Security Risk Analysis in Accounting Information Systems Based on Data Dashboard from the Palo Alto Network PA-820 UTM

Abdul Roup
Program Studi Akuntansi, Institut Bisnis dan Informatika Kesatuan
EMail : abdulrouf.ci@gmail.com

ABSTRACT

This study analyzes security risks in accounting information systems using data from the Palo Alto Network PA-820 UTM dashboard, which monitors various aspects such as network activity, user activity, and application usage. The data includes information on data transfers, source and destination IP activities, and system rule usage. The study aims to identify potential threats that could affect the integrity and security of accounting information systems. Monitoring dashboard data provides a clear picture of potential threats, both external and internal, that could impact the integrity and confidentiality of financial data. Implementing appropriate security policies, supported by continuous monitoring, is essential to ensuring that accounting information systems remain protected from various potential threats. By taking proactive measures, organizations can reduce security risks and maintain trust in their information systems.

Keywords: Accounting Information Systems, Security, Risk, Dashboard, Network Activity.

INTRODUCTION

Accounting Information Systems (AIS) are integral to managing financial data within an organization. As Romney and Steinbart (2021) note, AIS plays a crucial role in supporting decision-making, management control, and financial reporting, making it a vital element of a company's operational structure. However, as business operations become more complex and reliant on technology, AIS is increasingly vulnerable to various security threats (Hall, 2022). These threats stem not only from external attacks like hacking and malware but also from internal risks, including human error and unauthorized access by internal users (Whitman & Mattord, 2018). Therefore, managing security risks within AIS is essential for maintaining the integrity and confidentiality of financial data.

Advances in information technology significantly impact data management within AIS but also introduce new risks. Gelinas et al. (2018) emphasize that while digital transformation has enhanced the efficiency of information systems, it has also increased exposure to cyberattacks. The use of various applications and digital platforms in daily operations heightens the risk of cyberattacks (Chen, 2021). User activities, both within and outside the organization, need to be closely monitored to ensure no security breaches that could compromise the system. This is where the importance of monitoring dashboards comes into play, enabling real-time oversight of network, application, and user activities (Simkin, Norman, & Rose, 2018).

These monitoring dashboards provide valuable data for analyzing activity patterns that may indicate potential threats. According to Fish and Ryoo (2016), continuous monitoring of network and user activities is crucial for detecting anomalies that could signal cyberattacks. By tracking data transfers, IP activities, and application usage, management can quickly identify anomalies that may indicate security risks (Whitman & Mattord, 2018). However, despite the availability of this data, the main challenge lies in

JIMKES

Jurnal Ilmiah Manajemen Kesatuan
Vol. 12 No.5, 2024
pp. 1449 - 1456
IBI Kesatuan
ISSN 2337 – 7860
E-ISSN 2721 – 169X
DOI: 10.37641/jimkes.v12i5.2775

effectively analyzing and interpreting it to take appropriate preventive actions (Ghosh & Turrini, 2018).

This study aims to explore data from monitoring dashboards in accounting information systems to identify existing security risks. By analyzing network, user, and application activities over a specific period, this research will uncover potential vulnerabilities that may have been overlooked (Laudon & Laudon, 2020). The analysis focuses not only on external threats but also on internal ones, which are often more difficult to detect (Warren & Tayler, 2019).

In the current digital era, where data is the most valuable asset, safeguarding the security of accounting information systems is a top priority. Any security breach can have significant impacts, not only on data integrity but also on a company's reputation (Schneier, 2015). Therefore, this study contributes to understanding how monitoring data can be used to enhance AIS security and mitigate existing risks (Verma, 2019).

METHOD

This study uses a descriptive analysis approach based on data obtained from system dashboards. The data includes network activity, application usage, and user activity monitored from January 1 to July 31, 2024. The analysis is conducted to identify patterns that may indicate security risks.

RESULTS AND DISCUSSION

The analysis of data obtained from the accounting information system monitoring dashboard provides deep insights into the potential security risks faced by organizations. The results reveal various patterns of network, user, and application activity that may indicate threats to system integrity and security. This section discusses the main findings of the analysis and their implications for managing security risks in accounting information systems.

Network Activity

The data shows significant fluctuations in data transfer between January 1 and July 31, 2024, with peak activity occurring in July. This activity reflects high application usage, which could increase risks if not balanced with adequate security protocols.

User Activity

User activities recorded include user sessions and the amount of data uploaded and downloaded. These patterns can provide insights into potential insider threats, where internal users may access or manipulate data without proper authorization.

Application Usage

The dashboard records various categories of applications used, such as social networking, business, and software updates. The use of these applications, particularly those related to social networking and file-sharing, needs to be monitored as they could open doors to external threats.

Security Risk Implications

Based on the data analysis, several key risks were identified, including threats from non-business application usage, potential cyberattacks from high network activity, and insider threats from user activities. Each of these risks needs to be managed with appropriate security policies to maintain AIS integrity.

CONCLUSION

Security in accounting information systems is crucial to ensuring the integrity and confidentiality of a company’s financial data. Using dashboard data, this study

successfully identified several risks that could affect AIS security and provided recommendations for more effective risk management.

CLOSING

In conclusion, this study emphasizes the importance of monitoring and deeply analyzing activities within accounting information systems to identify and manage security risks. Monitoring dashboard data provides a clear picture of potential threats, both external and internal, that could impact the integrity and confidentiality of financial data. Implementing appropriate security policies, supported by continuous monitoring, is essential to ensuring that accounting information systems remain protected from various potential threats. By taking proactive measures, organizations can reduce security risks and maintain trust in their information systems.

RECOMMENDATIONS

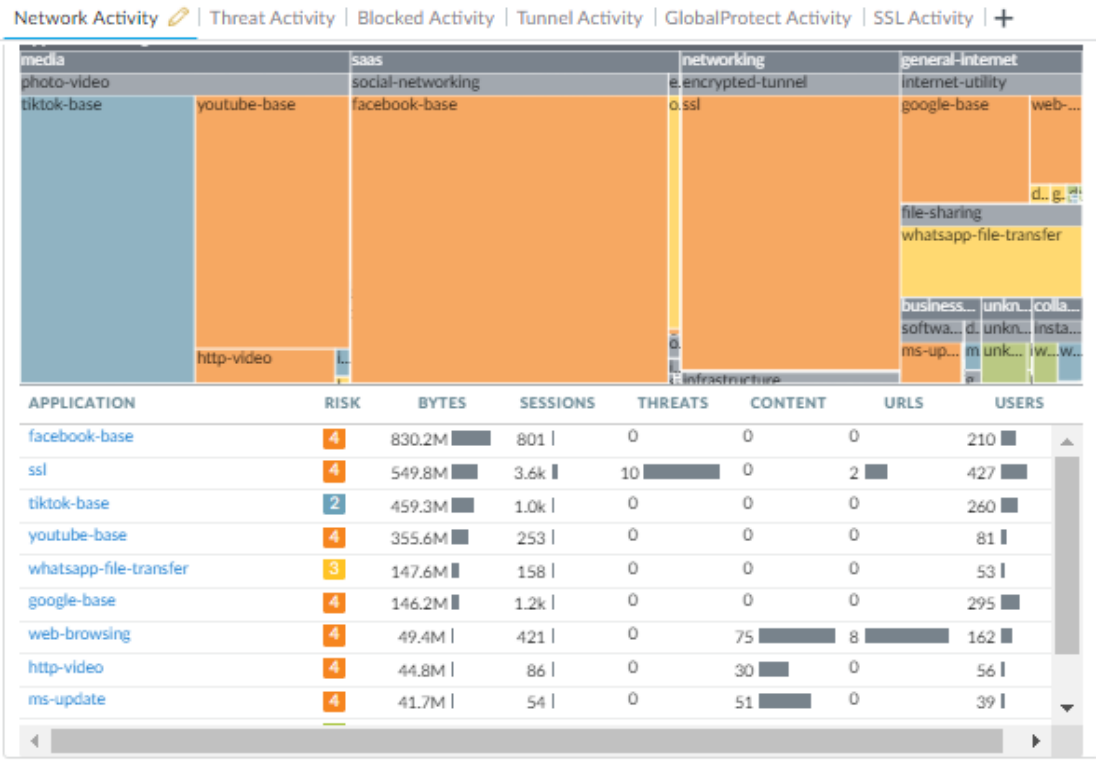
This study recommends implementing stricter security policies, enhancing network activity monitoring, and training users on the importance of data security. Additionally, routine audits of application usage and user activity are necessary to detect and prevent potential threats.

REFERENCES

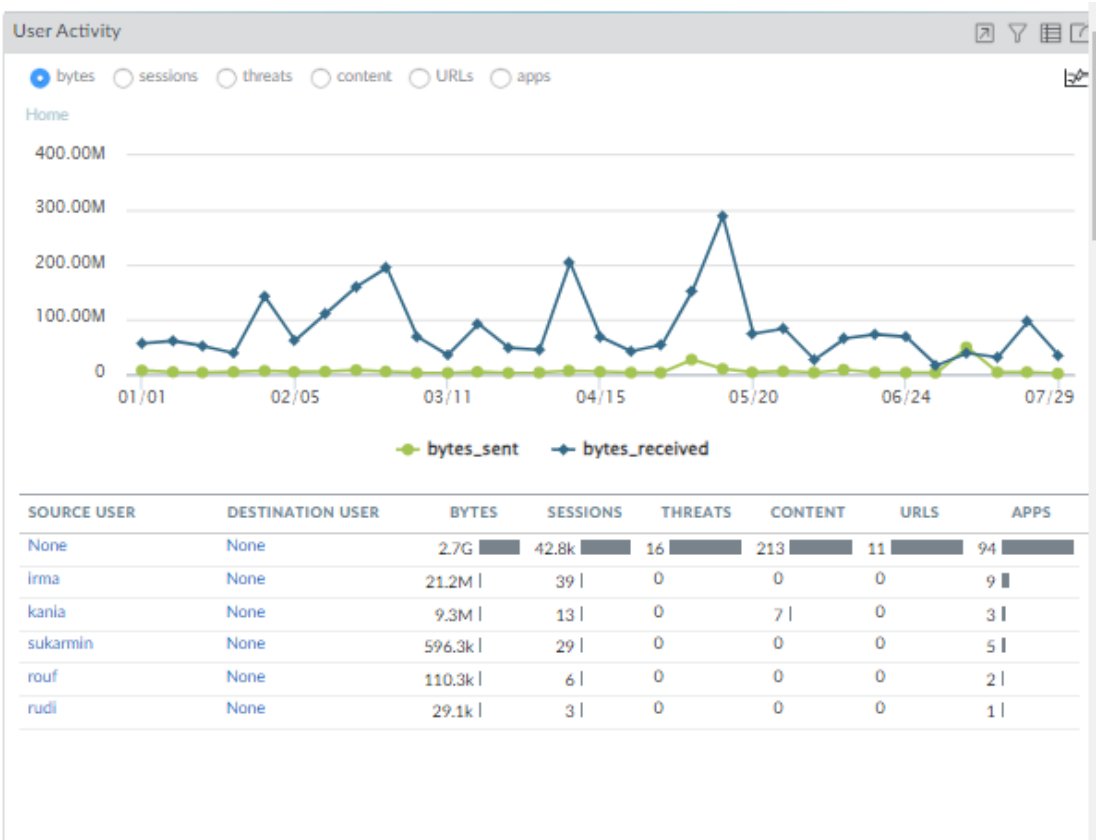
[1] Romney, M. B., & Steinbart, P. J. (2021). *Accounting Information Systems*. 15th Edition. Pearson.
[2] Hall, J. A. (2022). *Accounting Information Systems*. 10th Edition. Cengage Learning.
[3] Gelinas, U. J., Dull, R. B., & Wheeler, P. (2018). *Accounting Information Systems*. 10th Edition. Cengage Learning.
[4] Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm*. 16th Edition. Pearson.
[5] Bodnar, G. H., & Hopwood, W. S. (2016). *Accounting Information Systems*. 12th Edition. Pearson.
[6] Weygandt, J. J., Kimmel, P. D., & Kieso, D. E. (2020). *Accounting Principles*. 14th Edition. Wiley.
[7] Simkin, M. G., Norman, C. S., & Rose, J. M. (2018). *Core Concepts of Accounting Information Systems*. 14th Edition. Wiley.
[8] Stair, R., & Reynolds, G. (2021). *Fundamentals of Information Systems*. 10th Edition. Cengage Learning.
[9] Chen, Y. (2021). *Cybersecurity in Accounting and Financial Systems*. Routledge.
[10] Warren, S., & Tayler, M. (2019). *Accounting Information Systems: Controls and Processes*. 3rd Edition. Wiley.
[11] Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.
[12] Verma, S. (2019). *Security in Computing and Networking*. Springer.
[13] Fish, A., & Ryoo, J. (2016). *Information Security: Principles and Practices*. 2nd Edition. Pearson.
[14] Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security*. 6th Edition. Cengage Learning.
[15] Fitzgerald, J., & Dennis, A. (2020). *Business Data Communications and Networking*. 13th Edition. Wiley.
[16] Ghosh, A., & Turrini, E. (2018). *Cybercrimes: A Multidisciplinary Analysis*. Springer.
[17] Rainer, R. K., Prince, B., Watson, H. J., & Cegielski, C. G. (2019). *Introduction to Information Systems*. 8th Edition. Wiley.
[18] Beasley, M. S., Branson, B. C., & Hancock, B. V. (2021). *Developing Key Risk Indicators to Strengthen Enterprise Risk Management*. COSO.

[19] Leech, T. J. (2020). *Risk Management: A Practical Guide for Accounting Professionals*. Wiley.

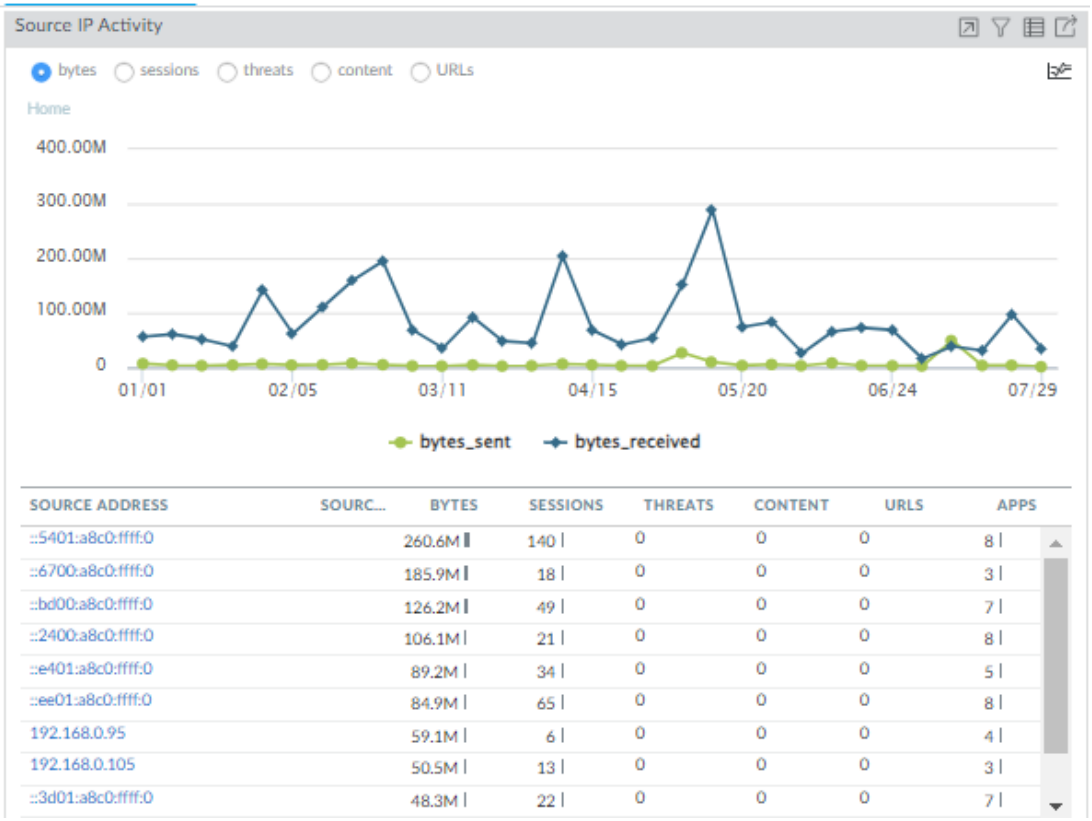
[20] D'Arcy, J. & Hovav, A. (2007). "Deterring Internal Information Systems Misuse." *Communications of the ACM*, 50(10), 113-117.



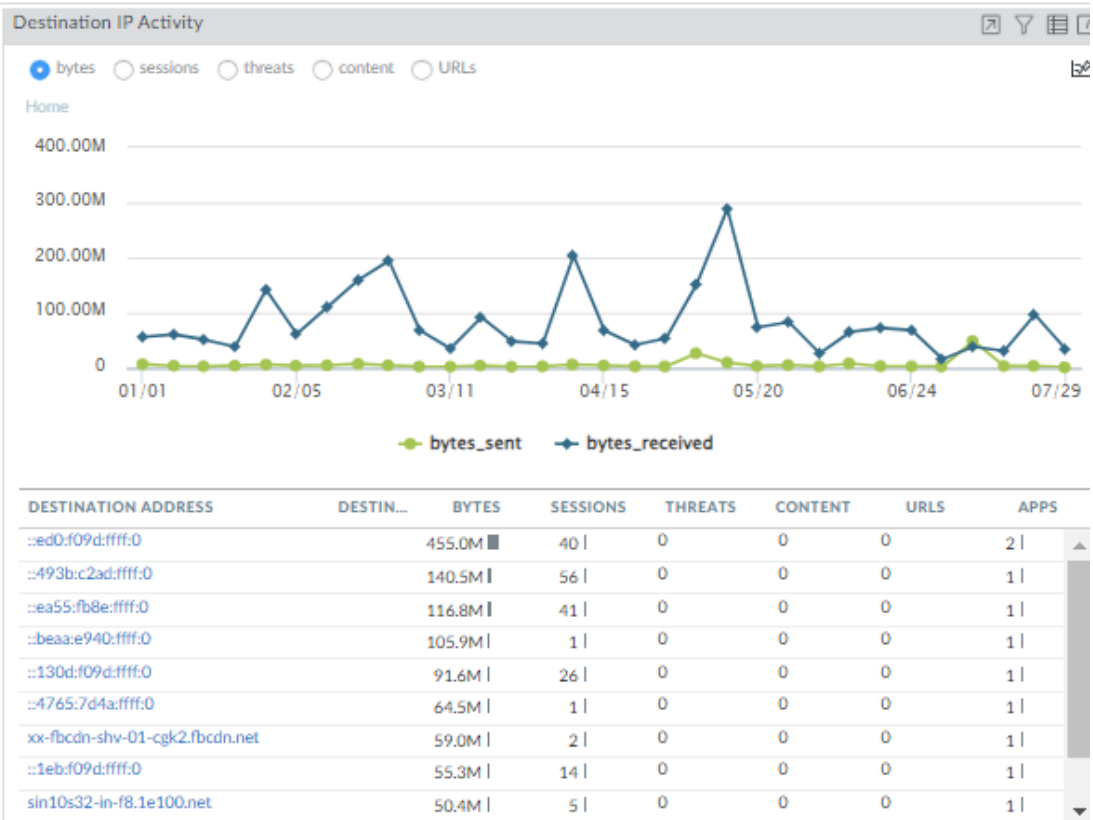
User Activity



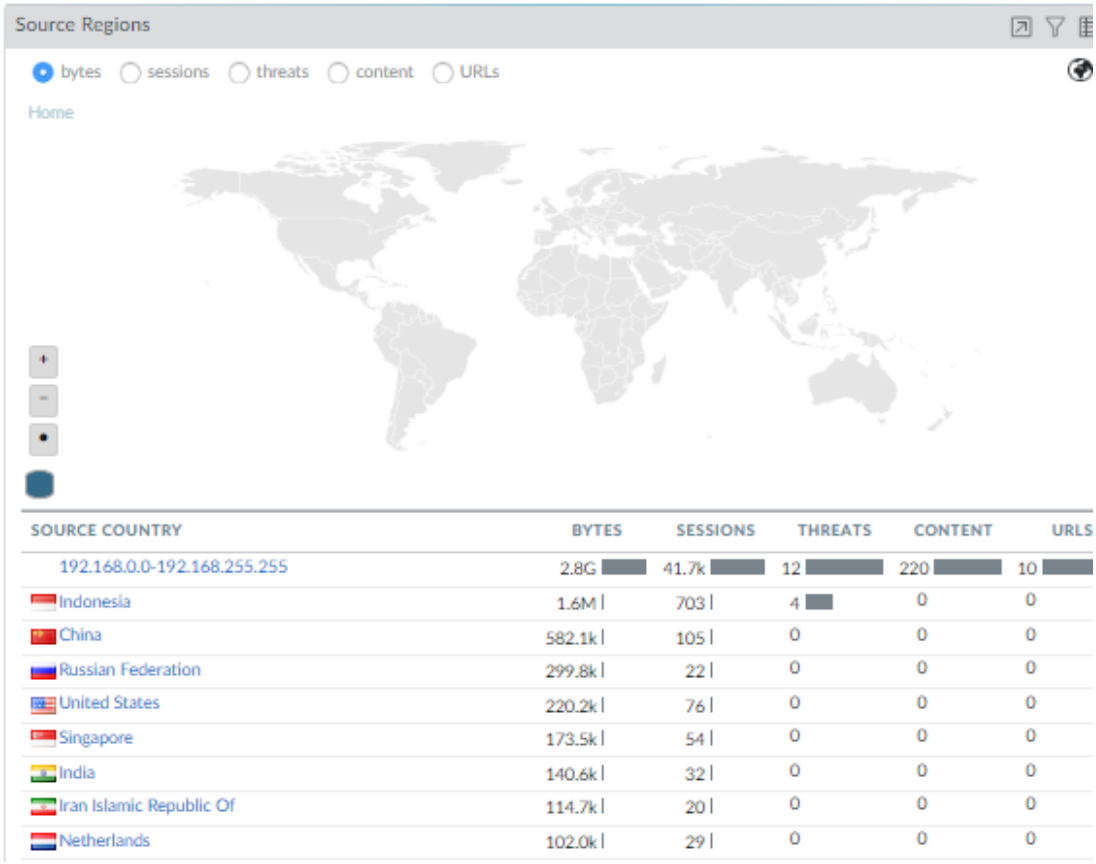
Source IP Activity



Destination IP Activity

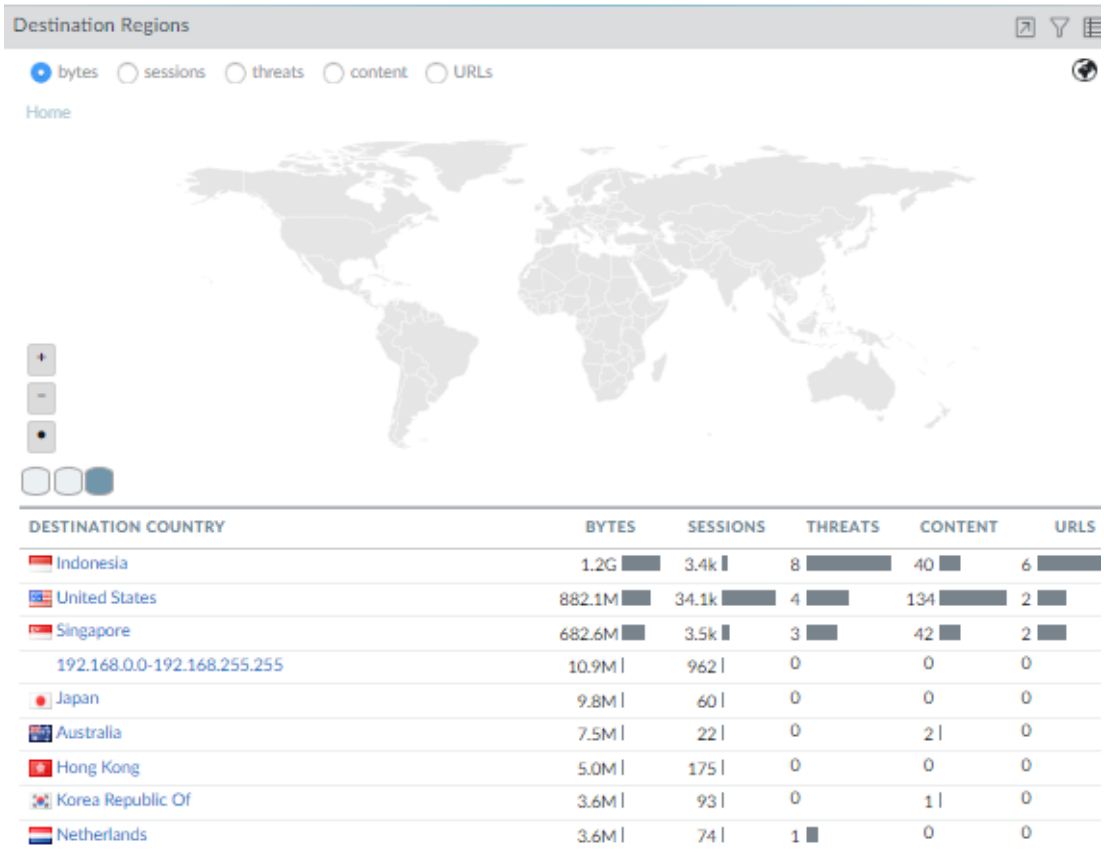


Source Region



SOURCE COUNTRY	BYTES	SESSIONS	THREATS	CONTENT	URLS
192.168.0.0-192.168.255.255	2.8G	41.7k	12	220	10
Indonesia	1.6M	703	4	0	0
China	582.1k	105	0	0	0
Russian Federation	299.8k	22	0	0	0
United States	220.2k	76	0	0	0
Singapore	173.5k	54	0	0	0
India	140.6k	32	0	0	0
Iran Islamic Republic Of	114.7k	20	0	0	0
Netherlands	102.0k	29	0	0	0

Destination Region

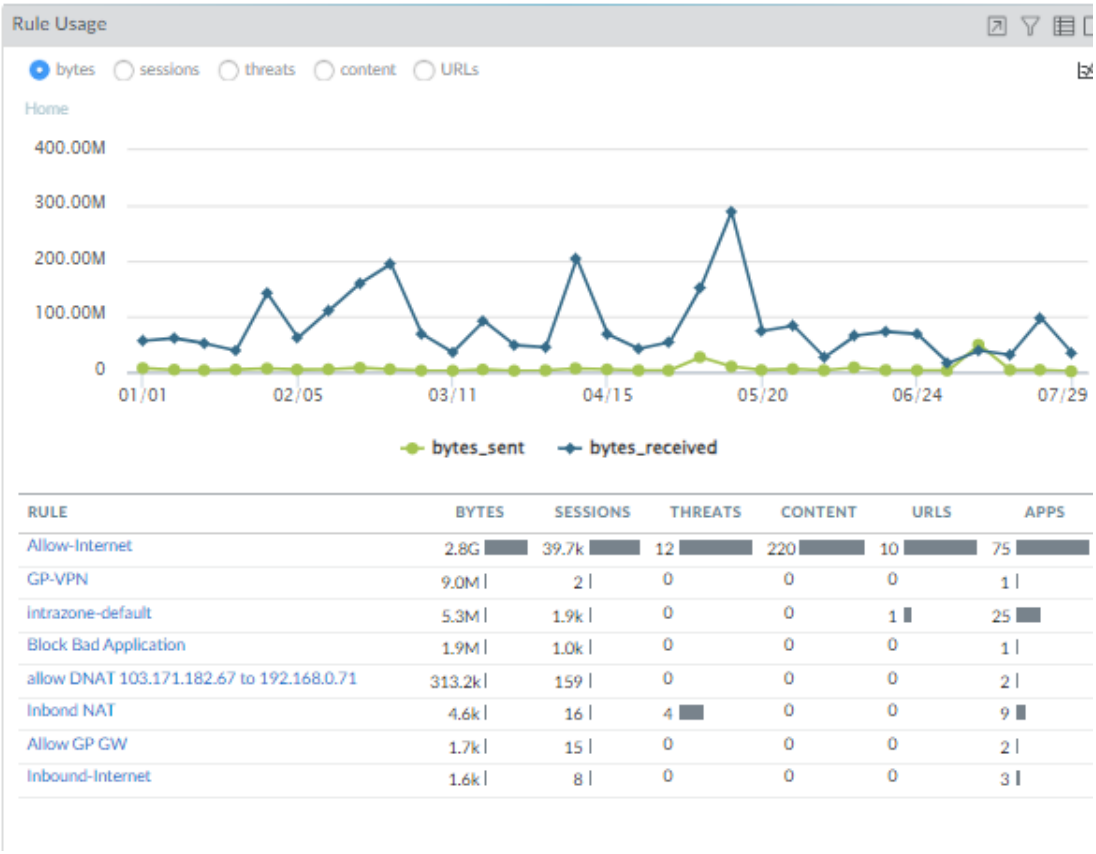


DESTINATION COUNTRY	BYTES	SESSIONS	THREATS	CONTENT	URLS
Indonesia	1.2G	3.4k	8	40	6
United States	882.1M	34.1k	4	134	2
Singapore	682.6M	3.5k	3	42	2
192.168.0.0-192.168.255.255	10.9M	962	0	0	0
Japan	9.8M	60	0	0	0
Australia	7.5M	22	0	2	0
Hong Kong	5.0M	175	0	0	0
Korea Republic Of	3.6M	93	0	1	0
Netherlands	3.6M	74	1	0	0

Security Risk and Accounting Information System

1456

Rule Usage



RULE	BYTES	SESSIONS	THREATS	CONTENT	URLS	APPS
Allow-Internet	2.8G	39.7k	12	220	10	75
GP-VPN	9.0M	2	0	0	0	1
intrazone-default	5.3M	1.9k	0	0	1	25
Block Bad Application	1.9M	1.0k	0	0	0	1
allow DNAT 103.171.182.67 to 192.168.0.71	313.2k	159	0	0	0	2
Inbond NAT	4.6k	16	4	0	0	9
Allow GP GW	1.7k	15	0	0	0	2
Inbound-Internet	1.6k	8	0	0	0	3