Firewalls em Redes Definidas por Software: Estado da Arte

Maurício M. Fiorenza[1], **Diego Kreutz**[1]

[1]Laboratório de Estudos Avançados (LEA)
Mestrado Profissional em Engenharia de Software (MPES)
Universidade Federal do Pampa (UNIPAMPA)

{mauriciofiorenza,diegokreutz}@unipampa.edu.br

Resumo. *Redes Definidas por Software, ou SDNs, representam um novo paradigma onde o controle da rede é logicamente centralizado. Este novo paradigma vem transformando o modo de pensar e gerir as redes, incluindo mudanças significativas na engenharia de tráfego e controle da topologia da rede, por exemplo. Serviços de segurança, como firewalls, também podem tirar proveito da flexibilidade oferecida pelas SDNs, como de fato de ocorrido. O objetivo deste trabalho é apresentar e discutir uma revisão do estado da arte sobre firewalls em SDNs, buscando identificar padrões que possibilitem classificar as soluções existentes quanto a sua arquitetura e modos de operação e, também, identificar oportunidades e desafios de pesquisa.*

1. Introdução

As redes definidas por software, ou SDN (*Software-Defined Networking*), representam um novo paradigma, uma alternativa, ao engessado território das redes de computadores, oferecendo maior flexibilidade, simplificação no gerenciamento e na escalabilidade das redes [Kreutz et al. 2014]. A maior flexibilidade permitiu que pesquisadores e empresas desenvolvessem novas funcionalidades e serviços numa velocidade muito maior, isto é, sem depender mais dos lentos processos de atualização e desenvolvimento de produtos por parte de um conjunto limitado de fabricantes de equipamentos de rede.

Em uma rede definida por software, o plano de controle é fisicamente separado do plano de dados, isto é, fica alocado em um dispositivo físico separado, mais conhecido como controlador, e não mais no próprio dispositivo de encaminhamento (e.g. switch). O controlador, implementado em software, é a entidade que define e instala as regras que os dispositivos do plano de dados devem aplicar aos fluxos de dados. Com isto, desenvolver um novo protocolo, ou mesmo um firewall, passa a ser uma tarefa de engenharia de software, ou seja, criar uma aplicação que irá executar junto ao controlador.

Estudos indicam que os mecanismos de segurança tradicionais são inadequados para proteger infraestruturas baseadas em redes definidas por software [Dixit et al. 2018]. De fato, as funções tradicionais de um firewall, baseadas em conjuntos de regras estáticas, não são o suficiente para atender demandas e características essenciais de SDNs, como granularidade, adaptabilidade e escalabilidade. Por exemplo, um firewall, em uma SDN, passa a ser uma aplicação com visão global da rede, podendo aplicar políticas nas bordas da rede em tempo real e não apenas de forma estática e em um único ponto central.

Além de uma breve conceituação de firewalls em redes tradicionais, as contribuições deste trabalho podem ser resumidas em: (a) caracterização e classificação de firewalls em SDNs; e (b) discussão de desafios de desenvolvimento e pesquisa.

2. Firewalls tradicionais

Firewalls são definidos como sistemas de software ou hardware que impõe políticas de controle de acesso entre redes. Um firewall tem como função principal proteger as redes privadas de ataques externos, filtrando o tráfego a partir de políticas pré-definidas [Ioannidis et al. 2000]. Os tipos mais comuns de firewalls são o filtro de pacotes, o firewall de estados, o firewall de aplicação e os firewalls de nova geração [Gouda and Liu 2005].

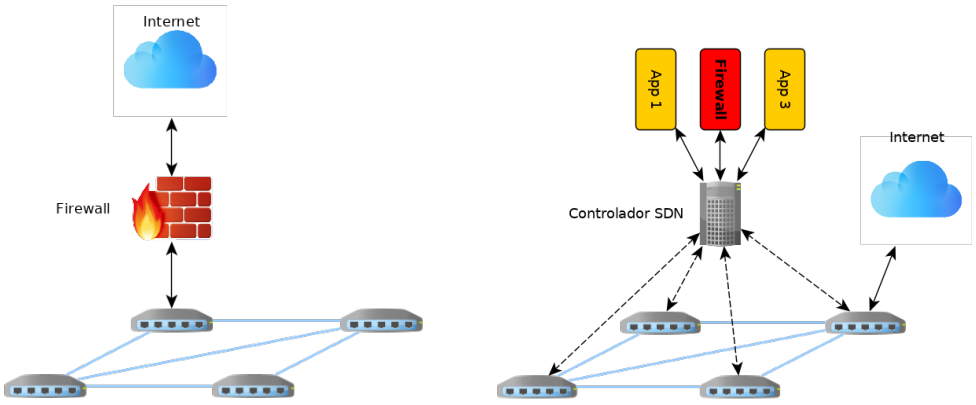
O **filtro de pacotes** é um mecanismo simples que analisa diferentes informações do cabeçalho do pacote para definir se ele será liberado ou não de acordo com as regras pré-estabelecidas. Um **firewall de estados** realiza a análise do tráfego buscando encontrar estados, ou seja, padrões permitidos segundo regras pré-estabelecidas. Os padrões são armazenados em tabelas de estados e são utilizados como parâmetro de controle dos fluxos de dados subsequentes. Já um **firewall de aplicação** é também conhecido como proxy por atuar na camada de aplicação. Isto permite a criação de regras específicas e de acordo com a aplicação. Finalmente, os **firewalls de nova geração** adicionam camadas extras de proteção aos firewalls de estados. A principal diferença é capacidade de controle na camada de aplicação, permitindo um grau de granularidade maior nas políticas de segurança.

Apesar da ampla utilização e do relativo sucesso, os firewalls tradicionais não atendem as demandas das novas redes, como as SDNs, onde a quantidade e a diversidade de equipamentos conectados e os novos desafios de segurança exigem novos tipos de políticas que são difíceis de serem implementadas nos firewalls atuais [Dixit et al. 2018]. Questões como flexibilidade, granularidade, desempenho, capacidade de identificar e bloquear novos malwares e necessidade de manutenção simplificada levam a academia e a indústria a propor e desenvolver novas soluções.

3. Firewalls em SDNs: flexibilidade e inovação

As SDNs oferecem a flexibilidade necessária para potencializar a inovação no que diz respeito a arquiteturas e recursos de firewalls [Satasiya et al. 2016]. Por exemplo, regras de filtragem podem ser aplicadas diretamente nos dispositivos de encaminhamento, na borda da rede, bloqueando o tráfego indesejado (ou malicioso) na origem. A Figura 1 ilustra um firewall tradicional e um baseado em SDN. Como pode ser observado, um firewall tradicional é tipicamente um dispositivo físico que fica localizado em um local específico da rede (e.g. entre a rede interna e a Internet). Já um firewall SDN é mais uma aplicação executando no controlador SDN [Dixit et al. 2018]. Entre as principais vantagens de um firewall SDN estão o acesso a informações cruciais da rede (como a topologia detalhada) e a possibilidade de aplicar, em tempo de execução, políticas de segurança em todos os dispositivos da rede gerenciados pelo controlador.

A Tabela 1 apresenta uma classificação de firewalls em SDNs considerando características e recursos como arquitetura, modo de operação, estado das conexões e protocolo utilizado. Como pode ser observado, a maioria dos firewalls são logicamente centralizados, reativos e *stateful*. Além disso, o protocolo predominante é o OpenFlow, com apenas uma exceção.



(a) Firewall tradicional (b) Firewall SDN

Figura 1. Firewalls tradicionais e SDN

Tabela 1. Classificação de firewalls SDN

	Arquitetura		Modo de operação		Estado da conexão		
Firewall SDN	Centralizada	Distribuída	Reativo	Proativo	Stateless	Stateful	Protocolo
Fireflow[Fiessler et al. 2018]		✓	✓	✓		✓	Openflow
FORTRESS[Caprolu et al. 2019]		✓	✓	✓		✓	Openflow
Firewall Floodlight[Morzhov et al. 2016]	✓		✓	✓	✓		Openflow
FlowGuard[Hu et al. 2014]	✓		✓		✓		Openflow
FlowTracker[Tran and Ahn 2016]	✓		✓			✓	Openflow
Firewall for POX[Othman et al. 2017]	✓		✓		✓		Openflow
RSF[Zerkane et al. 2016b]	✓		✓			✓	Openflow
PSF [Zerkane et al. 2016a]	✓		✓	✓		✓	Openflow
REFLO[Visoottiviseth et al. 2017]	✓		✓			✓	Openflow
SDFS[Zeineddine and El-Hajj 2018]	✓		✓	✓		✓	Openflow
SMPU-P4[Vörös and Kiss 2016]		✓	✓			✓	P4

Arquitetura

As arquiteturas dos firewalls estão intimamente ligadas à arquitetura e ao tipo de controlador SDN utilizado. A maioria dos firewalls é implementada como uma aplicação que utiliza os recursos de um controlador centralizado, caracterizando uma arquitetura centralizada. Neste tipo de arquitetura, todas as requisições são enviadas ao firewall para a tomada de decisão. Observando as políticas implementadas, o firewall gera as regras de fluxo a serem instaladas nos dispositivos do plano de dados. Tipicamente, as regras podem ser de três tipos: (i) permite o tráfego; (ii) bloqueia o tráfego; ou (iii) redireciona o tráfego para algum dispositivo específico (e.g. IDS, IPS).

Existem também os firewalls distribuídos, criados para lidar com desafios de desempenho, escalabilidade, entre outros [Caprolu et al. 2019, Fiessler et al. 2018]. Este tipo de arquitetura de firewall utiliza tecnologias como P4 ou plano de dados *stateful* para adicionar camadas de pré-processamento nos dispositivos de encaminhamento. Com isto, a aplicação do firewall, no controlador, é dispensada da análise e tomada de decisão nos casos mais simples. Um exemplo prático é o controle de acesso por porta, algo que pode ser processado diretamente na borda da rede, reduzindo o volume de tráfego no plano de controle e as demandas de processamento do controlador.

Modo de operação

Os firewalls SDN podem ser classificados em reativos e proativos. Os reativos são caracterizados pela execução de ações sob demanda, isto é, o firewall aplica as políticas de encaminhamento de tráfego a cada novo fluxo de dados na rede [Visoottiviseth et al. 2017]. Apesar de esta abordagem levar a uma maior segurança e um controle mais granular sobre o que acontece na rede, ela pode resultar em problemas de desempenho. Na prática, o firewall reativo acaba virando o gargalo da rede. Por exemplo, um firewall reativo centralizado, implementado como uma aplicação no controlador, pode resultar em um grande volume de requisições entre os dispositivos de encaminhamento e o controlador. Como consequência direta, podem ocorrer atrasos (latência) significativos no encaminhamento de todos os fluxos de dados que precisam ser analisados pelo firewall antes de seguir o seu curso.

Um firewall proativo é capaz de adicionar previamente regras de liberação e bloqueio de fluxos de dados nas tabelas de encaminhamento dos dispositivos do plano de dados [Zerkane et al. 2016a]. Por exemplo, regras simples, como as que definem a liberação do tráfego de protocolos como o HTTP e o ICMP, podem ser instaladas de forma proativa no plano de dados. Com isto, nenhum dos novos fluxos de dados HTTP e ICMP necessitam passar pelo firewall para análise, evitando assim a latência de comunicação do plano de controle e o tempo necessário para a instalação das regras no plano de dados. Entretanto, estas regras, instaladas de forma proativa, ficam potencialmente mais suscetíveis a vulnerabilidades e ataques ao plano de dados (e.g. *overflow* das tabelas de fluxo), podendo, inclusive, levar ao comprometimento de serviços sem o conhecimento da aplicação de firewall.

Estado das conexões

De forma análoga aos firewalls tradicionais, soluções baseadas em SDN também podem ser classificadas com relação à manutenção dos estados das conexões. Um firewall *stateless* não tem a capacidade de manter os estados das conexões, isto é, a cada novo fluxo o firewall toma uma nova decisão. Isto torna o firewall mais simples de implementar, mas aumenta consideravelmente o custo computacional uma vez que todo pacote deve ser analisado pelo firewall.

Por outro lado, um firewall *stateful* é capaz de detectar e monitorar os estados de todos os fluxos de dados da rede, armazenando informações como hosts envolvidos e parâmetros da conexão [Tran and Ahn 2016]. Para isto, o firewall precisa acessar dados da camada de transporte, o que demanda uma comunicação frequente entre o plano de controle e o plano de dados. Devido a esses e outros motivos, a implementação de um firewall *stateful* precisa levar em consideração as potenciais sobrecargas no plano de dados e no controlador.

Protocolos

Como a maioria dos firewalls é apenas uma aplicação executando no plano de controle, a comunicação com os dispositivos de encaminhamento, para instalação e aplicação das regras no plano de dados, é determinada pelo controlador. Atualmente, o protocolo mais aceito e utilizado na academia e na indústria é o OpenFlow [McKeown et al. 2008, ONF 2019], um protocolo de código aberto desenvolvido especificamente para atender os conceitos e a flexibilidade introduzida por redes definidas por software.

O surgimento de tecnologias como o P4 [Bosshart et al. 2014] levam o desenvolvimento de firewalls, entre outros mecanismos de segurança, a um novo patamar. Quando comparado ao OpenFlow, o P4 oferece mais flexibilidade e programabilidade aos desenvolvedores de aplicações. Em particular, os dispositivos do plano de dados podem conter regras e códigos mais complexos, capazes de realizar pré-processamento de fluxos de dados sem recorrer ao controlador da rede. Entretanto, como é uma tecnologia recente, existem apenas algumas poucas iniciativas, incipientes, de firewalls com P4 [Vörös and Kiss 2016]. Em resumo, ainda há espaço para pesquisa e desenvolvimento neste contexto.

Requisitos essenciais (REs)

Independente das características escolhidas para a criação de firewalls em SDNs, alguns requisitos, considerados essenciais, são esperados para que a solução seja vista como robusta e aplicável na prática. A seguir, são apresentados e detalhados alguns dos requisitos mais importantes e destacados na literatura [Dixit et al. 2018, Scott-Hayward et al. 2015].

(RE_1) **Aplicação centralizada de políticas**: A finalidade de um firewall é aplicar políticas de segurança a uma máquina ou rede. Numa SDN, as políticas devem ser aplicadas a partir de um ponto central, com conhecimento global da rede, provido pelo controlador, variando em granularidade de acordo com as necessidades da organização. As políticas são convertidas pelo firewall em regras de fluxo, que são instaladas de forma reativa ou proativa nos dispositivos do plano de dados.

(RE_2) **Rastreamento de fluxo centralizado**: O firewall deve ter conhecimento global sobre os fluxos de dados que trafegam pela rede. Isto torna viável o gerenciamento das regras em todos os dispositivos da rede por onde o fluxo de dados deve passar, além de facilitar a detecção de conflitos nas regras aplicadas.

(RE_3) **Resolução de conflitos**: Ao detectar conflitos de regras, o firewall deve ser capaz de realizar a resolução dos conflitos de forma a garantir a aplicação efetiva e segura das políticas de segurança.

(RE_4) **Manipulação automática de prioridades**: Aplicativos, controladores, ou administradores podem alterar as tabelas de encaminhamento dos dispositivos do plano de dados. É imprescindível delegar níveis de autorização a cada entidade de forma a evitar que regras de baixa prioridade se sobreponham a regras de alta prioridade. Por exemplo, assumindo que segurança é a prioridade maior da rede, um aplicativo de firewall deve ter prioridade sobre outros aplicativos ou administradores.

(RE_5) **Suporte a múltiplas instâncias**: Redes complexas, como as de grandes data centers, podem conter diversas sub-redes que atendem diferentes clientes e serviços. Nestes casos, o firewall deve ser capaz de prover gerenciamento individualizado a cada cliente e suas sub-redes.

(RE_6) **Escalabilidade e concorrência**: Em uma rede dinâmica e escalável, as atualizações de políticas de segurança nem sempre são sequenciais. Diferentes aplicativos em execução em um controlador podem realizar atualizações simultâneas de regras que controlam os fluxos de dados e, eventualmente, podem violar alguma política de segurança do firewall. Um exemplo disto seria um software de balanceamento de carga adicionar uma regra que redirecione um tráfego TCP, antes do firewall aplicar uma regra de bloqueio. Para evitar esse tipo de problema, o firewall deve controlar a aplicação das regras nos dispositivos do plano de dados.

(RE_7) **Suporte stateful**: Manter os estados de conexoes ativas permite ao firewall ter um conhecimento geral do que acontece na rede. Ao conhecer os parâmetros da comunicação, como protocolo, portas utilizadas, origem e destino dos pacotes, um firewall stateful se torna capaz de tomar decisões baseadas em decisões anteriores. Por exemplo, em uma conexão é bidirecional, após acontecer o *handshake* TCP entre dois hosts, os próximos pacotes participantes desta conexão simplesmente serão aceitos sem a necessidade novas regras ou inspeções adicionais como acontece na filtragem de pacotes *stateless*. Em ambientes SDN, o firewall deve buscar estas informações utilizando recursos do Openflow/P4 ou através da visão holística da rede provida pelo controlador.

A Tabela 2 resume o atendimento aos requisitos essenciais a pouco apresentados. Como pode ser observado, nenhum dos firewalls atende mais do que 4 (quatro) dos 7 (sete) requisitos essenciais, demonstrando que há oportunidades de pesquisa e desenvolvimento nesta área.

Tabela 2. Atendimentos aos Requisitos Essenciais (REs)

Firewall SDN	RE_1	RE_2	RE_3	RE_4	RE_5	RE_6	RE_7
Fireflow[Fiessler et al. 2018]	✓				✓		✓
FORTRESS[Caprolu et al. 2019]	✓	✓					✓
Firewall Floodlight[Morzhov et al. 2016]	✓		✓	✓			
FlowGuard[Hu et al. 2014]	✓	✓	✓	✓			
FlowTracker[Tran and Ahn 2016]	✓	✓					✓
Firewall for POX[Othman et al. 2017]	✓		✓	✓			
RSF[Zerkane et al. 2016b]	✓						✓
PSF [Zerkane et al. 2016a]	✓		✓	✓			✓
REFLO[Visoottiviseth et al. 2017]	✓	✓			✓		✓
SDFS[Zeineddine and El-Hajj 2018]	✓				✓		✓
SMPU-P4[Vörös and Kiss 2016]	✓						✓

4. Desafios e Oportunidades

Apesar dos avanços da tecnologia e das características e requisitos essenciais das soluções existentes, resumidos nas Tabelas 1 e 2, os firewalls em SDNs ainda tem uma longa jornada de inovação e desenvolvimento pela frente. A seguir são apresentados e discutidos alguns dos principais desafios e oportunidades de pesquisa nesta área.

Desempenho: Estudos apontam que um dos principais desafios para o sucesso de firewalls em redes SDN está atrelado ao desempenho [Dixit et al. 2018]. Experimentos práticos demonstram que um acréscimo de 100 conexões simultâneas pode causar um atraso de 200% no tempo de resposta do firewall [Tran and Ahn 2016]. Apesar de existirem algumas alternativas, como a instalação proativa de regras nos dispositivos do plano de dados [Fiessler et al. 2018, Zerkane et al. 2016b] e firewalls parcialmente implementados no plano de dados [Vörös and Kiss 2016], ainda não existem soluções que atendem os requisitos de desempenho dos mais diversos cenários, em particular data centers e infraestruturas críticas, que requerem altos níveis de segurança e baixa latência nas comunicações.

Resolução de conflitos: Regras de tráfego de dados e regras de políticas de segurança dividem o mesmo espaço nas tabelas de encaminhamento dos dispositivos de rede.

Este cenário potencializa a sobreposição de regras que violam condições cruciais das políticas de segurança e de tráfego de dados da organização. Alguns firewalls fazem uso de módulos adicionais para garantir prioridade às regras derivadas de políticas de segurança [Hu et al. 2014, Othman et al. 2017]. Entretanto, estas alternativas não resolvem de fato os conflitos, podendo levar a problemas no encaminhamento dos dados. Por exemplo, um pacote que deveria ser encaminhado por uma regra inserida pelos administradores da rede acaba bloqueado pelas políticas de segurança do firewall.

Segurança: Como os firewalls dividem o ambiente do controlador com outras aplicações, diferentes tipos de problemas de segurança podem surgir. Por exemplo, aplicações terceiras podem explorar vulnerabilidades do controlador que permitam ao atacante burlar o firewall, seja injetando regras maliciosas diretamente no plano de dados, ou manipulando o controlador em prol de um ataque [Dixit et al. 2018, Yoon et al. 2017, Thimmaraju et al. 2017].

A pesquisa e a inovação no que diz respeito a aspectos como desempenho, resolução de conflitos e segurança são exemplos de suma importância para utilização prática e popularização de firewalls SDN. Além disso, observando as tecnologias e demandas atuais de instituições públicas e privadas, recursos de segurança como IPS (*Intrusion Prevention System*), IDS (*Intrusion Detection System*) e soluções avançadas de controle de pragas eletrônicas (e.g. antivírus, malwares) precisam ser também consideradas no contexto dos firewalls SDN. Atualmente, há sistemas deste tipo que trabalham em conjunto com firewalls tradicionais, utilizados pelas organizações. Portanto, o gerenciamento destes ambientes heterogêneos, representa mais uma oportunidade de pesquisa.

5. Conclusão

Neste trabalho, foi realizado o levantamento do estado da arte de firewalls para redes definidas por software (SDNs). Os firewalls foram classificados de acordo com quatro características e recursos, incluindo arquitetura, modo de operação, estado das conexões e protocolo utilizado para programar o plano de dados. A maioria dos firewalls possui uma arquitetura centralizada, opera de modo reativo, é *stateful* e utiliza o protocolo OpenFlow.

As análises realizadas também permitem identificar que a maioria das soluções atende no máximo 4 dos 7 requisitos identificados como essenciais para firewalls SDN. Portanto, é possível concluir que há oportunidades de pesquisa nesta área, em especial no que diz respeito a desafios como desempenho, resolução de conflitos e segurança.

Referências

Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., Schlesinger, C., Talayco, D., Vahdat, A., Varghese, G., et al. (2014). P4: Programming protocol-independent packet processors. *ACM SIGCOMM CCR*, 44(3):87–95.

Caprolu, M., Raponi, S., and Di Pietro, R. (2019). Fortress: an efficient and distributed firewall for stateful data plane sdn. *Security and Communication Networks*, 2019.

Dixit, V. H., Kyung, S., Zhao, Z., Doupé, A., Shoshitaishvili, Y., and Ahn, G.-J. (2018). Challenges and Preparedness of SDN-based Firewalls. In *Proc. of the ACM Int. Workshop on Security in SDNs & NFV*, pages 33–38. ACM.

Fiessler, A., Lorenz, C., Hager, S., and Scheuermann, B. (2018). FireFlow-High Performance Hybrid SDN-Firewalls with OpenFlow. In *43rd LCN*, pages 267–270. IEEE.

Gouda, M. G. and Liu, A. X. (2005). A model of stateful firewalls and its properties. In *IEEE DSN*, pages 128–137. IEEE.

Hu, H., Han, W., Ahn, G.-J., and Zhao, Z. (2014). Flowguard: building robust firewalls for software-defined networks. In *Proceedings of the third workshop on Hot topics in software defined networking*, pages 97–102. ACM.

Ioannidis, S., Keromytis, A. D., Bellovin, S. M., and Smith, J. M. (2000). Implementing a distributed firewall. In *Proceedings of the 7th ACM Conference on Computer and Communications Security*. ACM Press.

Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C. E., Azodolmolky, S., and Uhlig, S. (2014). Software-defined networking: A comprehensive survey. *arXiv preprint arXiv:1406.0440*.

McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., and Turner, J. (2008). OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74.

Morzhov, S., Alekseev, I., and Nikitinskiy, M. (2016). Firewall application for floodlight sdn controller. In *Int. SIBCON*, pages 1–5. IEEE.

ONF (2019). OpenFlow. `http://bit.do/e3jhe`.

Othman, W. M., Chen, H., Al-Moalmi, A., and Hadi, A. N. (2017). Implementation and performance analysis of sdn firewall on pox controller. In *IEEE 9th Int. Conference on Communication Software and Networks (ICCSN)*, pages 1461–1466. IEEE.

Satasiya, D. et al. (2016). Analysis of software defined network firewall (sdf). In *WiSPNET*, pages 228–231. IEEE.

Scott-Hayward, S., Natarajan, S., and Sezer, S. (2015). A survey of security in software defined networks. *IEEE Communications Surveys & Tutorials*, 18(1):623–654.

Thimmaraju, K., Schiff, L., and Schmid, S. (2017). Outsmarting network security with sdn teleportation. In *IEEE EuroS&P*, pages 563–578. IEEE.

Tran, T. V. and Ahn, H. (2016). FlowTracker: A SDN stateful firewall solution with adaptive connection tracking and minimized controller processing. In *2016 International Conference on Software Networking (ICSN)*, pages 1–5. IEEE.

Visoottiviseth, V., Lertviriyasawat, S., Suppiyatrakoon, P., Chitkornkitsil, P., and Yamai, N. (2017). REFLO: Reactive firewall system with OpenFlow and flow monitoring system. In *TENCON 2017-2017 IEEE Region 10 Conference*, pages 2273–2278. IEEE.

Vörös, P. and Kiss, A. (2016). "security middleware programming using p4". In *Human Aspects of Information Sec., Privacy, and Trust*, pages 277–287. Springer.

Yoon, C., Lee, S., Kang, H., Park, T., Shin, S., Yegneswaran, V., Porras, P., and Gu, G. (2017). Flow wars: Systemizing the attack surface and defenses in software-defined networks. *IEEE/ACM Transactions on Networking*, 25(6):3514–3530.

Zeineddine, A. and El-Hajj, W. (2018). Stateful distributed firewall as a service in sdn. In *2018 4th IEEE Conf. on Network Softwarization (NetSoft)*, pages 212–216. IEEE.

Zerkane, S., Espes, D., Le Parc, P., and Cuppens, F. (2016a). A proactive stateful firewall for software defined networking. In *International Conference on Risks and Security of Internet and Systems*, pages 123–138. Springer.

Zerkane, S., Espes, D., Le Parc, P., and Cuppens, F. (2016b). Software defined networking reactive stateful firewall. In *IFIP International Conference on ICT Systems Security and Privacy Protection*, pages 119–132. Springer.