pois foi idealizada por centros de pesquisa, que eram ligados ao Departamento Estadunidense de Defesa. Em 1983, nesta rede haviam cerca de 300 computadores, mas em 1993 foi aberta comercialmente, e o crescimento foi tão grande que os endereços IP acabariam em 2 ou 3 anos (ALMEIDA; INES, 2009).

O IPv4 era, e ainda é, a versão do Protocolo Internet com maior uso, e seu endereço é composto por uma sequência binária de 32 bits, ou 4 octetos, resultando em cerca de 4 bilhões de endereços possíveis. Inicialmente, os endereços possíveis com 32 bits foram divididos em classes A, B e C, apresentadas na Tabela 2. A **classe A** podia atender 128 redes, com a possibilidade de ter aproximadamente 16 milhões de *hosts* em cada uma destas redes. Já a **classe B** podia endereçar 16 mil redes, com cerca de 65 mil endereços de *host* cada uma. Por fim, a **classe C** endereçaria 2 milhões de redes, com 254 *hosts* cada uma.

Tabela 2: Estrutura de três classes IP criadas no IPv4

Classe	Endereço IP	Identificação da Rede	Identificação do Host
A	w.x.y.z	w.	x.y.z
B	w.x.y.z	w.x.	y.z
C	w.x.y.z	w.x.y.	z

Fonte: Autoria Própria

O problema da política de classes é que a classe A ocupava metade de todos os endereços disponíveis, e isso era um grande desperdício (RODRIGUES, 2009). Se uma empresa precisasse endereçar, por exemplo, 300 dispositivos em uma rede, precisaria de um bloco de endereços classe B, desperdiçando assim cerca de 65 mil endereços.

Com isso, um novo protocolo passou a ser desenvolvido, de nome *Internet Protocol next generation* (IPng), e medidas paliativas foram tomadas até o término de seu desenvolvimento, como a criação da *Classless Inter-Domain Routing* (**CIDR**), especificada pela RFC 1518 (REKHTER; LI, 1993), que eliminava o sistema de classes dita anteriormente, pois causava problemas de desperdício de endereços já citados. A CIDR permitiu alocar blocos de endereços de tamanhos variados, adequando-os de acordo com a quantidade de *hosts* desejados. A Tabela 3

apresenta as máscaras de sub-redes[2] que são criadas quando um antigo bloco da classe C é dividido em blocos menores.

Tabela 3: Sub-redes criadas com um antigo bloco da classe C

Notação CIDR	Máscara	Nº de Redes	Nº de Hosts
/24	255.255.255.0	1	254
/25	255.255.255.128	2	126
/26	255.255.255.192	4	62
/27	255.255.255.224	8	30
/28	255.255.255.240	16	14
/29	255.255.255.248	32	6
/30	255.255.255.252	64	2

Fonte: Autoria Própria

Outras medidas para evitar o término dos endereços IP incluem: **RFC 1918** (REKHTER et al., 1996), que define 3 faixas de endereços privados para uso em redes locais, apresentado na Tabela 4; *Network Address Translation* (**NAT**), RFC nº 2663 (SRISURESH; HOLDREGE, 1999), onde toda uma rede local, que utiliza endereços privados, poderia se comunicar na Internet com um endereço válido; e o *Dynamic Host Configuration Protocol* (**DHCP**), RFC nº 1531 (DROMS, 1993), que dinamicamente alocaria e desalocaria endereços IP para uso nos computadores.

Tabela 4: As 3 faixas de endereços privados do IPv4

Classe	Faixa de endereços IP	Prefixo
A	10.0.0.0 - 10.255.255.255	/8
B	172.16.0.0 - 172.31.255.255	/12
C	192.168.0.0 - 192.168.255.255	/16

Fonte: Autoria Própria

O NAT, embora seja uma técnica amplamente utilizada no IPv4 (SANTOS, 2004), apresenta problemas como:

[2] A máscara de sub-rede é um endereço de 32 bits que distingue a identificação da rede com a do host.

- Quebra do modelo de comunicação fim-a-fim[3] da Internet;
- Requer equipamentos com poder de processamento suficiente para gerenciar as tabelas de conexões NAT;
- Falsa sensação de segurança, devido à este isolamento dos endereços privados com os válidos (públicos);
- Impossibilita algumas técnicas de segurança do IPsec.

O NAT é o mapeamento de 1 endereço válido para 1 endereço privado, já o *Port Address Translation* (PAT) é 1 endereço válido para vários endereços privados, variando a porta de acesso. A Figura 3 apresenta uma representação do PAT.

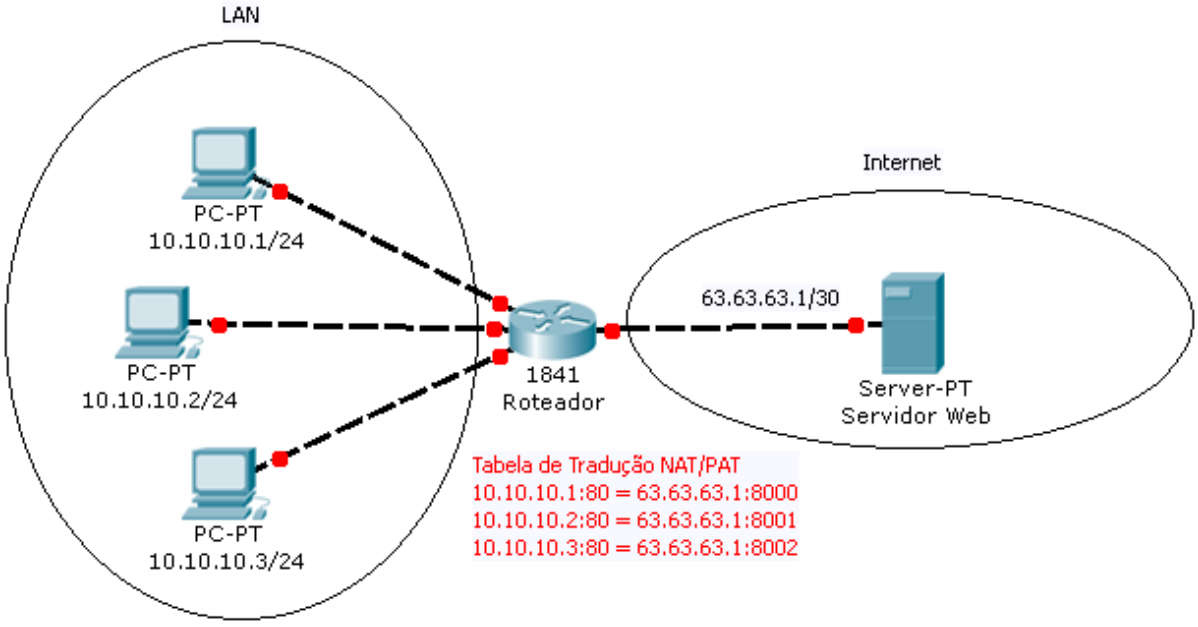

Figura 3: Roteador utilizando o PAT

Fonte: Autoria Própria

Porém, ainda havia a necessidade de uma solução definitiva para a escassez de endereços IP, e que permitisse o crescimento do número de dispositivos na Internet. O IPv6 é a solução definitiva (ALMEIDA; INES, 2009).

Por fim, a respeito de uma versão 5 do *Internet Protocol*, e que seria o IPv5, houve a utilização do número 5 dos protocolos que atuam na camada Internet para designar um protocolo que seria para uso específico no envio de voz e vídeo, chamado de *Internet Stream Protocol*

[3]Este modelo caracteriza o uso de endereços válidos para a comunicação, através da Internet, entre dispositivos.

(ST), e seria empregado para este fim como alternativa ao IP. O protocolo ST é definido como um protocolo experimental (DELGROSSI; BERGER, 1995).

2.1.2 O IPv6

O protocolo IPv6, RFC nº 2460 (DEERING; HINDEN, 1998), foi desenvolvido ao longo de 10 anos, desde 1990, quando foram feitas as medidas paliativas para evitar o esgotamento de endereços IP. Esta nova versão também foi desenvolvida para solucionar problemas que haviam na versão anterior, como a falta de segurança do protocolo de comunicação IPv4 (SILVA, 2006).

A principal diferença entre os protocolos IPv4 e o IPv6 é que a quantidade de bits para o endereçamento que subiu de 32 bits para 128 bits. Porém, a metade destes bits são utilizadas para o endereçamento local, ou seja, para a identificação da rede. A Figura 4 ilustra a divisão dos bits de rede e dos bits de *host*[4]. Devido a grande quantidade de endereços proporcionados pelo IPv6, todos os dispositivos que são conectados à Internet podem ter endereços válidos nela.

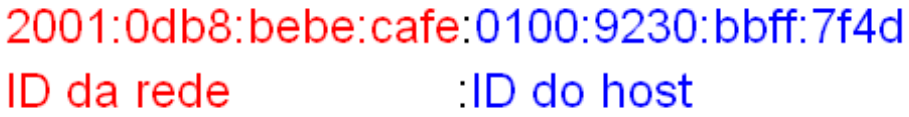

Figura 4: Divisão dos bits de endereçamento do IPv6
Fonte: Autoria Própria

O cabeçalho do pacote IPv6 base possui 8 campos, que somados resultam em 40 Bytes. Informações adicionais, caso sejam necessárias, são enviadas por cabeçalhos de extensão, que não possuem um tamanho ou quantidade fixas. Os itens a seguir apresentam os campos do cabeçalho base do IPv6:

- Versão (*Version*): indica a versão do protocolo utilizado, que no caso do IPv6 é 6[5], e tem o tamanho de 4 bits;
- Classe de Tráfego (*Traffic Class*): caso necessário, identifica a classe ou prioridade do pacote. Tamanho de 8 bits;
- Identificador de Fluxo (*Flow Label*): 20 bits para um tratamento específico dos pacotes, caso necessário;

[4] Qualquer equipamento que está em uma rede.
[5] Assim como no IPv4 é 4.

- Tamanho dos Dados (*Payload Length*): 16 bits para identificar, em bytes, o tamanho dos dados transportados, incluindo os cabeçalhos de extensão, caso utilizados;
- Próximo Cabeçalho (*Next Header*): Identifica o próximo cabeçalho que segue o atual. Tem 8 bits de tamanho;
- Limite de Encaminhamento (*Hop Limit*): 8 bits para indicar o número máximo de roteadores que o pacote pode percorrer, antes de ser descartado;
- Endereço de Origem (*Source Address*): 128 bits que indicam a origem do pacote;
- Endereço de Destino (*Destination Address*): 128 bits que indicam o destino do pacote.

Os cabeçalhos de extensão, caso utilizados, não necessitam ser processados pelos roteadores intermediários, somente pelo nó de destino, tornando o processamento mais rápido. Novos cabeçalhos de extensão podem ser criados, caso sejam precisos, pois não modificam a estrutura base do pacote IPv6. Já foram definidos 6 cabeçalhos de extensão para o IPv6, que são:

- *Hop-by-Hop Options Header*: informações especiais de descarte. Único cabeçalho que possui a exceção, se for usado, de ser lido por roteadores intermediários;
- *Routing Header*: utilizado no mecanismo de mobilidade do IPv6;
- *Fragmentation Header*: configurações especiais para a unidade máxima de transmissão de dados, ou MTU;
- *Authentication Header*: informações sobre autenticação e integridade do pacote;
- *Encapsulating Security Payload Header*: informações sobre a criptografia dos dados de um pacote;
- *Destination Options Header*: utilizado no mecanismo de mobilidade do IPv6.

A Figura 5 apresenta, em forma gráfica, como é um pacote IPv6 com o seu cabeçalho base, com as suas extensões, e demais partes que o compõem.

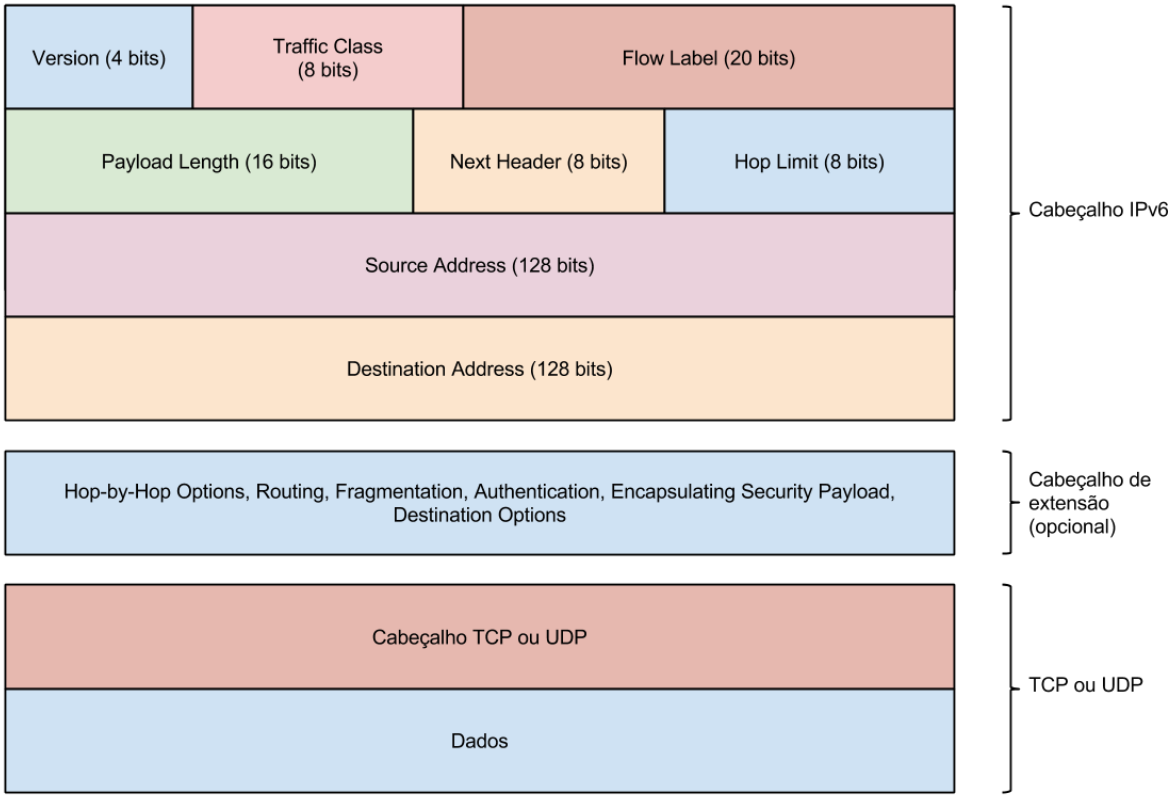

Figura 5: Estrutura de um pacote IPv6

Fonte: Autoria Própria

O IPv6 não é somente uma atualização de versão, mas sim um protocolo novo, com novas características e funcionalidades (FALCONI, 2004). Uma característica diferente entre os dois protocolos é que, no IPv4, os roteadores realizam o serviço de fragmentação de pacotes e, no IPv6, somente os nós de origem fragmentam (SANTOS, 2004). As questões de segurança também foram revisadas, como a exigência dos equipamentos que suportam IPv6 também terem de suportar o IPsec (RADWAN, 2006).

2.1.3 O IPsec

Definida pela RFC nº 4301 (KENT; SEO, 2005), o IPsec fornece um conjunto de serviços de segurança para o protocolo IP, como autenticidade da origem dos dados, integridade dos dados, e privacidade através de criptografia. Uma rede privada virtual pode utilizar o IPsec para a transmissão de dados e comunicação através da Internet (ADEYINKA, 2008).

O IPsec foi desenvolvido originalmente para o IPv4, porém a utilização de NAT impede o seu uso, pois prejudica a identificação fim-a-fim. Com o IPv6, o uso de NAT não é mais

necessário, assim o IPsec pode ser utilizado sem restrições. O funcionamento do IPsec é praticamente igual nas duas versões de IP, mas os equipamentos com suporte ao IPv4 não eram obrigados a suportar o IPsec, já os que suportam IPv6 devem suportar o IPsec (SILVA, 2006).

Para o efetivo uso do IPsec no IPv6, os administradores de rede devem habilitar e configurar o IPsec em cada nó da rede onde sua utilização é desejada. O IPsec não é um único protocolo, mas um conjunto de funções independentes, que fazem uso dos cabeçalhos de extensão do IPv6, como o cabeçalho *Autentication Header* (AH), e o cabeçalho *Encapsulating Security Payload* (ESP). Também faz uso do protocolo *Internet Key Exchange* (IKE).

O AH tem como objetivo garantir a autenticação e a integridade dos pacotes IP. Já o ESP é utilizado para garantir a confidencialidade dos dados nos pacotes IP. Por fim, o protocolo IKE diz respeito às chaves de segurança que são geradas e gerenciadas pelo IPsec. O IKE é o protocolo padrão utilizado pelo IPsec para a associação segura de chaves (HIRATA; JÚNIOR; SOUZA, 2008).

O IPsec pode operar em dois modos: Modo Transporte e Modo Túnel. O Modo Transporte é o uso do IPsec entre dois *hosts*, ou seja, é necessário que os dois hosts que estão se comunicando tenham suporte ao IPsec. Já o Modo Túnel é caracterizado pela comunicação entre dois roteadores de borda, assim, ambos os roteadores devem ter suporte ao IPsec.

Outro detalhe sobre os dois modos de operação do IPsec é que, no Modo Transporte, o cabeçalho IP original fica exposto, pois se trata de uma comunicação direta entre dois *hosts*. Toda autenticação e criptografia são realizadas apenas na parte de dados (FAGUNDES, 2007). Já no Modo Túnel, todo o pacote IP original é encapsulado dentro de um outro pacote IP, que é criado pelo roteador, assim os *hosts* não precisam ter o IPsec configurado. A Figura 6 apresenta como ficam os pacotes IP após este tratamento do IPsec.

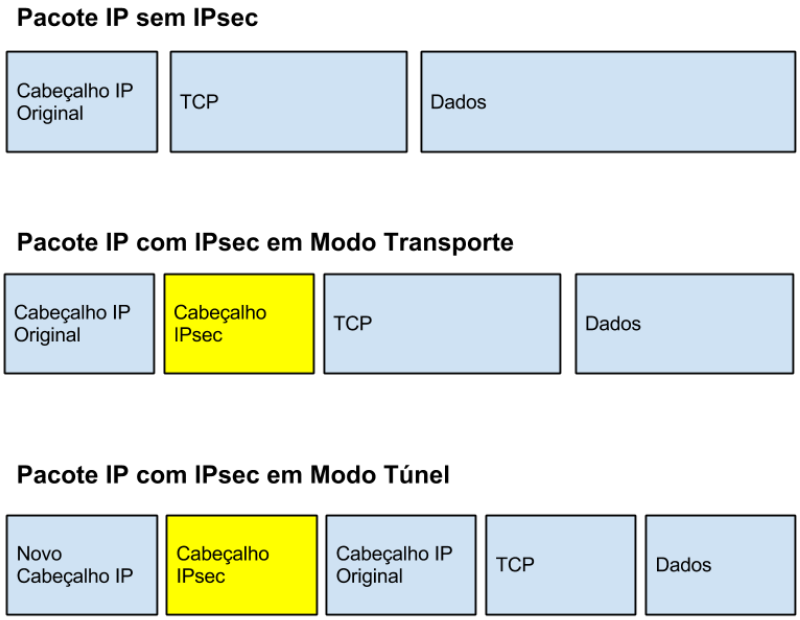

Figura 6: Modos Transporte e Túnel no IPsec

Fonte: Autoria Própria

Resumidamente, o IPsec promove os seguintes serviços: autenticação, integridade, confidencialidade, proteção contra *replay*[6] e controle de acesso. O estabelecimento de uma conexão IPSec deve seguir uma série de regras que compõem uma política de segurança envolvendo as duas pontas da conexão (CASTRO, 2004).

2.1.4 Ferramentas para a experimentação de topologias virtuais

Para a realização de testes com diferentes topologias de redes, é necessário o uso de diversos tipos de equipamentos de redes. O custo de adquirir estes equipamentos e o espaço físico necessário podem impossibilitar a realização de experimentos de redes. Logo, há disponíveis certos tipos de *softwares* que permitem a construção de redes simuladas em computadores.

Dentre os *softwares* para simulação de redes temos: GNS3[7], Cisco Packet Tracer[8], NetLAB[9], NetSimK[10], Netkit[11], ns-2[12] e o Common Open Research Emulator (CORE)[13].

[6] Pacotes são capturados e enviados posteriormente, sob forma de um ataque.
[7] http://www.gns3.net/
[8] https://www.netacad.com/pt/web/about-us/cisco-packet-tracer
[9] http://netlab.sourceforge.net/
[10] http://netsimk.com/
[11] http://wiki.netkit.org/index.php/Main_Page
[12] http://nsnam.isi.edu/nsnam/index.php/Main_Page
[13] http://cs.itd.nrl.navy.mil/work/core/

O *Graphical Network Simulator* 3 (GNS3) é um *software* de código aberto para a criação de redes, utilizando uma interface gráfica. Ou seja, permite que um computador seja utilizado para a configuração de redes virtuais sem ter os *hardwares* específicos para tal, como roteadores e comutadores. A Figura 7 apresenta o GNS3 em funcionamento.

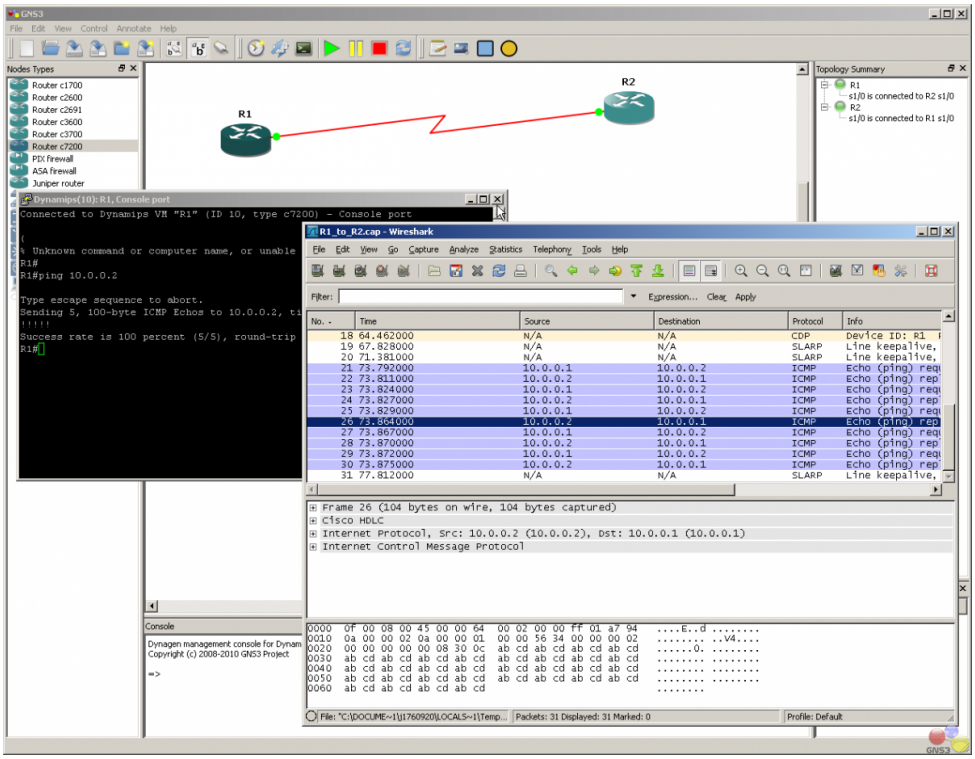

Figura 7: *Graphical Network Simulator* 3

Fonte: http://www.gns3.net/screenshots/

Já o Cisco Packet Tracer é um *software* de simulação de redes com equipamentos Cisco, utilizado por estudantes das certificações Cisco como apoio aos seus estudos além dos equipamentos físicos. A Figura 8 apresenta o Packet Tracer em operação.

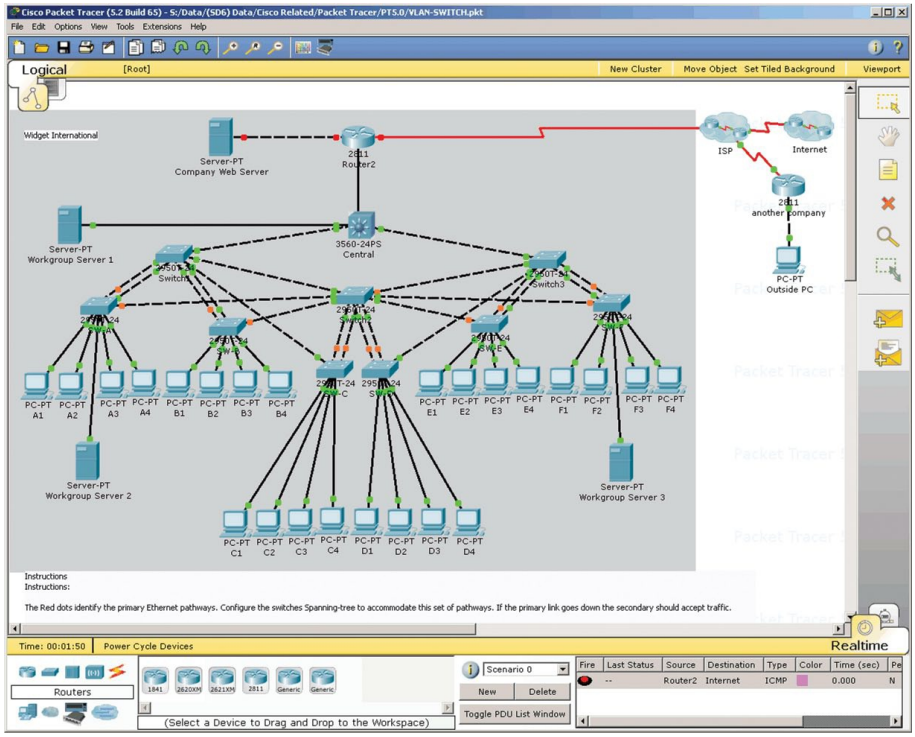

Figura 8: Cisco Packet Tracer

Fonte: https://www.netacad.com/pt/web/about-us/cisco-packet-tracer

A ferramenta NetLAB é um *software* livre que fornece o monitoramento, o diagnóstico, e explica o comportamento que ocorre em uma rede. A Figura 9 apresenta a interface do NetLAB.

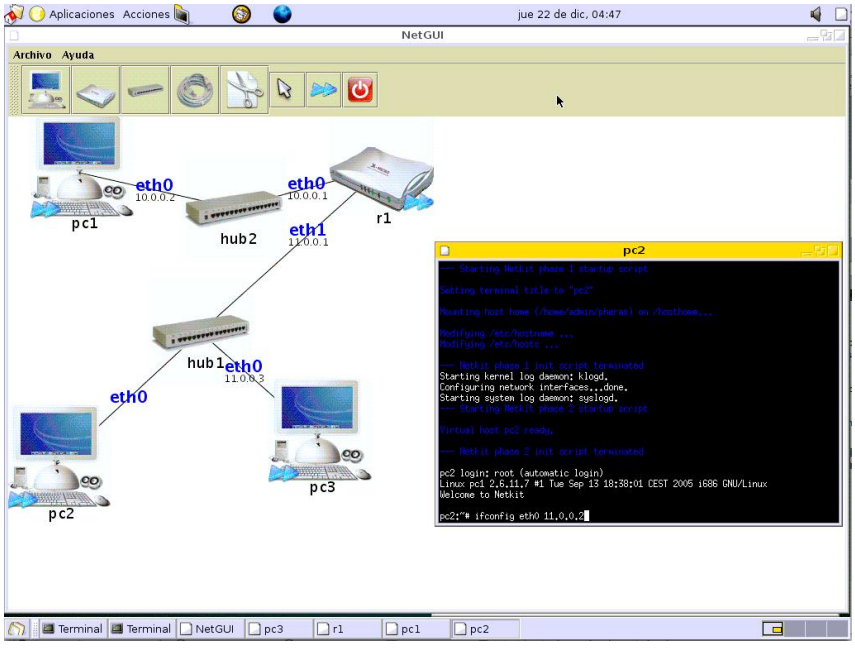

Figura 9: NetLAB

Fonte: http://netlab.sourceforge.net/

O NetSimK é uma ferramenta gratuita que foi desenvolvida por um instrutor Cisco para o ensino de configurações para roteadores Cisco. Há vários cenários disponíveis para os estudantes das certificações Cisco praticarem. A Figura 10 exibe a interface do NetSimK.

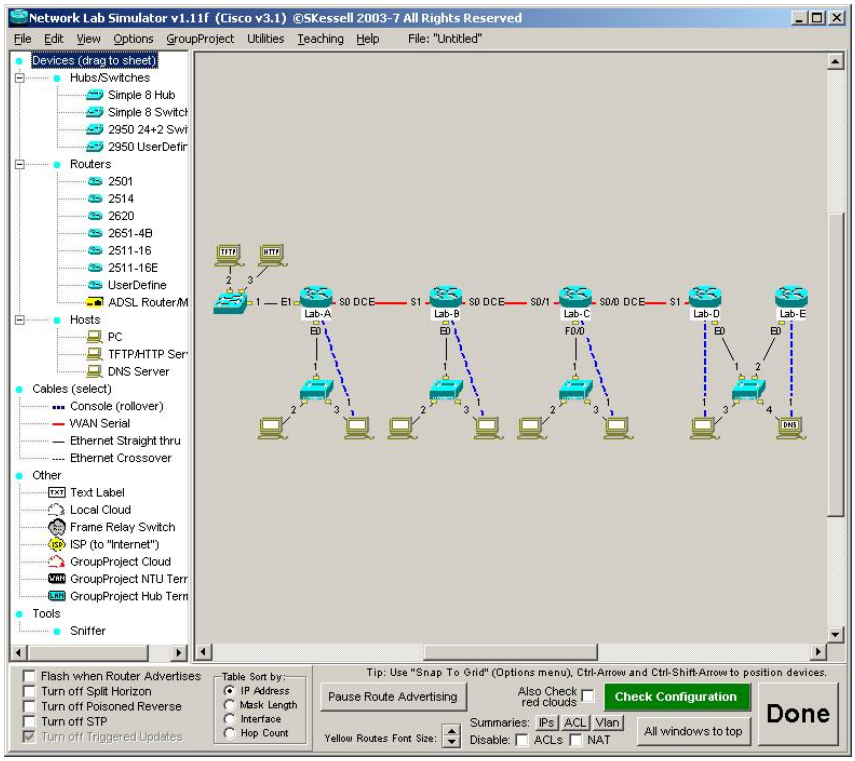

Figura 10: NetSimK

Fonte: http://netsimk.com/Screenshots.htm

Já o Netkit foi desenvolvido para permitir a realização experimentos com redes em um simples computador, ou seja, com baixo custo em relação a compra e o uso de equipamentos de redes físicos. Embora os arquivos de configuração dos equipamentos virtuais sejam idênticas aos dos equipamentos físicos, não são utilizados os sistemas operacionais verdadeiros. A Figura 11 exibe a realização de um *ping* no Netkit.

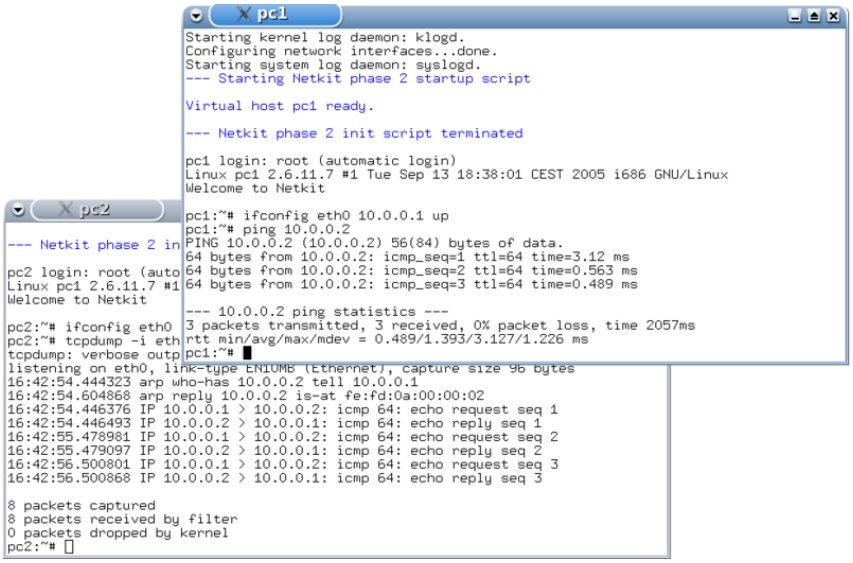

Figura 11: Netkit

Fonte: http://wiki.netkit.org/index.php/Screenshots

A ferramenta Network Simulator 2 (ns-2) é utilizado para os interessados em realizar testes com protocolos de redes. Possui uma interface gráfica que permite a visualização dos pacotes em funcionamento. A Figura 12 exibe a realização de um experimento no ns-2.

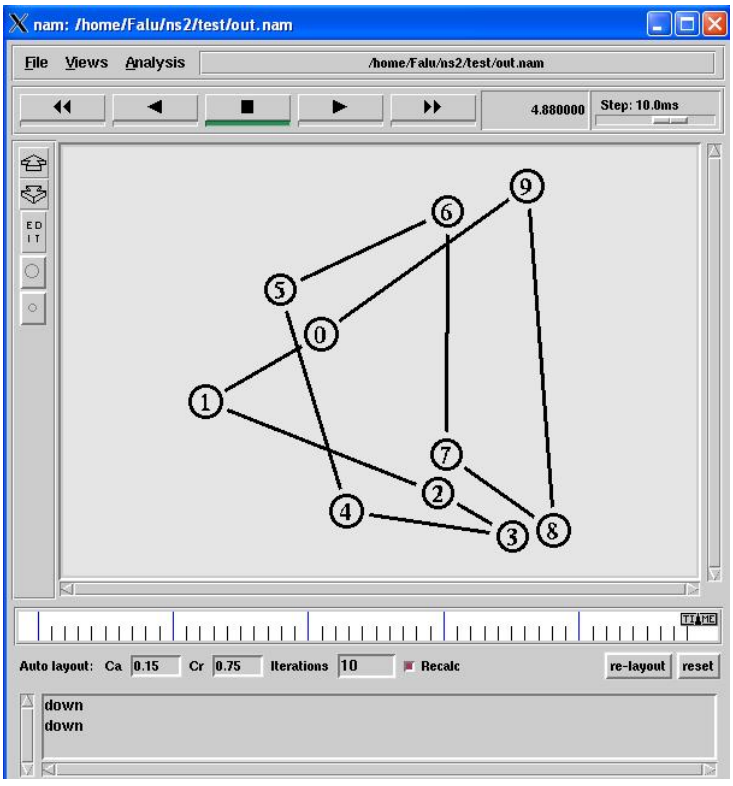

Figura 12: Network Simulator 2

Fonte: http://www.cs.sjsu.edu/ flashworm/updates.htm

O Common Open Research Emulator (CORE) é uma ferramenta utilizada para a construção de redes interconectáveis. Possui a vantagem de construir redes rapidamente, pois a realização da configuração dos endereços IP para cada nó é feita de maneira automática. A Figura 13 exibe com é a interface do CORE.

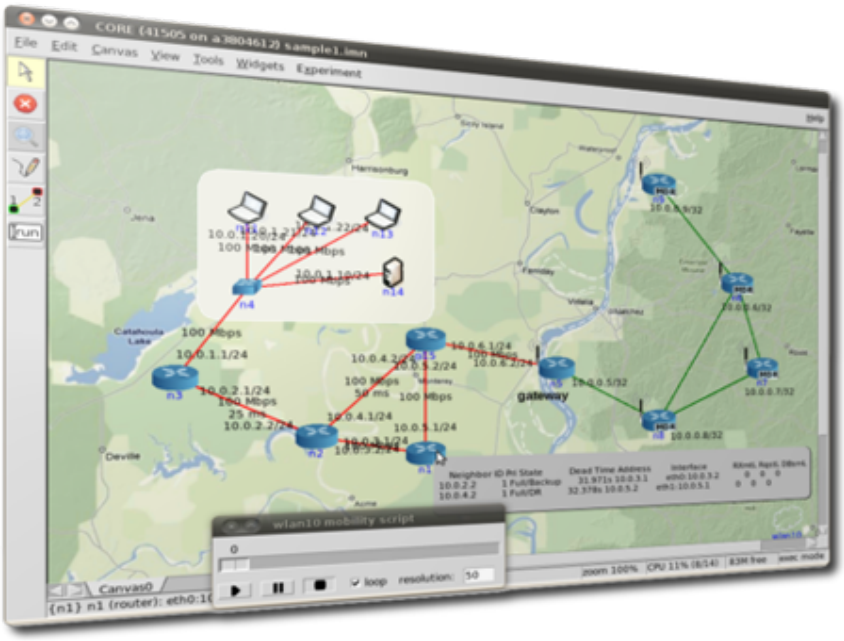

Figura 13: Common Open Research Emulator

Fonte: http://www.nrl.navy.mil/itd/ncs/products/core

Com exceção do GNS3, os outros *softwares* de rede não trabalham com sistemas operacionais reais de roteadores, ou seja, podem não disponibilizar todas as funcionalidades que um dispositivo real permite realizar.

O GNS3 trabalha com a emulação do sistema operacional de roteadores, o *Internetwork Operating System* (IOS), que é obtido dos próprios roteadores físicos. O Dynamips[14] funciona em conjunto com o GNS3 para realizar a emulação destes roteadores. A desvantagem do GNS3 é o uso excessivo de recursos de um computador, problema que pode ser superado com algumas configurações (RIETSCHE; RUSSELL; KARDUCK, 2011).

A respeito da análise dos pacotes IP que trafegam em uma rede, é possível com a utilização da ferramenta denominada Wireshark[15], que é um analisador de protocolos de rede inclusa no GNS3. Permite-se verificar detalhadamente cada pacote, e, por isso, esta ferramenta é destinada tanto para as empresas como para o ensino de redes. A Figura 14 exibe a interface do Wireshark.

[14] http://dynagen.org/
[15] http://www.wireshark.org/

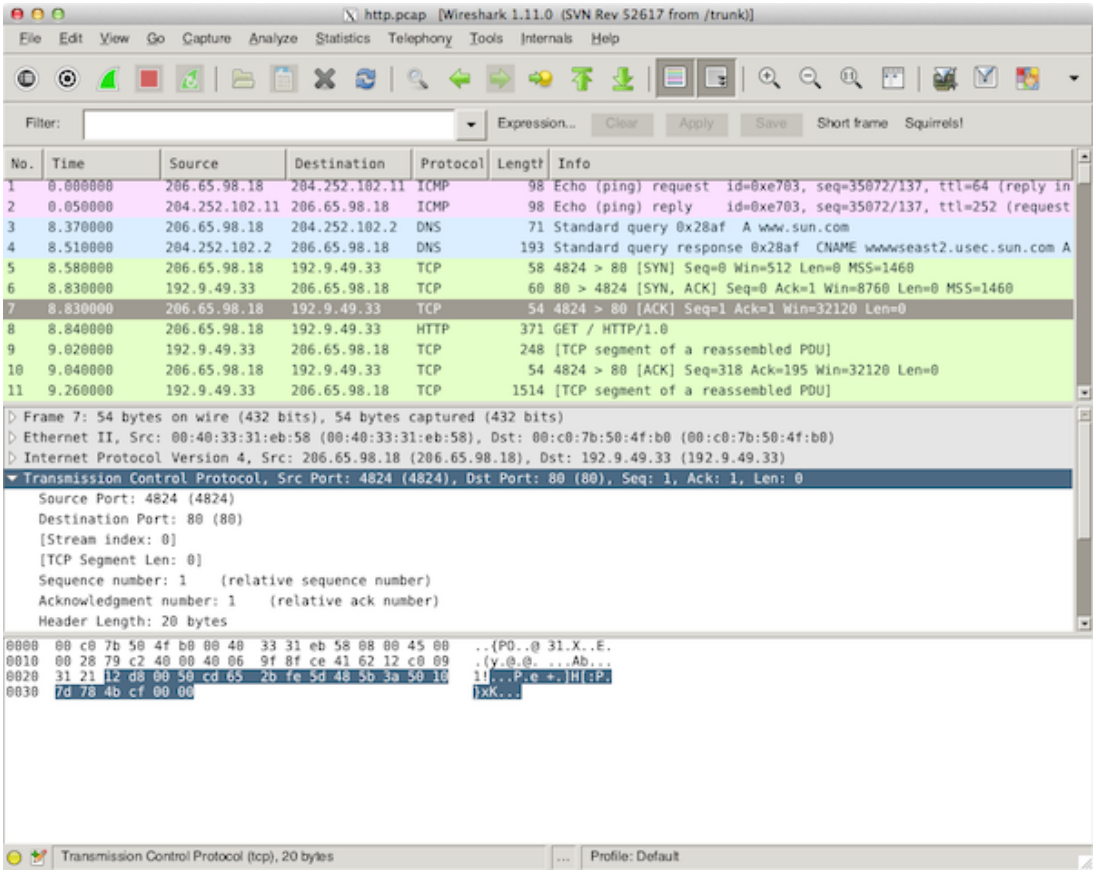

Figura 14: Wireshark

Fonte: https://blog.wireshark.org/

Por fim, para a mensuração do desempenho de um rede, se faz factível através da utilização do *software* Iperf[16], que, por meio da criação de fluxos de dados, pode simular a transferência de arquivos de um ponto ao outro. Esta ferramenta está disponível em uma máquina virtual que é utilizada no GNS3[17] como uma estação de trabalho. Alguns parâmetros possíveis de serem utilizados nos comandos do Iperf incluem:

- -s: Iniciar Iperf em modo servidor;
- -V: Indica que serão utilizados pacotes IP da versão 6;
- -c *host*: Iniciar Iperf em modo cliente e conectar ao servidor endereçado em *host*;
- -n tamanho: Indica o tamanho do fluxo de dados para transferir.

A Figura 15 exibe, graficamente, um exemplo do Iperf sendo utilizado nos modos cliente e servidor, e configurado com os parâmetros que foram citados acima.

[16]http://sourceforge.net/projects/iperf/
[17]http://www.gns3.net/news/microcore-and-tinycore-3-8-2-qemu-images/

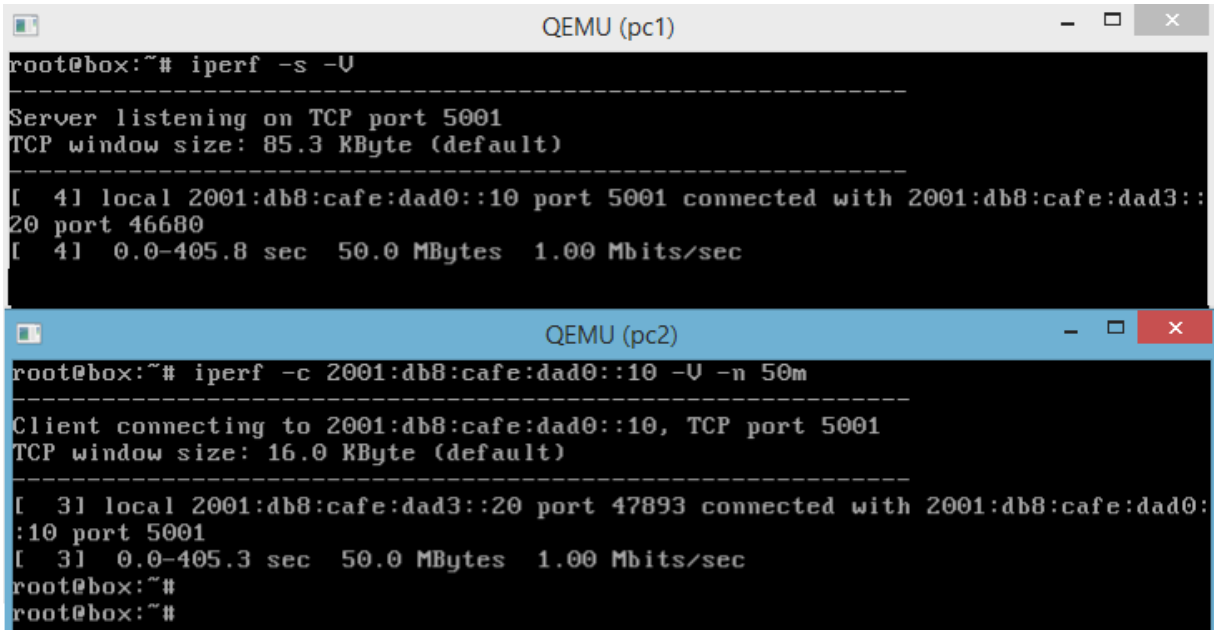

Figura 15: Iperf

Fonte: Autoria Própria

2.2 TRABALHOS CORRELATOS

Nesta seção, são analisados outros trabalhos correlatos à este presente trabalho, que é o uso do IPsec. Inclui também uma matriz de documentos dos trabalhos correlatos, segundo sugerido por Wazlawick (WAZLAWICK, 2008), que sumariza as informações sobre estes trabalhos.

Em Santos (2004), é relatado um estudo sobre os impactos do IPv6, seus problemas e limitações, assim como as estratégias de transição entre o IPv4 e o IPv6. É feito o uso do IPsec, em modo transporte, para interligar ambientes cooperativos, ou seja, uma rede segura que integraria várias organizações.

O trabalho feito por Castro (2004) teve como objetivo a analise de várias soluções de VPN, que incluem o uso de um túnel seguro entre redes distintas. Foca na utilização do IPsec, da versão do IPv4, para prover uma VPN. Porém, não foi realizado uma implantação efetiva.

Outro trabalho analisado é o de Falconi (2004), que tratou do uso dinâmico do IPsec com o IPv6, para a utilização do IPsec somente em alguns casos específicos, e desabilitando-o em outros que não necessitem do uso de IPsec. Somente foram realizados testes do tipo de conectividade computador-a-computador, ou seja, o modo transporte do IPsec.

Já em Silva (2006), o respectivo trabalho teve como objetivo a realização de uma análise dos protocolos IP versão 4, IP versão 6, e do IP versão 4 com IP *security*. Como pode ser

identificado, não foram realizados testes que envolveram o IP versão 6 configurado para utilizar o IP *security*.

Outro trabalho que envolve a utilização do IPsec é o de Adeyinka (2008), que apresenta o IPsec para a implantação de VPN's. Realiza também a demostração dos modelos de conexão segura, como o *host-to-host*, *host-to-gateway* e *gateway-to-gateway*. Por fim, mostra que o modo *gateway-to-gateway* (modo túnel entre dois roteadores de borda de uma rede) pode implementar múltiplas conexões IPsec, para diferentes tipos ou classes de tráfego.

O trabalho realizado por Almeida e Ines (2009) também faz uma analise geral do IP versão 6, assim como a execução de testes entre dois hosts, interligados por meio do equipamento de redes denominado switch. Os experimentos incluíram o uso do IPSec e a não utilização do mesmo. O modo IPsec implantado para a realização dos testes foi o de transporte.

Em Basso (2011), é abordado o uso do IPv6 com IPsec. Uma análise de desempenho é feita somente com o modo transporte. Não foram realizados testes sobre segurança. Uma das conclusões apresentadas é que arquivos de até 100 MB tiveram o mesmo tempo de transferência de um computador para outro, usando IPsec e sem IPsec, ou seja, não houveram perdas no desempenho de transferência ao utilizar o IPsec.

Por fim, o projeto feito por Godinho (2012) teve como objetivo a realização de uma proposta de utilização do IPsec para criar uma VPN entre roteadores, utilizando o modo túnel do IPsec. Porém, neste trabalho foi utilizado o protocolo IPv4. É feita, na parte de trabalhos futuros deste trabalho, há a sugestão de estudar uma implantação em IPv6.

A matriz de documentos dos trabalhos pesquisados, representado na Tabela 5, nos fornece uma visão geral dos mesmos. É possível identificar que este presente trabalho complementa os trabalhos aqui pesquisados, pois estuda o protocolo IPv6, assim como o IPsec em modo túnel, e também realiza a implantação para os experimentos com estes protocolos.

Tabela 5: Matriz de documentos dos trabalhos pesquisados

Trab./Atributo	Protocolos estudados	Modo IPsec estudado	Houve implantação para testes?
Santos (2004)	IPv4, IPv6	Transporte	Sim
Castro (2004)	IPv4	Túnel	Não
Falconi (2004)	IPv6	Transporte	Sim
Silva (2006)	IPv4, IPv6	Túnel	Sim, exceto IPv6
Adeyinka (2008)	IPv4, IPv6	Transporte, Túnel	Não
Almeida e Ines (2009)	IPv4, IPv6	Transporte	Sim
Basso (2011)	IPv6	Transporte	Sim
Godinho (2012)	IPv4	Túnel	Sim

Fonte: Autoria Própria

Concluindo, este capítulo abordou os trabalhos correlatos ao tema desta presente pesquisa, enfatizando os que tiveram o uso ou implantação do protocolo IPsec, em conjunto com o protocolo IP das versões 4 e 6.

3 METODOLOGIA

Esta etapa apresenta como foi o desenvolvimento do trabalho, descrevendo os cabeçalhos do IPsec que foram utilizados no túnel, a ferramenta de simulação de redes, e os procedimentos para a construção de uma rede 100% IPv6. Os procedimentos apresentam como a rede foi implantada, como o IPsec é aplicado nesta rede, e como os experimentos de desempenho e segurança foram realizados nesta topologia de rede.

3.1 CABEÇALHOS IPSEC UTILIZADOS

O IPsec que foi analisado neste trabalho é o que opera com a versão 6 do *Internet Protocol*. Os cabeçalhos IPsec que são utilizados, para realizar um estudo de caso, foram o AH e o ESP. O AH garante a autenticidade da origem dos pacotes, assim como a sua integridade. O ESP garante a criptografia dos dados transportados nos pacotes.

Os roteadores de borda receberam a instalação do IPsec, assim trabalharam em modo túnel. Uma rede que não opera em modo túnel, ou seja, somente em modo transporte, necessitaria que todos os dispositivos nela suportassem o IPsec, e teriam de ser configurados individualmente para a sua utilização.

3.2 FERRAMENTAS

Sobre a ferramenta que foi utilizada na simulação de redes, era necessária uma ferramenta que permitiria a implantação do IPsec em seus roteadores virtuais, e que trabalhariam de forma fiel aos roteadores físicos. Também era necessário uma ferramenta que possibilitasse a análise dos pacotes que passariam por estes roteadores virtuais.

O Capítulo 2 deste trabalho indicou que a ferramenta que atenderia aos requisitos descritos no parágrafo anterior, principalmente ao requisito de fidelidade aos roteadores físicos, era a ferramenta de simulação de redes GNS3.

Para fins de testes, foram utilizados, inicialmente, os computadores do laboratório de redes do Departamento Acadêmico de Informática (DAINF), do Campus Curitiba da Universidade Tecnológica Federal do Paraná, que possuíam o GNS3 instalado. Ressaltamos que o departamento estava ciente da realização deste trabalho, e havia concedido a permissão para tal. Porém, foi utilizado, um computador pessoal para a realização dos experimentos.

O GNS3 foi utilizado sem o apoio dos equipamentos físicos de rede, pois houveram problemas de *hardware* com os roteadores físicos, além da falta de algumas funções necessárias. Os roteadores virtualizados que são utilizados para a realização dos experimentos possuíam a compatibilidade adequada para o uso de todas as características necessárias do IPsec para IPv6.

3.3 PROCEDIMENTOS

Nesta seção é descrita como a rede IPv6 foi implantada, como o IPsec foi aplicado nesta rede, e como os experimentos de desempenho e segurança foram realizados nesta rede. A Figura 16 apresenta uma representação visual de como é uma rede que não realiza o uso do IPsec e outra rede que faz o uso do IPsec.

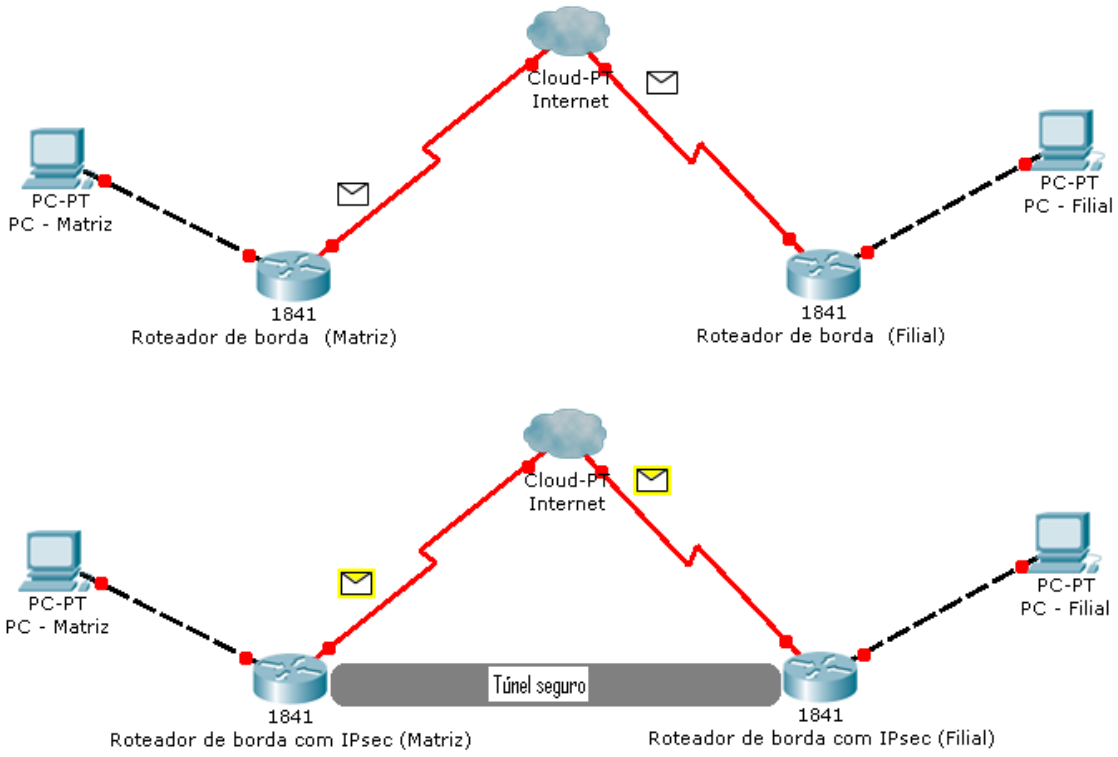

Figura 16: 2 topologias, uma sem o IPsec e outra com o IPsec

Fonte: Autoria Própria

3.3.1 Implantação da rede IPv6

Antes da implantação efetiva de uma rede completamente IPv6, se fez necessário realizar a instalação do GNS3, em conjunto com a ferramenta Dynamips (emulação dos roteadores) e o Wireshark (análise dos pacotes IP), já comentadas no Capítulo 2.

A Figura 17 apresenta a rede que foi implantada para a realização dos testes com o IPsec. O **R1** e o **R2** são os roteadores que realizaram a ligação entre as duas redes distintas. O computador **pc1** recebeu os arquivos vindos do **pc2**, localizados em redes distintas. Somente a rede que interliga as duas redes, que se comunicaram, utilizaram o IPsec.

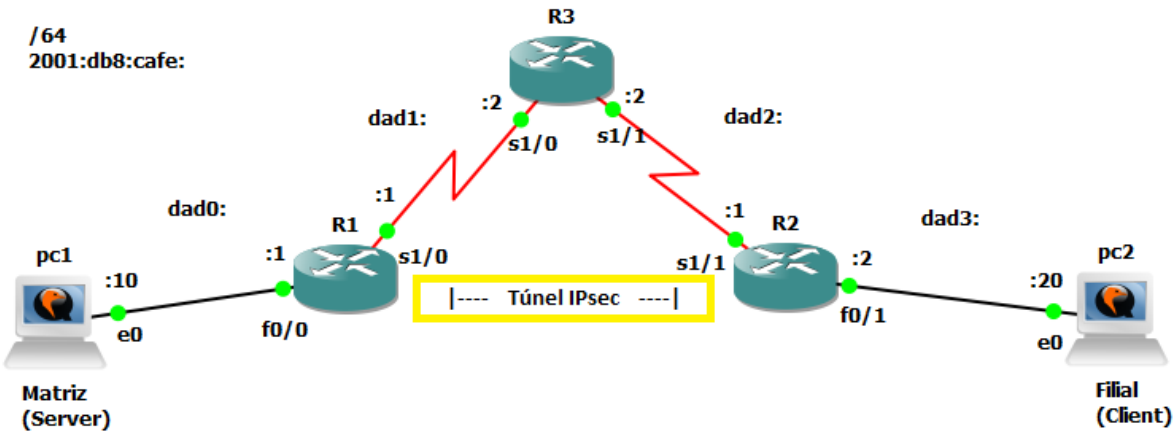

Figura 17: 2 redes que utilizaram o IPsec

Fonte: Autoria Própria

3.3.2 Aplicação do IPsec

Após a construção da rede IPv6, foi realizada a implantação do IPsec, que atuou como um túnel seguro entre as duas redes que desejam se comunicar. Para a troca de chaves entre os roteadores, que permitiria o acesso ao conteúdo dos pacotes, foi escolhida a modalidade de chaves pré-compartilhadas, pois a modalidade de certificado digital (certificados X.509) exigiria que uma Autoridade Certificadora, como a Certisign[1] realizasse a emissão do mesmo.

Após a criação do mecanismo de chaves, foi feita a configuração do IPsec em cada um dos roteadores de borda. Foram realizados as configurações do modo IPsec a ser utilizado, que neste trabalho foi o modo túnel, assim como o uso dos cabeçalhos ESP e AH, que garantem a

[1] http://www.certisign.com.br/certificado-digital

confidencialidade e autenticação dos pacotes IP.

3.3.3 Experimentos de desempenho e segurança

Para a realização dos experimentos deste trabalho, foram feitos 4 principais cenários de testes. O primeiro cenário refere-se a transmissão de pacotes sem a utilização do IPsec. O segundo cenário teve a ativação do AH (autenticação e integridade), e, no terceiro, do ESP (criptografia). Por fim, o quarto cenário teve a configuração do AH + ESP no IPsec.

No primeiro cenário, para a realização dos testes, foi utilizado a ferramenta Iperf, que gerou um fluxo de dados, simulando a transferência de um arquivo vindo da rede Filial para a rede Matriz. A mensuração de quanto tempo durou a transferência de um arquivo é medida em segundos, porém, a conversão para minutos pode facilitar a compreensão dos resultados. Portanto, os arquivos do tamanho de 50, 100, 200, 400, 800, 1600 Megabytes são transferidos da rede Filial, que está no **R2**, para a rede Matriz, que está no roteador de borda **R1**, com o uso do Iperf.

Já nos cenários segundo e terceiro foi realizado a mesma transferência descrita no parágrafo anterior, porém o IPsec foi ativado com os cabeçalhos AH e ESP, separadamente. A ferramenta de análise Wireshark habilitou a verificação da utilização destes cabeçalhos nos pacotes IP.

Por fim, no último cenário, o de número quatro, os pacotes IP utilizaram o IPsec com ambos os cabeçalhos estudados neste presente trabalho, ou seja, o AH em conjunto com o ESP. Deste modo, assim como no parágrafo anterior, a ferramenta Wireshark permitiu a verificação do uso do AH, que garante a integridade dos pacotes, assim como o uso do ESP, que garante a criptografia dos dados.

3.4 RESULTADOS DOS EXPERIMENTOS REALIZADOS

A Tabela 6 fornece os resultados dos experimentos de desempenho que foram realizados com 3 roteadores. Os pacotes foram do tipo TCP, com o tamanho de janela igual a 16 KBytes, ou seja, o receptor dos dados confirmava o recebimento dos mesmos a cada 16 KBytes transferidos. Já a respeito da transmissão dos dados, esta foi igual a cerca de 1 Mbits por segundo. Deste modo, 1 Mbit é equivalente a 128 Kilobytes, que divididos por 16 KBytes da janela, resulta em 8 confirmações de recebimento de dados por segundo.

Tabela 6: Matriz com os resultados dos experimentos mensurados (3 roteadores)

Tamanho do arquivo (MB)	Sem IPsec (Min)	Somente AH (Min)	Somente ESP (Min)	AH + ESP (Min)
50	6	7	7	7
100	12	13	13	14
200	25	26	27	27
400	49	53	54	54
800	100	105	107	109
1600	199	211	215	218

Fonte: Autoria Própria

Sobre a variância entre os resultados que não utilizaram IPsec, e os que utilizaram os dois cabeçalhos do IPsec, em conjunto com as projeções de tendência apresentadas na Tabela 7, é visualizado que a diferença fica estabilizada em 9% entre as duas modalidades citadas.

Tabela 7: Matriz com os resultados dos experimentos projetados (3 roteadores)

Tamanho do arquivo (MB)	Sem IPsec (Min)	AH + ESP (Min)	Variação entre Sem IPsec e AH + ESP (%)
3200	399	436	9
6400	797	872	9
12800	1595	1744	9
25600	3191	3488	9
51200	6382	6975	9

Fonte: Autoria Própria

A Figura 18 apresenta, em forma gráfica, a variação entre os experimentos descritos.

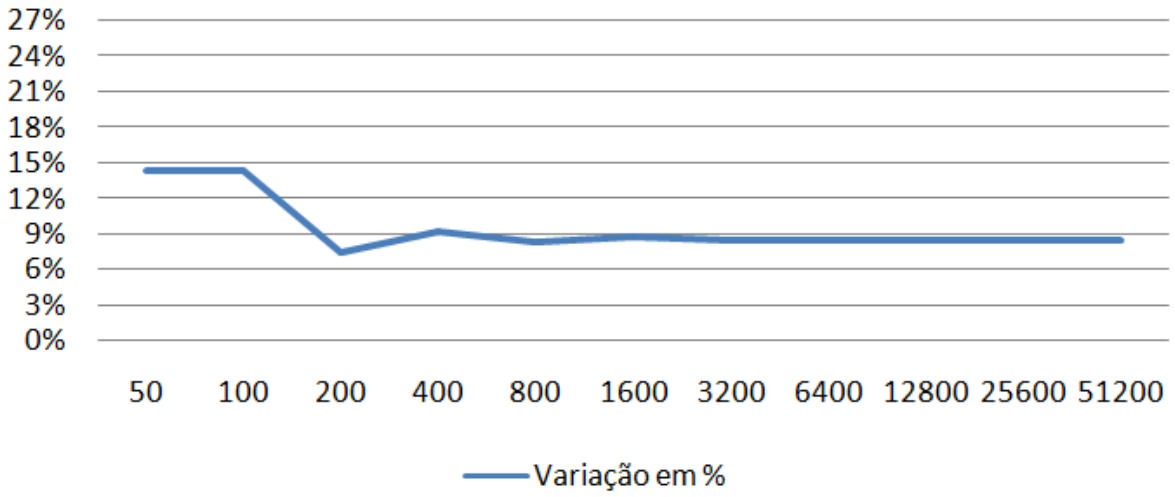

Figura 18: Variação entre os experimentos sem IPsec e com os cabeçalhos AH + ESP (3 roteadores)

Fonte: Autoria Própria

Na Tabela 8 são apresentados os resultados dos experimentos de desempenho que foram realizados com 7 roteadores. O aumento de 3 para 7 roteadores foi para confirmar se a diferença entre os resultados dos experimentos atingem proporções de estabilidade equivalentes.

Tabela 8: Matriz com os resultados dos experimentos mensurados (7 roteadores)

Tamanho do arquivo (MB)	Sem IPsec (Min)	AH + ESP (Min)
50	6	7
100	13	14
200	26	29
400	52	57
800	103	113
1600	206	222

Fonte: Autoria Própria

Novamente, a variância entre os resultados foram analisados, e, também em conjunto com as projeções de tendência realizadas e apresentadas na Tabela 9, estas indicaram que a diferença entre as duas modalidades testadas, sem o uso do IPsec, e com o uso do IPsec, ficaram estabili-

zadas em 7%.

Tabela 9: Matriz com os resultados dos experimentos projetados (7 roteadores)

Tamanho do arquivo (MB)	Sem IPsec (Min)	AH + ESP (Min)	Variação entre Sem IPsec e AH + ESP (%)
3200	412	445	7
6400	824	888	7
12800	1647	1774	7
25600	3294	3547	7
51200	6589	7092	7

Fonte: Autoria Própria

A Figura 19 apresenta, em forma gráfica, a variação completa entre os experimentos relatados.

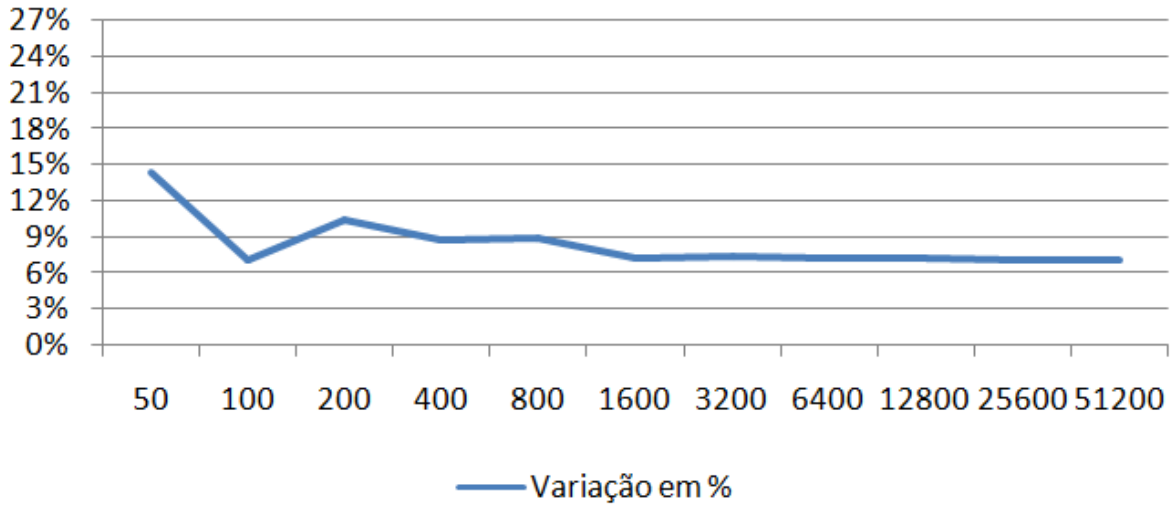

Figura 19: Variação entre os experimentos sem IPsec e com os cabeçalhos AH + ESP (7 roteadores)
Fonte: Autoria Própria

Já a respeito do uso dos cabeçalhos AH e ESP, que garantem a utilização da segurança fornecida pelo IPsec, é possível verificar a sua presença na Figura 20, onde o pacote apresenta o uso do cabeçalho de autenticação, e na Figura 21, que assegura a utilização do cabeçalho ESP para realizar a criptografia dos dados.

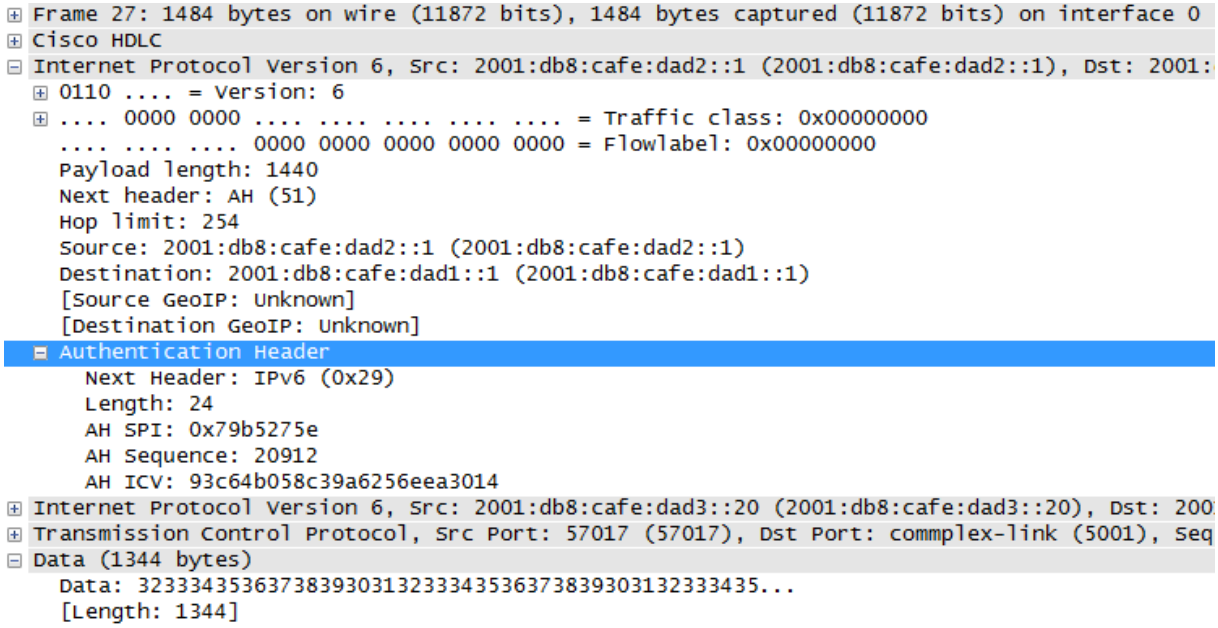

Figura 20: Pacote utilizando somente o cabeçalho AH

Fonte: Autoria Própria

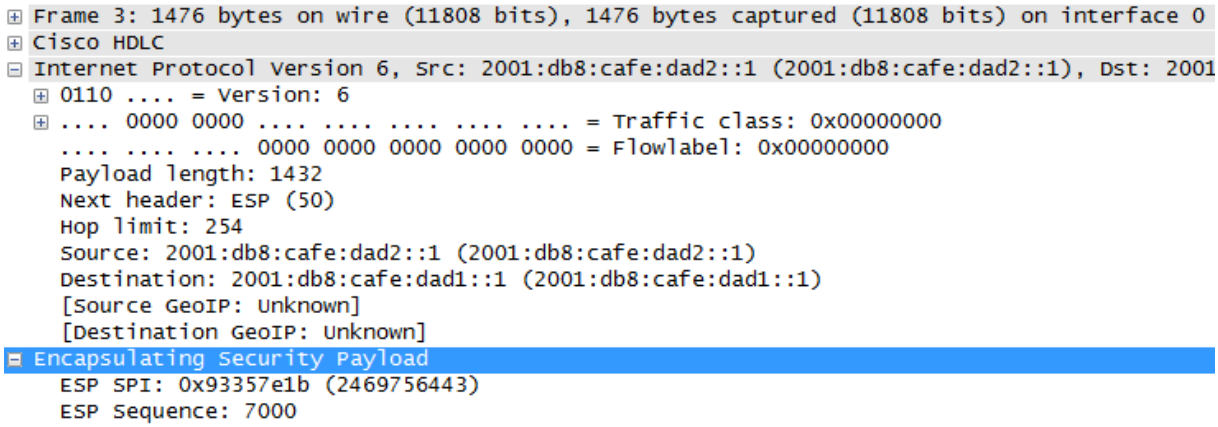

Figura 21: Pacote utilizando somente o cabeçalho ESP

Fonte: Autoria Própria

Por fim, a Figura 22 exibe o uso em conjunto dos dois cabeçalhos do IPsec estudados, no pacote TCP em questão.

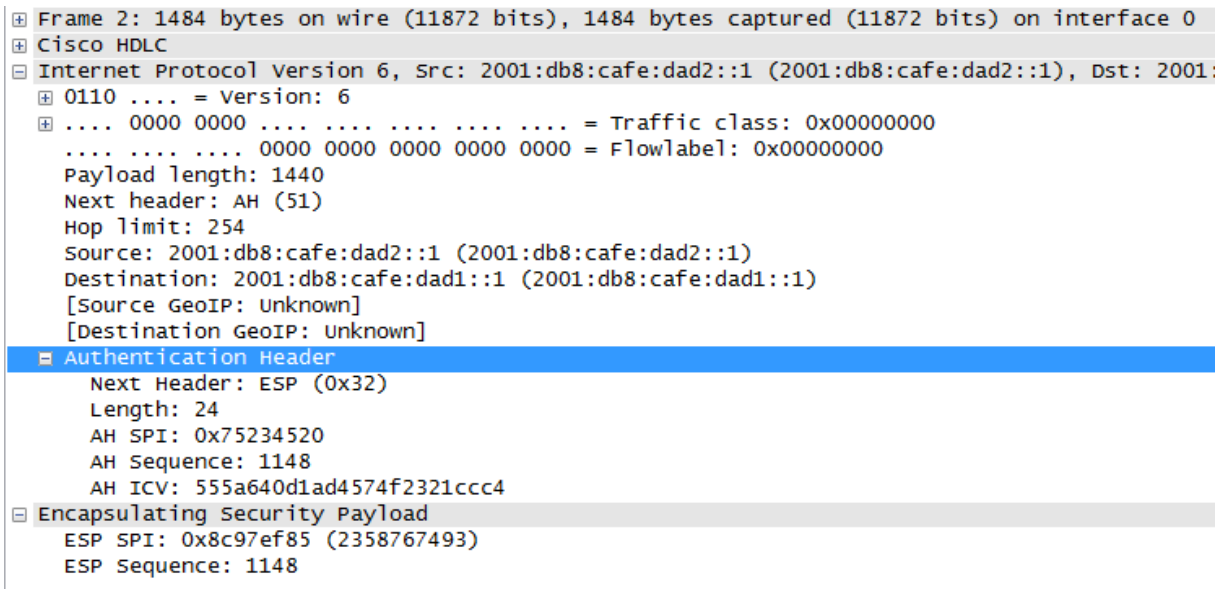

Figura 22: Pacote utilizando o cabeçalho AH com o ESP

Fonte: Autoria Própria

Para fins de complemento, a Figura 23 indica como é formado um pacote TCP que não faz o uso de um túnel IPsec.

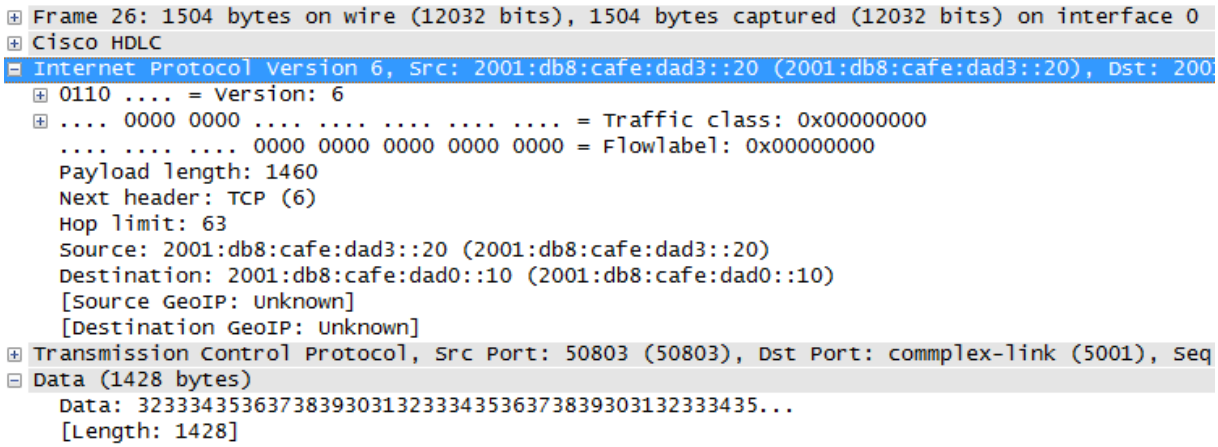

Figura 23: Pacote sem os cabeçalhos que compõem o túnel IPsec

Fonte: Autoria Própria

4 CONSIDERAÇÕES FINAIS

O capítulo descreve as considerações finais deste presente trabalho, e apresentará se os seus objetivos, através do desenvolvimento do trabalho, foram atingidos. Há também os comentários finais do trabalho, como os pontos positivos, os pontos negativos, e a indicação de oportunidades de pesquisa para trabalhos futuros.

4.1 CONSIDERAÇÕES FINAIS SOBRE OS OBJETIVOS DO TRABALHO

Para consolidar as considerações finais, primeiramente, são analisados cada um dos itens que foram descritos na subseção de objetivos específicos, localizado na seção do objetivos, comentando como cada um deles é atingido. Após o relato de todos os itens dos objetivos específicos, é realizado uma análise do objetivo geral, verificando se o mesmo é atingido.

O primeiro e o segundo item dos objetivos específicos indicou o estudo do estado da arte do protocolo IPv6 e do IPsec, cujo estudo foi realizado através da prospecção de documentos e trabalhos que realizaram a utilização destes protocolos.

Em seguida, houve o item que requeria a exploração do IPsec no IPv6, mais precisamente sobre os cabeçalhos AH e ESP. A revisão bibliográfica apresentou pesquisas que envolveram o uso do IPsec com o IPv4, que, em relação aos cabeçalhos de autenticação e criptografia, são os mesmos para ambas as versões de IP.

Outro item dos objetivos específicos foi a prospecção dos equipamentos de rede, assim como a de ferramentas computacionais que permitem a implantação de uma rede virtual. A revisão bibliográfica indica que o *software* GNS3 permitiria a construção desta topologia virtual. Os equipamentos físicos de redes, que o laboratório do DAINF disponibilizava para uso, tinham suporte ao IPsec, porém houveram limitações com o *hardware* de memória dos roteadores disponíveis, pois tinham 32 Megabytes, e o IOS que suporta todos os recursos necessários para a total implantação da rede necessitava de 64 Megabytes.

Sobre a implantação efetiva de uma rede completamente IPv6, esta foi construída na ferra-

menta GNS3, cujo motivo já foi explicado no parágrafo anterior. Foram feitas duas topologias, uma com 3 roteadores, e outra com 7 roteadores, para que os resultados dos experimentos disponibilizassem mais dados para serem analisados.

Já o item sobre a utilização da rede, descrita anteriormente, para a realização dos testes, permitiu a verificação da viabilidade do uso dos cabeçalhos do IPsec. A análise dos pacotes apresentaram a utilização efetiva da segurança provida pelos cabeçalhos AH e ESP. Já sobre o desempenho, o uso dos cabeçalhos AH e ESP, em comparação com a não utilização do IPsec, mostraram ser recomendáveis para serem utilizados pelos interessados em autenticação, integridade, e confidencialidade dos pacotes, pois a diferença de desempenho entre as duas modalidades de configuração se estabilizaram, nos testes realizados, em 7% (com 7 roteadores) e 9% (com 3 roteadores).

O último item dos objetivos específicos, que trata do fornecimento da metodologia adotada para a realização dos experimentos neste presente trabalho, pôde ser atendida após a conclusão dos itens anteriormente destacados.

Finalmente, sobre o objetivo geral deste presente trabalho, que era o de avaliar o desempenho e a segurança de uma rede completamente IPv6 que utiliza o modo túnel do IPsec, e que após o relato realizado nos parágrafos anteriores, é visto que o objetivo foi atingido.

4.2 COMENTÁRIOS FINAIS SOBRE O TRABALHO

As contribuições deste presente trabalho são para o encorajamento ao uso do IPsec, que, quando utilizado com os seus cabeçalhos AH e ESP, garantirão, respectivamente, que o pacote de rede tenha a sua integridade preservada, a autenticidade do remetente deste pacote assegurada, assim como a confidencialidade do seu conteúdo protegida.

Sobre as limitações deste trabalho, incluem a não utilização de equipamentos reais de redes, como foi planejado anteriormente. Porém, a ferramenta GNS3 garantiu que os experimentos tivessem a mesma credibilidade que os equipamentos reais, através da virtualização dos roteadores, que utilizaram, fielmente, o mesmo sistema operacional (IOS) que os equipamentos reais.

Por fim, a oportunidade futura de pesquisa que o presente trabalho indica é a de realizar estes mesmos experimentos com roteadores no paradigma *Software-Defined Networking* (SDN), que, basicamente, retiram a camada de controle (responsável por definir os processos de roteamento, engenharia de tráfego, políticas de segurança), que ficavam no próprio equipamento de rede, e a colocam em um servidor SDN, centralizando assim o controle de toda uma rede.

REFERÊNCIAS

ADEYINKA, O. **IPsec Mechanism for Implementing VPN**. 2008. Disponível em: <http://www.researchgate.net/publication/200446086_IPSec_Mechanism_for_Implementing_VPN>.

ALMEIDA, E. N. d.; INES, O. A. d. S. **Introdução ao protocolo IPv6 e análise de desempenho do IPsec sobre os protocolos IPv4 e IPv6**. 2009. Disponível em: <http://pt.scribd.com/doc/24420672/Introducao-ao-IPv6-e-Desempenho-do-IPSec-com-IPv4-e-IPv6>.

BASSO, C. **Implementação de IPSEC integrado com o IPv6**. 2011. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/handle/1/198>.

CASTRO, R. d. A. e. **Uma analise de soluções VPN em redes corporativas de alta capilaridade**. 2004. Disponível em: <http://www.bibliotecadigital.unicamp.br/document/?code=vtls000346103>.

DEERING, S.; HINDEN, R. **Request for Comments: 2460**. 1998. Disponível em: <http://tools.ietf.org/html/rfc2460>.

DELGROSSI, L.; BERGER, L. **Request for Comments: 1819**. 1995. Disponível em: <http://tools.ietf.org/html/rfc1819>.

DROMS, R. **Request for Comments: 1531**. 1993. Disponível em: <http://tools.ietf.org/html/rfc1531>.

FAGUNDES, B. A. **Uma Implementação de VPN**. 2007. Disponível em: <http://www.lncc.br/ borges/doc/Uma%20Implementa%E7%E3o%20de%20VPN.TCC.pdf>.

FALCONI, A. P. **Uso dinâmico do IPsec com IPV6**. 2004. Disponível em: <http://mtc-m18.sid.inpe.br/col/sid.inpe.br/jeferson/2005/01.07.10.46/doc/publicacao.pdf>.

GODINHO, M. E. M. **Uma arquitetura de implementação de redes virtuais privadas sobre a estrutura da Universidade do Contestado - UnC**. 2012. Disponível em: <http://feb.ufrgs.br/feb/objetos/1156289>.

HIRATA, L. A.; JÚNIOR, K.; SOUZA, J. A. d. **Internet Protocol Security - IPsec**. 2008. Disponível em: <http://pt.scribd.com/doc/55097243/Trabalho-ipsec-tcp-IP-3Q2008>.

KENT, S.; SEO, K. **Request for Comments: 4301**. 2005. Disponível em: <http://tools.ietf.org/html/rfc4301>.

RADWAN, A. M. **Using IPsec in IPv6 Security**. 2006. Disponível em: <https://www.uop.edu.jo/csit2006/vol2%20pdf/pg471.pdf>.

REKHTER, Y.; LI, T. **Request for Comments: 1518**. 1993. Disponível em: <http://tools.ietf.org/html/rfc1518>.

REKHTER, Y. et al. **Request for Comments: 1918**. 1996. Disponível em: <http://tools.ietf.org/html/rfc1918>.

RIETSCHE, R.; RUSSELL, G.; KARDUCK, A. P. **Creation of an online virtual Cisco router learning environment**. 2011. Disponível em: <http://researchrepository.napier.ac.uk/4639/1/Russell2.pdf>.

RODRIGUES, R. A. **IPv6: Uma nova era para a Internet e seus serviços**. 2009. Disponível em: <www.ppgia.pucpr.br/ jamhour/Download/pub/RSS/MTC/referencias/TCC - RaimundoRodrigues.pdf>.

SANTOS, C. R. d. **Integração de IPv6 em um ambiente cooperativo seguro**. 2004. Disponível em: <http://www.bibliotecadigital.unicamp.br/document/?code=vtls000334763>.

SILVA, E. L. d. **Estudo comparativo e análise de desempenho entre os protocolos de comunicação IPv4 e IPv6**. 2006. Disponível em: <http://gravatai.ulbra.tche.br/ roland/tcc-gr/monografias/2006-2-tc2-Everton_Luis_da_Silva.pdf>.

SRISURESH, P.; HOLDREGE, M. **Request for Comments: 2663**. 1999. Disponível em: <http://tools.ietf.org/html/rfc2663>.

WAZLAWICK, R. S. **Metodologia de pesquisa para ciência da computação**. Rio de janeiro: Elsevier, 2008.

APÊNDICE A – RECURSOS DE *HARDWARE* E *SOFTWARE*

Neste capítulo são apresentados todos os recursos para o desenvolvimento do trabalho, assim como a origem destes recursos.

A.1 RECURSOS DE *HARDWARE*

Os recursos de *hardware* deste trabalho têm a sua origem no laboratório de redes do DAINF, do campus Curitiba da UTFPR. Seriam utilizados os roteadores já disponíveis no laboratório de redes, pois possuem suporte ao IPsec do IPv6. Porém, algumas limitações como a capacidade de memória e falta de algumas características para a efetiva implantação do IPsec impediram a utilização de tais roteadores. O modelo destes equipamentos estão em detalhes na Tabela 10.

Tabela 10: Equipamentos disponíveis no laboratório de redes

Quantidade	Tipo	Modelo	Fabricante
1	Switch L3	2948G	Cisco
2	Switch L3	8500	Cisco
2	Servidor	PowerEdge 2450	Dell
3	Roteador	2600	Cisco

Fonte: Autoria Própria

A configuração do computador do laboratório de redes, que serviria de suporte para a execução do GNS3, e que receberia a topologia de testes citada no capítulo de Metodologia, é detalhada na Tabela 11.

Tabela 11: Configuração do computador do laboratório

Processador	Memória	Disco Rígido	Sistema Operacional
Pentium Core 2 Duo	4 GB RAM	160 GB SATA	Linux Debian 3.7.2

Fonte: Autoria Própria

Contudo, os experimentos acabaram por ser executados em um computador pessoal. A configuração do computador é detalhada na Tabela 12.

Tabela 12: Configuração do computador pessoal

Processador	Memória	Disco Rígido	Sistema Operacional
Pentium Core I5 3210M	4 GB RAM	500 GB SATA II	Windows 8 (64 bits)

Fonte: Autoria Própria

A.2 RECURSOS DE *SOFTWARE*

Os recursos de *software* que são utilizados neste projeto são: o GNS3 da versão 0.8.6, que já estava preparado para uso nos computadores do laboratório de redes e no computador pessoal; e a programação de roteadores, especificamente para a IOS dos roteadores CISCO c3745, com memória RAM de 128 MB. Os IOS são retirados de roteadores físicos para serem utilizados em *softwares* como o GNS3. A versão do IOS utilizado é a 12.4-4T.

APÊNDICE B – CONFIGURAÇÕES PARA OS EXPERIMENTOS

Neste capítulo são apresentadas todas as configurações utilizadas para a realização dos experimentos deste presente trabalho.

B.1 FASE 1: ESTABELECER A TOPOLOGIA BÁSICA

Nas estações (exemplo):

```
sudo su
ifconfig eth0 add 2001:db8:cafe:dad0::10/64 up
route -A inet6 add 2001:db8:cafe::/48 gw 2001:db8:cafe:dad0::1
```

Nos roteadores (exemplo):

```
ipv6 unicast-routing
ipv6 router rip rip_ng
exit
```

Nas interfaces, configurar RIPng (exemplo):

```
ipv6 enable
ipv6 add 2001:db8:cafe:dad0::1/64
ipv6 rip rip_ng enable
no shut
```

B.2 FASE 2: ESTABELECER O TÚNEL IPSEC ENTRE R1 E R2

ISAKMP (Estabelecimento de um ”idioma”entre os peers):

```
crypto isakmp enable
crypto isakmp policy 10
encryption aes 256
authentication pre-share
hash sha
```

```
group 5
lifetime 3600
exit
```

ISAKMP (Configuração da chave):

```
crypto isakmp key 0 minhachave address ipv6 2001:db8:cafe:dad2::1/64
```

IPsec Transform Set (Configuração do IPsec):

```
crypto ipsec transform-set set_ah ah-sha-hmac
exit
crypto ipsec transform-set set_esp esp-aes 256
exit
crypto ipsec transform-set set_ah_esp esp-aes 256 ah-sha-hmac
exit
```

IPsec profile:

```
crypto ipsec profile tunel_ah
set transform-set set_ah
exit
crypto ipsec profile tunel_esp
set transform-set set_esp
exit
crypto ipsec profile tunel_ah_esp
set transform-set set_ah_esp
exit
```

Criação do túnel virtual, com o AH (R1):

```
interface tunnel1
ipv6 enable
ipv6 unnumbered s1/0
tunnel source s1/0
tunnel destination 2001:db8:cafe:dad2::1
tunnel mode ipsec ipv6
tunnel protection ipsec profile tunel_ah
exit
```

Criação do túnel virtual, com o AH (R2):

```
interface tunnel1
ipv6 enable
```

ipv6 unnumbered s1/1
tunnel source s1/1
tunnel destination 2001:db8:cafe:dad1::1
tunnel mode ipsec ipv6
tunnel protection ipsec profile tunel_ah
exit

Configuração da rota para utilizar o túnel (R1):
ipv6 route 2001:db8:cafe:dad3::/64 tunnel1

Configuração da rota para utilizar o túnel (R2):
ipv6 route 2001:db8:cafe:dad0::/64 tunnel1

B.3 FASE 3: TRANSFERÊNCIA DE 50 MB ENTRE A FILIAL E A MATRIZ

Lado Matriz (Servidor):
iperf -s -V

Lado Filial (Cliente):
iperf -c 2001:db8:cafe:dad0::10 -V -n 50m

B.4 COMANDOS GERAIS PARA VERIFICAR AS CONFIGURAÇÕES

Troubleshooting:
show crypto isakmp sa de
show crypto ipsec sa (pipe) in encrypt
sh run (pipe) sec crypto