Avaliação de Desempenho em Nuvens Computacionais utilizando IPsec em conjunto com SR-IOV

Thiago R. M. Almeida, Ewerton R. Andrade, Bruno M. Barros e Marcos A. Simplicio Jr.

***Resumo*— A implementação de mecanismos de segurança de redes é essencial para proteger as comunicações em um cenário de computação em nuvem com múltiplos usuários, o que tem motivado o constante desenvolvimento de tecnologias de software e hardware para essa finalidade. Em termos de software, a utilização de protocolos de rede tradicionais, como o IPsec (Internet Protocol Security), pode fornecer isolamento lógico para pacotes enquanto eles atravessam a infra-estrutura de rede do provedor da nuvem. Mais recentemente, soluções de virtualização assistida por hardware, como o Single Root I/O Virtualization (SR-IOV), também apareceram como potenciais ferramentas para melhorar o isolamento físico para pacotes de máquinas virtuais executadas em um mesmo ambiente, além de melhorar o desempenho de rede observado por elas. Embora a combinação dessas tecnologias seja recomendada para garantir que os dados dos usuários da nuvem possam trafegar de forma segura e confiável, o custo computacional resultante pode dificultar seu uso em aplicações de desempenho crítico. Neste trabalho, tendo como objetivo analisar os potenciais impactos dessas tecnologias na nuvem, é avaliado o desempenho do IPsec combinado com SR-IOV em alguns cenários de rede representativos.**

***Palavras-Chave*— nuvem; desempenho; segurança; IPsec; SR-IOV.**

***Abstract*— The deployment of network security mechanisms is essential to protect the communications in multi-tenant cloud computing environments, and many software and hardware-based technologies exist for this purpose. On the software front, the use of traditional network protocols such as IPsec (Internet Protocol Security) can provide logical isolation for packets from each tenant as they traverse the cloud provider's network infrastructure. On the hardware front, recent solutions such as Single Root I/O Virtualization (SR-IOV) have appeared as tools for improving isolation of packets from virtual machines sharing a physical host, potentially also improving their networking performance. Even though the combination of these technologies is recommended to ensure that the tenants' data can be transferred securely and reliably within the cloud, the resulting computational overhead may hinder their suitability in performance-critical applications. In this article, aiming to shed some light on the potential impacts of these technologies in the cloud, we evaluate the performance of IPsec combined with SR-IOV in some representative scenarios.**

***Keywords*— cloud; performance; security; IPsec; SR-IOV.**

I. Introdução

A computação em nuvem é um conceito que está em expansão atualmente, consistindo no provisionamento sob demanda de recursos computacionais, como armazenamento, processamento de dados, conectividade, plataformas, aplicações e serviços através da Internet [16]. A segurança dos serviços provisionados nesse tipo de ambiente é essencial para que os dados dos usuários sejam protegidos contra ataques, sejam eles realizados por usuários internos ao sistema ou por intrusos tentando interceptar informações ou comprometer o serviço oferecido. Assim, é necessário adotar mecanismos de segurança de acordo com as vulnerabilidades e aplicações envolvidas [7]. Em especial, dada a natureza compartilhada da nuvem, é importante garantir o isolamento entre máquinas virtuais (*virtual machines* – VMs) que utilizam a infraestrutura oferecida, de modo que as comunicações de cada usuário fiquem aproximadamente tão protegidas quanto estariam em um ambiente dedicado [1].

Existem diversos mecanismos tradicionais para prover *isolamento lógico* para comunicações realizadas em ambientes com hardware compartilhado, como é o caso da própria Internet. Especificamente na camada de rede, é amplamente utilizado o Internet Protocol Security (IPsec) [11] para prover serviços de cifração e autenticação. Como resultado, mesmo que todas as comunicações em um host físico passem por um switch compartilhado, (configuração padrão em soluções de nuvem, como o OpenStack [21]), a subversão do mesmo não permitiria ao atacante obter informações sigilosas ou modificar o conteúdo dos pacotes protegidos pelo IPsec. Entretanto, não se tem a mesma disponibilidade de soluções para prover *isolamento físico* das comunicações entre VMs executadas em um mesmo servidor e compartilhando uma mesma interface de rede. Neste caso, mesmo usando soluções que garantam isolamento lógico, uma VM que consiga burlar eventuais mecanismos de limitação de tráfego implementados no servidor poderia atacar a qualidade das comunicações de VMs alocadas na mesma interface de rede. Este tipo de ataque pode ser prevenido ao se implementar tecnologias como o *Single Root Input/Output Virtualization* (SR-IOV) [12], que provê o isolamento entre os recursos de rede de VMs compartilhando a mesma máquina física. Adicionalmente, o SR-IOV potencialmente eleva o desempenho de rede das VMs que dele se utilizam, pois provê uma conexão mais direta entre as VMs e a interface de rede física no servidor, removendo do caminho de tratamento dos pacotes camadas de abstração como o hipervisor e switches virtuais.

Embora a introdução dessas tecnologias de segurança em ambientes de nuvem seja recomendada para prover maior isolamento das comunicações entre VMs de diferentes usuários,

Thiago R. M. Almeida, Ewerton R. Andrade, Bruno M. Barros e Marcos A. Simplicio Jr. Escola Politécnica, Universidade de São Paulo, São Paulo-SP, Brasil, E-mails: talmeida@larc.usp.br, eandrade@larc.usp.br, bbarros@larc.usp.br, mjunior@larc.usp.br.

há que se considerar também o custo computacional envolvido na sua utilização, tanto em termos de utilização de banda como de processamento de dados [8]. Assim, é importante entender o impacto de tais mecanismos em aplicações em que desempenho é um fator crítico. Em especial, é interessante entender até que ponto as perdas de desempenho do protocolo IPsec podem ser compensadas pelos eventuais ganhos de desempenho obtidos com o SR-IOV. Para isso, é adotada uma abordagem experimental utilizando o OpenStack como plataforma de testes.

O resto deste documento está assim organizado. A Seção II discute as soluções de segurança que são alvo do presente estudo, IPsec e SR-IOV, e apresenta os trabalhos relacionados ao presente estudo. A Seção III apresenta e descreve os cenários utilizados para realizar a análise de desempenho das tecnologias propostas. A Seção IV descreve a obtenção dos dados utilizados para realizar a avaliação de desempenho, os quais são analisados na Seção V. Finalmente, a Seção VI apresenta as considerações finais do trabalho.

II. Tecnologias para isolamento físico e lógico na nuvem

Nesta seção são apresentadas em maiores detalhes as duas tecnologias que são objeto do presente estudo, o protocolo IPsec e o SR-IOV. São também discutidos trabalhos da literatura que, como o presente estudo, avaliam o seu desempenho.

A. IPsec

O protocolo IPsec opera na camada de rede, fornecendo os serviços de autenticação e cifração de pacotes na comunicação entre dois elementos quaisquer de uma rede (e.g., roteadores ou máquinas de usuários finais) [11]. Assim, o IPsec oferece proteção contra ameaças à confidencialidade, autenticidade e integridade de dados, como escutas e ataques de repetição [9], garantindo o devido isolamento lógico entre os canais de comunicação.

Para prover tais serviços, o IPsec estabelece chaves criptográficas simétricas entre os elementos participantes de uma sessão, o que pode ser feito manualmente ou via protocolos como o *Internet Key Exchange* versão 2 (IKEv2) [10], criando-se uma associação de segurança entre as partes. Essas chaves são então utilizadas nos protocolos *Authentication Header* (AH), responsável pela autenticação dos pacotes, e *Encapsulating Security Payload* (ESP), que fica responsável pela sua cifração.

B. SR-IOV

A interface SR-IOV [12] é uma extensão da especificação do barramento PCI-Express (PCIe) tradicional. Basicamente, tal tecnologia permite que um dispositivo, como um adaptador de rede virtual, obtenha acesso independente aos recursos do barramento PCIe no caso de uma comunicação *inter-host*; isso possibilita que o tráfego de rede flua diretamente entre a interface física e os elementos virtualizados [3]. Esta característica potencialmente permite ganhos consideráveis de desempenho na transferência de dados entre VMs e máquinas externas ao servidor no qual tais VMs são executadas. Afinal, a comunicação neste caso não depende de elementos como o hipervisor de VMs ou um switch virtual compartilhado entre elas. Adicionalmente, obtém-se melhor isolamento dos recursos físicos de rede utilizados pelas diversas VMs, protegendo os dados transmitidos contra ataques realizados por VMs maliciosas no mesmo servidor.

Deve-se notar, entretanto, que em comunicações *intra-host* o desempenho não é otimizado porque o pacote precisa ser enviado para a interface de rede física antes de ser direcionado para o destino quando poderia ser redirecionado diretamente pelo switch virtual onde já estão ligadas ambas as VMs de origem e destino.

C. Trabalhos relacionados

A análise de desempenho utilizando canais IPsec é um tema abordado em diversos estudos. Exemplos incluem estudos anteriores à popularização de tecnologias de computação em nuvem, como a análise comparativa de desempenho dos algoritmos HMAC-MD5 e HMAC-SHA1 [18] em conjunto com o IPsec [4], o estudo do IPsec em aplicações móveis baseadas em IPv6 [5], ou estudos sobre o atraso no tempo de resposta e saturação de rede ao utilizar o IPsec [22], [20], [15]. Já um exemplo mais recente é dado em [14], que verifica a viabilidade de se utilizar IPsec para a realização de videoconferências, trabalho que usa uma abordagem de análise similar à proposta no presente trabalho. A conclusão é que a utilização de túneis IPsec aumenta a utilização da banda consideravelmente, levando a uma possível saturação resultante da utilização desse mecanismo de segurança. Nenhum desses estudos apresenta, entretanto, uma análise do impacto do IPsec no ambiente de nuvem, nem discute sua utilização em conjunto com tecnologias de virtualização assistida por hardware (VAH), como é o caso do SR-IOV.

Já alguns trabalhos recentes têm se voltado especificamente à avaliação de técnicas de VAH [6], [13], [3] implementadas na nuvem, incluindo SR-IOV. Em todos os casos, os testes realizados mostram que tais tecnologias melhoram significativamente o desempenho de rede em ambientes virtualizados. Os resultados positivos obtidos nesses estudos servem como motivação adicional para o presente trabalho, que tem como objetivo verificar até que ponto tais ganhos são capazes de compensar os custos do IPsec quando executado no ambiente virtualizado que caracteriza aplicações de computação em nuvem.

III. Cenários de Aplicação

A seguir são descritos os cenários de aplicação utilizados para avaliar o desempenho dos mecanismos de segurança providos pelo IPsec em conjunto com a tecnologia SR-IOV. Eles foram elaborados sobre o sistema de computação em nuvem OpenStack, utilizando o switch virtual Open vSwitch (OvS) [19] para interligar VMs e uma interface de rede (*Network Interface Controller* – NIC) para realizar a comunicação entre as máquinas físicas. Assim, esses cenários possibilitam uma análise da comunicação entre VMs instanciadas em diferentes máquinas físicas executando o Openstack.

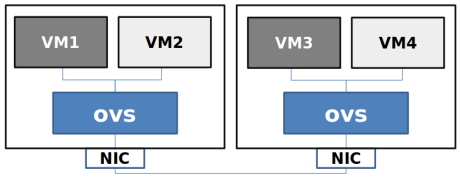

Fig. 1
CENÁRIO DE REFERÊNCIA.

- **Cenário de referência**
  O cenário de referência, ilustrado na Figura 1, implementa a comunicação entre VMs localizadas em máquinas físicas distintas utilizando apenas o OvS. A realização dos testes considera a transferência de pacotes de dados entre VM1 e VM3.
  Este cenário não utiliza mecanismos de segurança e tem como objetivo principal permitir sua comparação com os demais cenários que implementam SR-IOV e IPsec.
- **Cenário IPsec**

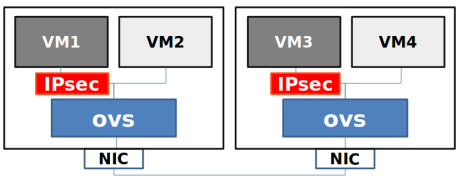

Fig. 2
CENÁRIO IPSEC

O Cenário IPsec, ilustrado na Figura 2, aplica o protocolo de segurança IPsec na comunicação entre as máquinas virtuais VM1 e VM3 e utiliza o switch virtual OvS para interligar VMs localizadas dentro de uma mesma máquina física. Dessa forma, considera-se a existência de uma associação de segurança entre o emissor e o receptor para cifrar as mensagens (usando AES-256 [17]) e autenticá-las (usando HMAC-SHA2 [18]).

- **Cenário SR-IOV**

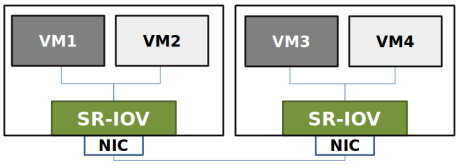

Fig. 3
CENÁRIO SR-IOV

No cenário SR-IOV, ilustrado na Figura 3, há a comunicação direta entre VM1 e VM3 através de suas respectivas portas de rede físicas. Isso leva ao isolamento lógico e físico entre VMs instanciadas em uma mesma máquina real, prevenindo que VMs maliciosas consumam excessivamente recursos de hardware para exaurir a disponibilidade dos mesmos para VMs vizinhas Neste caso, não é utilizado um switch virtual na transferência de dados.

- **Cenário IPsec com SR-IOV**

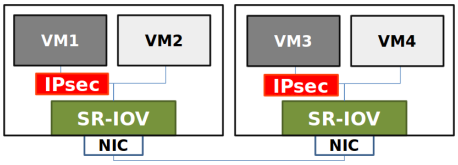

Fig. 4
CENÁRIO IPSEC COM SR-IOV

O cenário IPsec com SR-IOV combina a aplicação do protocolo IPsec com o encaminhamento de pacotes via SR-IOV entre VM1 e VM3, conforme ilustrado na Figura 4. Essa combinação busca prover isolamento de recursos físicos e lógicos através da aplicação do SR-IOV e a autenticação e cifração de pacotes através da utilização dos protocolos que compõem o IPsec.

IV. OBTENÇÃO DE DADOS

A análise e avaliação dos cenários de aplicação apresentados requer que seja primeiramente feito o levantamento dos tempos de resposta referentes a cada mecanismo utilizado para compor os cenários apresentados com o intuito de calcular suas respectivas taxas de processamento de pacotes (TP). Mais precisamente, o procedimento adotado foi a comparação entre os tempos de resposta obtidos de um cenário sem qualquer mecanismo de segurança (i.e., "cenário de referência") e um cenário onde o respectivo mecanismo é implementado (i.e., "cenário IPsec" e "cenário SR-IOV"). Para isso, os tempos de resposta foram coletados por meio da implementação dos cenários descritos na Seção III. Adicionalmente, também foi criado um cenário chamado Conexão Simples (CS), que consiste na conexão entre as máquinas físicas nas quais as VMs estão instanciadas, permitindo a comparação de um cenário que não utiliza virtualização com cenários que utilizam um switch virtual para a conexão entre VMs. Dessa forma, é possível calcular a latência adicional causada pela utilização do OvS, IPsec e SR-IOV isoladamente para a obtenção da taxa de processamento de cada mecanismo em cada um dos cenários que os utilizam.

Os tempos de resposta mostrados na Tabela I foram medidos em cada cenário como a mediana de 20 amostras de pacotes ICMP considerando dois cenários: sem saturação (TR) da capacidade de processamento de pacotes, no qual são usados pacotes com o tamanho padrão de 64 bytes da ferramenta *ping*; e com saturação do processamento (TRS), em que a comunicação é realizada utilizando pacotes de 65515 bytes, o máximo permitido pela ferramenta. Esta abordagem foi adotada porque o desvio padrão das medidas dos tempos de resposta foi superior a 2% em relação à média em todos os cenários, enquanto o aumento no número de amostras não diminuiu consideravelmente esse valor. Assim, o uso da mediana ao invés da média das amostras mostrou-se mais adequado para reduzir a sensibilidade da análise a valores extremos. Dessa forma, devido à utilização da mediana, o cálculo de dispersão foi realizado considerando a diferença entre o primeiro e o terceiro quartis do conjunto de medidas [2], resultando na

amplitude do intervalo interquartil (IQ), a qual é indicada na Tabela I. Assim, com o cálculo da diferença dos tempos de resposta entre cenários TR e TRS, é possível identificar a latência incorrida por cada mecanismo individualmente e, consequentemente, as taxas de processamento de pacotes em cada elemento com e sem saturação, como mostrado nas Tabelas II, III e IV.

A Tabela V mostra os resultados da conversão feita para transformar largura de banda (LB) em taxa de transmissão de pacotes em cada cenário durante os testes. Novamente, são considerados dois cenários: o primeiro utilizando a transferência de pacotes com tamanho padrão de 64 bytes (TT) e o segundo usando pacotes com o tamanho máximo de 65515 bytes (TTS) com a finalidade de saturar a capacidade de processamento para os pacotes na VM responsável pelo recebimento dos pacotes. Também cabe notar que a largura de banda de cada um dos cenários foi obtida utilizando a ferramenta de análise de desempenho *iperf* entre as VMs envolvidas, configurado para usar pacotes de 64 bytes em cada caso. Esse conjunto de métricas permite uma análise razoavelmente holística das ferramentas em questão: a taxa de transmissão de pacotes de cada cenário é utilizada para realizar a comparação entre os cenários de aplicação descritos na seção III, enquanto o cálculo da taxa de processamento em cada mecanismo utilizado, como mostrado nas Tabelas II, III e IV, permite uma comparação entre os elementos que compõem cada um desses cenários.

Finalmente, com relação à avaliação do cenário IPsec, é interessante observar que a utilização do algoritmo HMAC-SHA2 com blocos de 512 bits no *Authentication Header* mostrou-se adequada, pois o mesmo proporciona uma segurança maior e um desempenho similar ao algoritmo MD5. Mais precisamente, o tempo de resposta do cenário IPsec utilizando o algoritmo HMAC-MD5 foi de $1,060ms$, portanto apenas $0,045ms$ maior que o mesmo cenário utilizando HMAC-SHA2, que apresentou um tempo de $1,015ms$, mas ainda dentro do desvio padrão obtido, de $0,097ms$.

TABELA I

TEMPO DE RESPOSTA DE PACOTES NA REDE

Cenário	TR (ms)	IQ (ms)	TRS (ms)	IQ (ms)
Referência	0,910	0,040	3,422	0,131
IPsec	1,044	0,065	24,509	0,956
SR-IOV	0,353	0,012	1,719	0,125
IPsec+SR-IOV	0,478	0,010	24,040	0,740

TABELA II

CÁLCULO DA TAXA DE PROCESSAMENTO DO PROTOCOLO IPSEC

Cenário	TR (ms)	TRS (ms)
Referência	0,910	3,422
IPsec	1,044	24,509
Diferença	0,134	21,087
	t=0,134/2=0,067 e **TP=1/t=14,964 pacotes/ms**	t=21,087/2=10,543 e **TP=1/t=0,095 pacotes/ms**

V. ANÁLISE DOS DADOS OBTIDOS

Primeiramente, é interessante notar a existência de dois potenciais gargalos no sistema, o protocolo IPSec e o OvS.

TABELA III

CÁLCULO DA TAXA DE PROCESSAMENTO REFERENTE AO OPEN VSWITCH

Cenário	TR (ms)	TRS (ms)
CS	0,261	1,547
Referência	0,910	3,422
Diferença	0,649	1,875
	t=0,649/2=0,325 e **TP=1/t=3,080 pacotes/ms**	t=1,875/2=0,938 e **TP=1/t=1,066 pacotes/ms**

TABELA IV

CÁLCULO DA TAXA DE PROCESSAMENTO DA INTERFACE SR-IOV

Cenário	TR (ms)	TRS (ms)
CS	0,261	1,547
SR-IOV	0,353	1,719
Diferença	0,092	0,172
	t=0,092/2=0,050 e **TP=1/t=21,645 pacotes/ms**	t=0,172/2=0,086 e **TP=1/t=11,635 pacotes/ms**

Ao avaliar as taxas de processamento de pacotes (Tabelas II, III e IV), pode-se observar que o IPsec é o principal responsável pela perda de desempenho nos cenários onde é aplicado e há a saturação da capacidade de processamento. Mais precisamente, ao comparar as taxas de processamento com saturação nas Tabelas II e III, percebe-se que o IPsec apresenta uma taxa de processamento de 0,095 pacotes/ms, apenas 8.9% do obtido com o OvS, de 1,066 pacotes/ms. Esse fato pode ser explicado pela elevada carga de dados que deve ser cifrada pelo IPsec nessa situação. Por outro lado, quando a capacidade de processamento de pacotes não é saturada, o maior processamento incorrido pelo uso do IPSec não causa grandes atrasos nos pacotes, sendo o OvS o principal fator que leva à formação de filas nesse caso. Especificamente, conforme mostrado nas Tabelas II e III, a taxa de processamento do OvS quando não há saturação é de 3,080 pacotes/ms, apenas 20,6% da taxa obtida com o protocolo IPsec. Por fim, conforme mostrado na Tabela IV, o SR-IOV é de fato uma ferramenta interessante para elevar a taxa de processamento de pacotes em uma rede virtualizada.

Já a análise das taxas de transferência de pacotes mostrada na Tabela V revela que saturar o processamento tem elevado impacto na taxa total, que chega a cair cerca de 1000 vezes em todos os cenários; porém, como essa influência é muito semelhante para todos os cenários, ela é de pouco interesse para uma análise comparativa entre eles, de modo que a discussão a seguir se aplica a ambos. Novamente, o uso do SR-IOV na comunicação entre VMs em vez do OvS revela-se ao menos ligeiramente vantajoso, dado que o cenário SR-IOV apresenta uma taxa de transferência 5% superior àquela obtida no cenário de Referência. Isso se deve à característica da interface SR-IOV de fornecer acesso independente à interface

TABELA V

TAXA DE TRANSFERÊNCIA DE PACOTES NA REDE

Cenário	LB(Mb/s)	TT(p/s)	TTS(p/s)
Referência	896	1750000	1709
IPsec	314	613280	599
SR-IOV	943	1841800	1799
IPsec+SR-IOV	371	724610	707

de rede física para cada VM envolvida, diminuindo o atraso associado à utilização de um switch virtual. Entretanto, o SR-IOV não é capaz de camuflar a considerável queda de desempenho resultante do uso de IPSec: a queda na taxa de transferência quando o IPSec é utilizado com e sem o SR-IOV é, respectivamente, 35% e 41% daquela observada no cenário de Referência.

Finalmente, o SR-IOV também se mostra eficaz na tarefa de reduzir os tempos de resposta, estando o processamento saturado ou não: tais tempos chegam, respectivamente, a 39% e 50% daqueles obtidos no cenário de Referência. Porém, apenas no caso em que o processamento não está saturado o SR-IOV é capaz de camuflar o aumento no tempo de resposta ocasionado pelo IPSec: enquanto o IPSec puro leva a um atraso 14% superior ao do cenário de referência, esse tempo torna-se 50% da referência quando o IPSec é combinado com o SR-IOV. Já quando há saturação, o tempo de resposta do IPSec continua cerca de 700% daquele do cenário de referência, independentemente do uso do SR-IOV.

VI. Conclusões

A introdução de mecanismos de segurança em ambientes de computação em nuvem é essencial para que as redes virtuais de diferentes VMs sejam isoladas lógica e/ou fisicamente entre si, reduzindo interferências entre elas (e.g., interceptação ou perda de desempenho em todas as VMs devido a elevado volume de tráfego em uma delas). Dentre eles, tem destaque o uso do protocolo IPsec, para isolamento lógico de redes, e do SR-IOV, para isolar fisicamente interfaces de rede e também permitir maior desempenho das comunicações. Este trabalho teve como objetivo avaliar o quanto o uso conjunto dessas ferramentas afeta, positiva ou negativamente, o desempenho de redes virtuais que delas se utilizam. Para isso, foi analisada uma série de cenários experimentais, considerando-se como métricas tempo de resposta e taxa de transferência de pacotes.

A avaliação dos resultados obtidos nos permite observar que a utilização da tecnologia SR-IOV normalmente melhora de forma considerável a taxa de transferência de pacotes e o tempo de resposta da rede, em especial se comparada com a tradicional utilização do OvS para a conexão entre VMs. Já o IPsec proporciona um gargalo relevante em todos os cenários nos quais é utilizado, já que os cenários IPsec e IPsec+SR-IOV possuem taxas de transferência de pacotes inferiores aos demais em todas as situações analisadas, em especial quando há saturação da capacidade de processamento. De qualquer forma, o uso do SR-IOV ao invés de um switch virtual para comunicações entre hosts é interessante, em especial quando segurança é um requisito, dado que ele consegue mascarar o maior tempo de resposta causado pelo IPsec em cenários onde o processamento de pacotes é baixo. Por outro lado, cabe observar que o SR-IOV não é uma tecnologia voltada a comunicações *intra-host*, pois sua utilização nesse caso exigiria que os pacotes fossem enviados para a interface de rede física do host antes de serem direcionados para o destino; neste caso, seria mais adequado redirecionar os pacotes diretamente via um switch virtual no qual já estejam ligadas as VMs de origem e destino (potencialmente utilizando-se também IPsec para isolamento lógico da rede virtual interna).

Agradecimentos

Este trabalho teve o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), processos 473916/2013-4 e 305350/2013-7, e também do Centro de Inovação, Ericsson Telecomunicações S.A., Brasil.

Referências

[1] B. Barros, L. Iwaya, M. Simplicio, T. Carvalho, A. Méhes, and M. Näslund. Classifying security threats in cloud networking. In *5th Int. Conf. on Cloud Computing and Services Science (CLOSER'15)*, pages 214–220, 2015.

[2] Edite Manuela da GP Fernandes. Estatística aplicada. *Braga: American Mathematical Society*, 1999.

[3] Y. Dong, X. Yang, J. Li, G. Liao, K. Tian, and H. Guan. High performance network virtualization with SR-IOV. *Journal of Parallel and Distributed Computing*, 72(11):1471–1480, 2012.

[4] O. Elkeelany, M. Matalgah, K. Sheikh, M. Thaker, G. Chaudhry, D. Medhi, and J. Qaddour. Performance analysis of IPSec protocol: encryption and authentication. In *IEEE Int. Conf. on Communications (ICC'02)*, volume 2, pages 1164–1168. IEEE, 2002.

[5] Z. Faigl, P. Fazekas, S. Lindskog, and A. Brunstrom. Performance analysis of IPsec in mobile IPv6 scenarios. In *Mobile and Wireless Communications Summit*, pages 1–5. IEEE, 2007.

[6] R. Ganesan, Y. Murarka, S. Sarkar, and K. Frey. Empirical study of performance benefits of hardware assisted virtualization. In *Proc. of the 6th ACM India Computing Convention*, pages 1:1–1:8. ACM, 2013.

[7] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1):1–13, 2013.

[8] Z. He and G. Liang. Research and evaluation of network virtualization in cloud computing environment. In *3rd Int. Conf. on Networking and Distributed Computing (ICNDC)*, pages 40–44. IEEE, 2012.

[9] K. Ishimura, T. Tamura, S. Mizuno, H. Sato, and T. Motono. Dynamic IP-VPN architecture with secure IPsec tunnels. In *8th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT)*, pages 1–5. IEEE, 2010.

[10] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen. *RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)*. Internet Engineering Task Force (IETF), 2014. `tools.ietf.org/html/rfc7296`.

[11] S. Kent and K. Seo. *RFC 4301: Security Architecture for the Internet Protocol*. Internet Engineering Task Force (IETF), 2005. `tools.ietf.org/html/rfc4301`.

[12] P. Kutch. PCI-SIG SR-IOV primer: An introduction to SR-IOV technology. Technical Report 321211–002, Intel, 2011.

[13] J. Liu. Evaluating standard-based self-virtualizing devices: A performance study on 10 GbE NICs with SR-IOV support. In *IEEE Int. Symp. on Parallel & Distributed Processing*, pages 1–12. IEEE, 2010.

[14] R. Malik and R. Syal. Performance analysis of IP security VPN. *International Journal of Computer Applications*, 8(4):0975, 2010.

[15] S. Meenakshi and S. Raghavan. Impact of IPSec overhead on web application servers. In *Int. Conf. on Advanced Computing and Communications (ADCOM'06)*, pages 652–657. IEEE, 2006.

[16] P. Mell and T. Grance. The NIST definition of cloud computing. Technical report, National Institute of Standards and Technology, 2011.

[17] NIST. *FIPS 197 – Advanced Encryption Standard (AES)*. National Institute of Standards and Technology, November 2001. `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.

[18] NIST. *FIPS 198-1 – The Keyed-Hash Message Authentication Code (HMAC)*. National Institute of Standards and Technology, July 2008. `csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf`.

[19] B. Pfaff, J. Pettit, K. Amidon, M. Casado, T. Koponen, and S. Shenker. Extending networking into the virtualization layer. In *Proc. of Workshop on Hot Topics in Networks (HotNets-VIII)*, 2009.

[20] J. Raissi. IPsec offload performance. In *Proc. of SoutheastCon 2004*, pages 222–228. IEEE, 2004.

[21] O. Sefraoui, M. Aissaoui, and M. Eleuldj. OpenStack: toward an open-source solution for cloud computing. *International Journal of Computer Applications*, 55(3):38–42, 2012.

[22] C. Shue, M. Gupta, and S. Myers. IPsec: Performance analysis and enhancements. In *IEEE Int. Conf. on Communications (ICC'07)*, pages 1527–1532. IEEE, 2007.