Segurança e Desempenho do IPsec em Redes IPV6

Denis Pohlmann Gonçalves[1], Henrique Tamiosso Machado[1], Filipe Kulinski de Mello[2]

[1]Instituto Federal Farroupilha (IFFar-svs) – São Vicente do Sul – RS

[2]Instituto Federal Farroupilha (IFFar-fw) – Frederico Westphalen – RS

{denis.goncalves, henrique.machado, filipe.kulinski}@iffarroupilha.edu.br

Abstract. *This paper presents the evaluation of performance and security in IPV6 networks using tunnel-mode IPSec through the implementation of the StrongSwan solution. In this context, several tests were performed with some analysis tools in a scenario simulating the IPV6 network between an operator and its client institution, comparing the use of IPSec and without the use of this technology. The results demonstrate that the use of IPSec in tunnel-mode ensures extra security at the network layer and its performance, although decreasing, is practically negligible.*

Resumo. *Este artigo apresenta a avaliação de desempenho e segurança em redes IPV6 utilizando o IPSec com funcionamento em modo túnel através da implementação da solução StrongSwan. Nesse contexto, foram realizados vários testes com algumas ferramentas de análise em um cenário simulando a rede IPV6 entre uma operadora e sua instituição cliente, comparando a utilização do IPSec e sem o uso dessa tecnologia. Os resultados demonstram que a utilização do IPSec em modo túnel assegura segurança extra na camada de rede e seu desempenho, apesar de decrescido, é praticamente desprezível.*

1. Introdução

Devido ao esgotamento do protocolo de internet versão 4 já em fase final desde fevereiro de 2017 [Lacnic 2018] e o aumento exponencial de dispositivos na internet, torna-se cada vez mais necessária a implantação definitiva do *Internet Protocol Version* 6 (IPV6). Entretanto, para isto é fundamental a comunicação que possua um desempenho favorável e atenda os princípios da segurança da informação, como, confidencialidade, integridade, disponibilidade e autenticidade, segundo os padrões internacionais, [ISO/IEC 17799:2005 2018].

Com o objetivo de padronizar o método de fornecimento de privacidade do usuário em uma rede de dados, surgiu o IP *Security Protocol* (Protocolo de Segurança IP), conhecido pela sua sigla IPSec. Esse protocolo combina diversas tecnologias que possibilitam maior segurança na comunicação em redes comutadas por pacotes, se comparado a sistemas que não os possuem. Porém, pode haver um certo custo de processamento que poderá influenciar no seu desempenho.

Assim sendo, este artigo tem por objetivo avaliar a segurança e desempenho do IPSec modo túnel em redes IPV6 através de testes efetuados em um ambiente específico simulado a rede entre uma operadora e sua instituição cliente, utilizando algumas ferramentas de uso livre, como sistema operacional Linux, analisador de pacotes

Wireshark, a ferramenta StrongSwan como solução IPSec, dentre outros. Contudo, os resultados dos experimentos colaboram na construção de conhecimento para a comunidade acadêmica e demais interessados no assunto.

Este artigo está organizado da seguinte forma. Na seção 2 são apresentados alguns trabalhos relacionados. A abordagem dos conceitos teóricos sobre protocolo IPV6 e suas tecnologias de segurança são apresentados na seção 3. Na seção 4 são descritos os materiais e configurações utilizadas no ambiente de avaliação, seguidos pelos testes de segurança e desempenho do protocolo IPV6. Na seção 5 são apresentados os resultados e discussões dos testes realizados. Por fim, a seção 6 é destinada às considerações finais e trabalhos futuros.

2. Trabalhos Relacionados

Existem trabalhos que utilizam diferentes metodologias na análise de desempenho e segurança do IPSec. Entretanto, alguns fazem apenas análise de desempenho e outros apenas experimentos com a segurança.

O trabalho de [Basso 2011], apresenta uma análise de desempenho com testes efetuados somente com o IPSec em modo transporte utilizando cabeçalhos *Autentication Header* (AH) e *Encapsulated Security Payload* (ESP), fazendo um comparativo de desempenho utilizando esses cabeçalhos. A segurança foi verificada, constatando a autenticação e criptografia com o uso do AH e ESP respectivamente, ocasionando um pequeno atraso na transferência de arquivos maiores de 100MB.

No trabalho de [Oliveira 2012], é testado somente a segurança do IPSec, através de ataques do tipo *man-in-the-middle* utilizando a suíte "THC-IPV6 *tool kit"*, aonde são utilizadas as ferramentas, "*parasite6*" que captura mensagens ICMPv6 em uma rede para aplicar técnicas de *spoofer* e "*alive6*" que utiliza uma técnica de envio de mensagem de descoberta de vizinhança. Segundo o autor, os resultados foram satisfatórios, entretanto o desempenho do protocolo não foi avaliado.

3. Fundamentação Teórica

Esta seção apresenta a fundamentação teórica necessária para a compreensão deste artigo, tendo foco principal nas características do IPV6 que dizem respeito a segurança.

3.1. Protocolo IPV6

De acordo com [IPV6 2018], o *Internet Protocol version* 6 (IPV6), é a versão mais atual do Protocolo de Internet, oficializado em 6 de junho de 2012, é o resultado do esforço do *Internet Engineering Task Force* (IETF) para criar a nova versão do IP, tendo seu início descrito por Scott Bradner e Allison Marken, em 1994, na *Request for Comments* (RFC) 1752. Sua principal especificação encontra-se na RFC 2460.

O novo protocolo IPV6 está sendo implantado gradativamente na Internet e está funcionando atualmente em *dual stack* (pilha dupla), trabalhando lado a lado com o IPv4. A longo prazo, o IPV6 tem como objetivo substituir o IPv4, que suporta pouco mais de 4 bilhões de endereços, contra cerca de 79 octilhões de vezes essa quantidade no novo protocolo, [IPV6.br 2018].

O IPV6 oferece várias melhorias em relação a versão anterior IPv4. Os cabeçalhos foram alterados para aumentar o seu desempenho nos roteadores e aplicações. Um dos principais objetivos de sua criação é a enorme quantidade de endereços com capacidade de 128 bits ao contrário dos 32 bits do IPv4, [Gledson e Lobato 2013].

3.2. IPSec

De acordo com [Stallings 1998], o *Internet Protocol Security* (IPSec) surgiu em 1995, como uma resposta à necessidade de segurança contra o monitoramento e o controle do tráfego não autorizados da rede. No protocolo IPV6, o IPSec é uma especificação que está incorporada ao protocolo, ou seja, tem seu suporte obrigatório, diferentemente do IPv4 que tem seu uso opcional.

A autenticação e a codificação definidas pelo IPSec são independentes das versões IPv4 ou IPV6 e o protocolo vem se tornando o verdadeiro padrão utilizado pelos tuneis VPN, [Nakamura e Geus 2007].

Nos dias atuais, o IPSec usa basicamente duas diferentes tecnologias, descritas na Tabela 1. Entretanto, no passado já contou com o *Autentication Header* (Cabeçalho de Autenticação), que é inferior em termos de segurança ao cabeçalho ESP por não prover a confidencialidade, [Tanenbaum 2003].

Tabela 1. Tecnologias do IPSec

Tecnologia	Função
***Encapsulation Security Payload* – ESP** (Cabeçalho de encapsulamento do *Payload*)	Fornece confidencialidade, integridade e autenticação dos pacotes.
***Internet Key Exchange* – IKE** (Protocolo de negociação e troca de chaves)	Permite a negociação das chaves de comunicação entre as organizações de modo seguro.

Conforme sugere [Nakamura e Geus 2007], o IPSec pode ser usado para a segurança da comunicação entre dois pontos, sendo possível garantir o sigilo e a integridade da comunicação, além de possibilitar a autenticação das conexões. O IPSec trabalha de duas maneiras, sendo modo transporte e modo túnel, descritos a seguir.

A. Modo Transporte - Nesse modo há transmissão direta dos dados protegidos pelo IPSec entre os hosts. A codificação e a autenticação são realizadas no *payload* do pacote IP, e não no cabeçalho IP.

B. Modo Túnel - Nesse modo, o *gateway* encapsula o pacote IP com a criptografia do IPSec, incluindo o cabeçalho de IP original. Ele então, adiciona um novo cabeçalho IP no pacote de dados e o envia por meio da rede pública para o segundo *gateway*, no qual a informação é decodificada e enviada ao *host* destinatário, em sua forma original.

3.3. Gerenciamento de Chaves

O gerenciamento de chaves é um dos processos mais significativos do IPSec e grande parte da segurança da comunicação residente, principalmente nas trocas iniciais das chaves. Um processo bem definido de troca de chaves deve ser adotado para evitar ataques do tipo *man-in-the-middle,* nos quais o atacante pode capturar as trocas das informações dos dois lados da comunicação, alterando-as para seus objetivos.

De acordo com [Nakamura e Geus 2007], o gerenciamento das chaves definido pelo IPSec é realizado pelo *Internet Key Exchange* (IKE), que tem como base o *Internet Security Association and Key Management Protocol* (ISAKMP) e o *Oakley*, que é o responsável pela troca das chaves.

4. Metodologia

Esta seção descreve os materiais e métodos utilizados para a realização desta pesquisa, como *softwares* e *hardware*, que permitiram um ambiente de testes adequado para a realização dos experimentos.

Como *hardware* necessário para instalação de todos os recursos de *softwares* servindo de laboratório de testes, foi utilizado um microcomputador do tipo *desktop*, com a seguinte configuração: Processador Intel Core i3 4130, 8GB de memória RAM DDR3 e disco rígido de 320GB *Sata II*.

Os demais materiais utilizados foram todos *softwares*, sendo:

A. GNU/Linux *Ubuntu* 64-bits *desktop* v. 18.04 LTS. Sistema operacional utilizado para sistema hospedeiro e máquina virtual "intruso".

B. GNU/Linux *Ubuntu* 64-bits *server* v. 18.04 LTS. Sistema operacional utilizado para máquinas virtuais.

C. VirtualBox v. 5.2.10_*Ubuntu*. Sistema Hipervisor para hospedagem e gerenciamento de máquinas virtuais.

D. StrongSwan v. 5.6.3. Pacote solução *OpenSource* para implementação do IPSec.

E. Iperf v.3. Aplicativo para medir a largura de banda ou tráfego de rede.

F. Wireshark v. 2.4.5. Aplicativo gráfico analisador de tráfego de rede.

4.1. Cenário de Testes

Para que fosse possível realizar todos os testes desta pesquisa, foi elaborado um cenário e aplicado em ambiente virtualizado, mostrado na Figura 1, onde foram realizadas todas as configurações iniciais nas máquinas virtuais, tais como, enlaces e endereçamento.

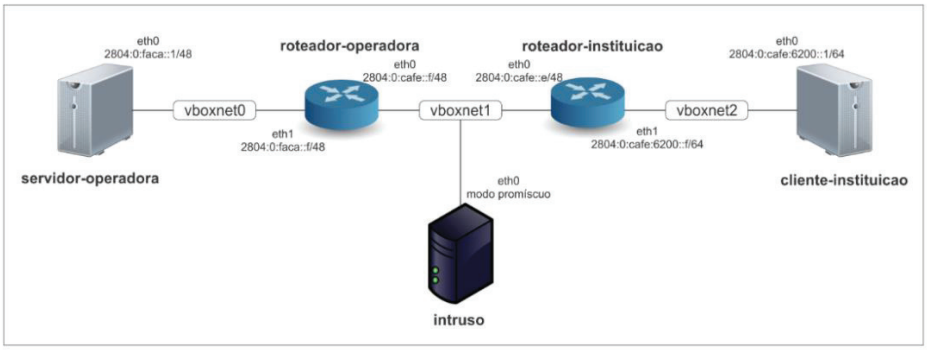

Figura 1. Cenário de testes em ambiente virtualizado
Fonte: dos autores

Este cenário é composto de cinco máquinas virtuais, sendo dois roteadores, um servidor, um cliente e um intruso. Com objetivo de possibilitar a comunicação das máquinas virtuais, foi necessário a criação de três redes exclusivas de hospedeiro com velocidade fixa de 100Mbps definida pelo VirtualBox, sendo "vboxnet0", "vboxnet1" e "vboxnet2". Essas redes virtuais simulam três enlaces fisicamente separados, não tendo ligação direta entre eles, utilizados para interligar o "roteador-operadora", "roteador-instituicao", "servidor-operadora", "cliente-instituicao" e "intruso".

Na instalação das seguintes máquinas virtuais, "roteador-operadora", "roteador-instituicao", "servidor-operadora" e "cliente-instituicao" foram utilizadas a distribuição *Ubuntu Server* somente em modo texto, visto que para todos os testes efetuados não se fez necessária a instalação da interface gráfica. Nos roteadores foram ativadas uma

segunda interface de rede, necessária para sua finalidade, diferentemente dos *hosts* "servidor-operadora" e "cliente-instituicao" que utilizam apenas uma interface cada.

Para a efetiva comunicação, cada uma das *interfaces* das máquinas virtuais foi adicionada em sua respectiva rede, conforme o cenário de testes. A instalação do *host* "intruso" foi realizada com a distribuição *Ubuntu Desktop*, sendo necessário somente uma interface de comunicação com o objetivo de simular um atacante capturando pacotes trafegados no respectivo enlace.

Como esta pesquisa é direcionada apenas para o IPV6, não foi utilizado endereçamento IPv4. O procedimento adotado para a configuração dos endereços IPV6 em todas as máquinas virtuais foi o mesmo, justo por utilizarem a mesma distribuição Linux, sendo atribuídos através de seu arquivo de configuração.

Para os roteadores, em cada, foram atribuídos endereços em ambas suas *interfaces* de rede de acordo com o cenário de testes já apresentado, bem como ativação da configuração de encaminhamento de pacotes IPV6 permitindo que o *host* atue na função de roteador. No *host* "intruso" não foi atribuído endereçamento, pois foi utilizada sua *interface* de rede em modo promíscuo, somente capturando pacotes que trafegaram durante todos os testes.

4.2. Testes de Segurança e Desempenho sem o uso do IPSec

A aplicação dos testes de segurança consistiu na análise de tráfego entre os *hosts* "servidor-operadora" e "cliente-instituicao", através da ferramenta Wireshark. Para tanto, foi gerado tráfego ICMPv6.

Para realizar os testes de desempenho foi utilizada a ferramenta *Iperf*, aplicando como métrica o tempo em que arquivos de 100, 300 e 900MB levaram para ser transferidos do *host* "servidor-operadora" para o *host* "cliente-instituicao", sem o mecanismo IPSec.

4.3. Testes de Segurança e Desempenho Utilizando o IPSec

Nesta etapa, primeiramente foi necessário realizar a instalação e configuração da solução StrongSwan, bem como a criação de certificado digital, chaves pública e privada, afim de estabelecer um túnel entre os roteadores. A instalação da solução foi realizada no "roteador-operadora" e "roteador-instituicao" de forma igual.

Após a instalação e configuração, efetivou-se o túnel IPSec entre os roteadores. Logo, iniciaram-se os mesmos testes de segurança efetuados anteriormente sem a implementação do IPSec, porém, agora com o IPSec ativado. Também foi utilizado o *host* "intruso" e auxílio da ferramenta Wireshark para análise do tráfego ICMPv6 gerado.

Para os testes de desempenho, foram repetidos os testes efetuados anteriormente sem o uso do IPSec, porém agora, com o túnel implementado.

5. Resultados e Discussões

Nos resultados dos testes de segurança sem o uso do IPSec, foi constatada uma segurança fraca, sendo possível capturar e visualizar as informações do tráfego comutado pelos roteadores, como endereços de origem e destino, protocolo, dentre outros.

Para os resultados dos testes efetuados com uso do IPSec, identificou-se uma grande segurança, pois todos os pacotes das camadas superiores foram encapsulados no pacote IPV6, como pode ser visto na Figura 2. A utilização desse mecanismo de

segurança, permitiu que toda a comunicação entre os roteadores fosse criptografada, não sendo possível visualizar a informação, e ainda, no caso do IPV6, descobrir a origem e destino final dos pacotes.

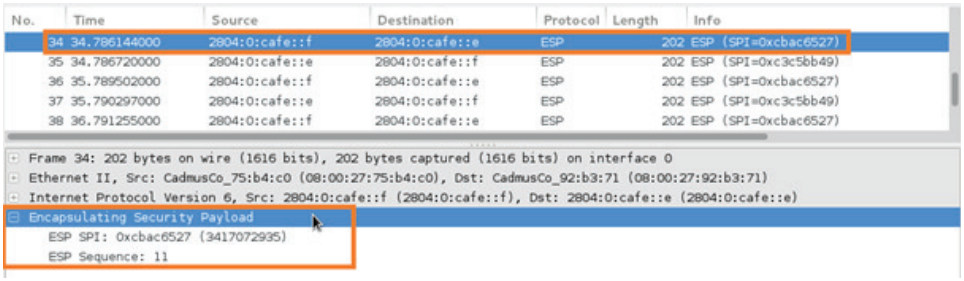

Figura 2. Tráfego encapsulado em camada de rede – Protocolo IPV6
Fonte: dos autores

Na questão do desempenho, os resultados comparativos do tempo da transferência dos arquivos são apresentados nas Figuras 3 e 4. Os pacotes que não utilizaram o IPSec implementado tiveram um melhor desempenho em relação aos pacotes que o utilizaram.

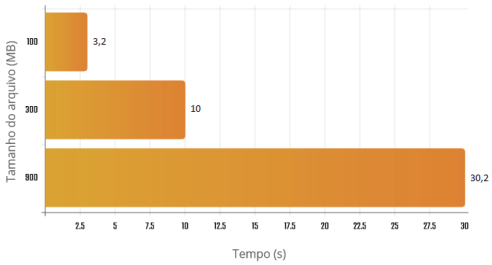

Figura 3. Desempenho sem IPSec
Fonte: dos autores

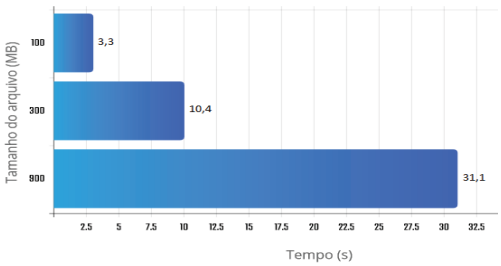

Figura 4. Desempenho com IPSec
Fonte: dos autores

Após análise utilizando a ferramenta Wireshark, foi identificado que na transferência utilizando IPSec houve um acréscimo de pacotes com média aproximada de 9,2%, sendo este o motivo da perda no desempenho em relação a comunicação sem o IPSec. A Tabela 2 apresenta o quantitativo de pacotes transferidos.

Tabela 2. Pacotes transferidos

	Quantidade de pacotes transferidos	
Tamanho do arquivo (MB)	**Sem IPSec**	**Com IPSec**
100	4.450	4.625
300	13.780	15.258
900	43.383	47.121

6. Considerações Finais

Este trabalho avaliou o uso do protocolo IPSec em modo túnel sobre redes IPV6. Essa associação do IPSec com IPV6 é o que há de mais novo em relação a questão de tunelamento feito na camada de rede da pilha de protocolos TCP/IP.

Os testes de segurança mostraram que o IPSec, implementado em modo túnel sobre redes IPV6, encapsula o pacote original em outro pacote IPV6, garantindo as redes trocarem informações de maneira segura.

Nos testes de desempenho efetuados foi constatado que a implementação do IPSec gera um pequeno atraso na transferência de arquivos entre os hosts utilizados com relação a não utilização dessa tecnologia. Esse retardo torna-se desprezível, pois o uso do IPSec proporciona uma camada muito grande de segurança para a proteção das informações, com pouco tempo de processamento.

Por fim, a utilização do IPSec modo túnel em redes IPV6 proporciona segurança das informações em um nível elevado, se comparado a sistemas que não a utilizem, sendo indicada sua implementação entre as operadoras e instituições clientes das mesmas, ou em sistemas que requeiram maior segurança a nível de rede, garantindo um canal seguro de comunicação a nível de camada de rede.

Para trabalhos futuros, poderiam ser exploradas as possíveis vulnerabilidades no tunelamento IPSec em redes IPV6, com auxílio de ferramentas de intrusão e auditoria de sistemas.

Ainda, simular alguns ataques para tentar adquirir informações dos cabeçalhos do IPSec, discutidos por Bellovin, em Bellovin (1997).

Referências

Basso, Cristina. (2011) "Implementação do Ipsec integrado com o IPV6", Universidade Tecnológica Federal do Paraná, Pato Branco.

Bellovin, Steven M. (1997) "Probable Plaintext Cryptanalysis of the IP Security Protocols", AT&T Labs Research, USA, Florham Park, Nj.

Gledson, Elias; Lobato, Luis C. (2013) "Arquitetura e protocolo de rede TCP-IP", RNP/ESR, Rio de Janeiro, 2ª edição.

IPV6 (2018) "Wikimedia Foundation", https://pt.wikipedia.org/w/index.php?title=IPV6&oldid=51737736, Abril.

IPV6.br (2018) "Órgão Responsável Pela Disseminação do IPV6 no Brasil", http://IPV6.br, Março.

ISO/IEC 17799:2005 (2018) "Information Technology - Security Techniques - Code of Practice for Information Security Management", http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39612, Fevereiro.

Lacnic (2018) "Fases de Esgotamento do IPv4", http://www.lacnic.net/1077/3/lacnic/fases-de-esgotamento-do-ipv4, Setembro.

Nakamura, Emilio Tissato; Lício de Geus, Paulo (2007) "Segurança de Redes em Ambientes Corporativos", Novatec, São Paulo, 1ª edição.

Oliveira, Ricardo Sato de. (2012) "Estudo de Vulnerabilidade do IPSec em Redes IPV6", Centro Universitário Eurípedes, Marília.

Stallings, Willian (1998) "Information Security", A Secure Foundation for VPNs, March.

Tanenbaum, Andrew S. (2013) "Redes de Computadores", Elsevier, Rio de Janeiro, 4ª edição.