



Document details

1 of 1

[Export](#) [Download](#) [More...](#)

Proceedings - 2018 4th International Conference on Computing, Engineering, and Design, ICCED 2018

12 April 2019, Article number 8691107, Pages 40-45

4th International Conference on Computing, Engineering, and Design, ICCED 2018; Asian Institute of Technology (AIT) Bangkok; Thailand; 6 September 2018 through 8 September 2018; Category number E6564; Code 147451

Software defined networking (SDN) and its security issues (Conference Paper)

Aziz, N.A., Mantoro, T., Khairudin, M.A., Murshid, A.F.B.A.

[View additional authors](#)[Save all to author list](#)^aDept of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia^bDepartment of Computer Science, FET, Sampoerna University, Jakarta, Indonesia[View additional affiliations](#)

Abstract

The demand of network infrastructure and services is ever increasing. The network architecture and related technology must be flexible enough to accommodate the ever-growing number of users. Software-Defined Networking (SDN) is an approach of networking architecture that improvise conventional network in terms of scalability, security, and availability. At the same time, SDN is vulnerable to security threats as well. This paper studies on SDN architecture, the improvement of SDN from conventional network, the vulnerability and threats in SDN, and possible solutions to some security threats examples. It gives an overview of SDN and security-the architecture advantages that can be leveraged to secure network systems, and the security threats that may occur if improper design and deployment of SDN take place. © 2018 IEEE.

SciVal Topic Prominence

Topic: [Controllers](#) | [Switches](#) | [Controller placement](#)Prominence percentile: 99.841 [i](#)

Author keywords

[DDoS Attack](#) [Packet Sniffing](#) [Security Best Practice](#) [Software-Defined Networking](#)
[Traditional network Security Threats](#)

Indexed keywords

Engineering
controlled terms:[Denial-of-service attack](#) [Network architecture](#) [Security systems](#) [Software defined networking](#)Engineering
uncontrolled terms[DDoS Attack](#) [Network infrastructure](#) [Networking architecture](#) [Packet Sniffing](#)
[Security Best Practices](#) [Security threats](#) [Software defined networking \(SDN\)](#)
[Traditional network Security Threats](#)Engineering main
heading:[Network security](#)

Cited by 1 document

Alshra'a, A.S. , Seitz, J.

External device to protect the software-defined network performance in case of a malicious attack

(2019) ACM International Conference Proceeding Series[View details of this citation](#)

Inform me when this document is cited in Scopus:

[Set citation alert](#)[Set citation feed](#)

Related documents

Find more related documents in Scopus based on:

[Authors](#) > [Keywords](#) >

ISBN: 978-153869378-0
Source Type: Conference Proceeding
Original language: English

DOI: 10.1109/ICCED.2018.00018
Document Type: Conference Paper
Sponsors: Kedutaan Besar Republik Indonesia,Nusa Putra University,Sampoerna University
Publisher: Institute of Electrical and Electronics Engineers Inc.

© Copyright 2019 Elsevier B.V., All rights reserved.

About Scopus

[What is Scopus](#)
[Content coverage](#)
[Scopus blog](#)
[Scopus API](#)
[Privacy matters](#)

Language

[日本語に切り替える](#)
[切换到简体中文](#)
[切换到繁體中文](#)
[Русский язык](#)

Customer Service

[Help](#)
[Contact us](#)

ELSEVIER

[Terms and conditions ↗](#) [Privacy policy ↗](#)

Copyright © Elsevier B.V. ↗. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.

We use cookies to help provide and enhance our service and tailor content. By continuing, you agree to the use of cookies.

 RELX