Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

TrustSec Micro segmentation: Performance Impact Analysis in Large-Scale Campus Networks

Vishwanath Hiremath

Software Engineer senior staff, Juniper networks inc

vishwavishal@gmail.com

ARTICLE INFO

Received: 02 Oct 2024

Revised: 19 Nov 2024

Accepted: 28 Nov 2024

ABSTRACT

Rapid changes in the paradigm of network security have pushed the further use of micro segmentation as one of the significant measures to secure sensitive data and reduce the possibility of cyberattacks across extensive campus networks. Cisco has advanced its security solution named TrustSec, which provides strong architecture to deploy micro segmentation that has granular control over traffic in the network. There is no study analyzing the performance impact of TrustSec micro segmentation on large-scale campus networks in detail and the impact of TrustSec micro segmentation on network performance. In a set of controlled experiments and simulations we determine the performance effects through the use of TrustSec segmentation techniques in terms of bandwidth utilization, latency, throughput, and scale along with the large enterprise environment. Our results indicate that micro segmentation is very effective in terms of network security as it isolates and controls access to high-value resources and is used to deny attackers access to the resources, but it comes with its own overheads, which may have implications on their performance metrics, particularly in high-traffic scenarios. The paper will also describe the trade-offs involved in the security benefit and the cost to performance, which would be of value to the network architect and administrator. With examples of the operational considerations of TrustSec on large-scale deployments, this paper will help guide future implementation of micro segmentation on academic and enterprise networks to provide the best balance between achieving security and maintaining network decompositions with acceptable performance.

Keywords: TrustSec, Micro segmentation, Large-Scale Campus Networks, cyber-attacks.

1. Introduction

With the advent of the digital and highly connected world today, network security solutions have been put under an even greater spotlight than ever before. Given the proliferation of the size and complexity of campus networks, campuses have increasingly found that traditional perimeter-based security models are insufficient to defend against advanced cyber-attacks. Strategies such as micro segmentation, which has seen networks split into small, isolated, and self-contained sections to reduce attack surfaces, has since become one of the ways through which networks can bolster security. Of the available micro segmentation solutions, the Cisco TrustSec framework is a noteworthy solution that goes beyond the control of access to sensitive resources and the enforcement of policies that are based on security levels in conjunction with physical network boundaries [1].

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

TrustSec incorporates Security Group Tags (SGTs) to define and mark devices and provides fine-grained control of network traffic. The segmentation will enable organizations to isolate vital resources and prevent possible lateral transfer of threats, and hence the risk of data being breached greatly reduced [2]. Nevertheless, the adoption of micro segmentation comes with some challenges especially in terms of the performance overview of large-scale campus network. Although the security advantages of micro segmentation are well-known, its impact on network performance, i.e. throughput, latency, and scale, is an increasingly researched and controversial topic [3].

It has been found that micro segmentation is capable of creating a great deal of security in the network by controlling the reach of unauthorized access, but this can cause overheads to the overall performances of the network. As an example, the need to tag packets plus policy enforcement overheads could be the performance bottleneck [4]. In addition, scalability of micro segmentation to large campus networks is an area of concern that must be critically evaluated since in campus networks, there may be hundreds or even thousands of devices. It is thus the aim of this paper to not only elaborate on the performance impact analysis of TrustSec micro segmentation in large-scale campus networks, but to do so in a way that addresses these concerns and also give an idea on how to strike a balance on choosing to have more security versus that of performance.

We will use theoretical analysis, controlled experimentation and simulation to assess the impact of micro segmentation provided by TrustSec on major performance attributes like bandwidth exploitation, delays and throughput. We hope our work can add to the mounting evidence of the benefits of micro segmentation, with guidance to the researcher and enterprise network planners looking to employ TrustSec within their campus networks [6].

1.1 Motivation

The sophistication and the ever-growing size of network on campuses pose great challenges in ensuring network security without affecting performance adversely. According to the evolving nature of that threat landscape, traditional network security models built on a perimeter-based defense are no longer up to the task on a large-scale campus network. With cyber threats increasingly becoming sophisticated, requirements to have more granular, dynamic and scaleable security solutions are ever increasing. The concept of micro segmentation especially in the form of TrustSec is a more sophisticated alternative, where important assets on the network are isolated and unauthorized network access is restrained. However, micro segmentation increases security but it affects network performance a matter that is of concern particularly at large-scale deployments. The motivation behind this study is the need to evaluate and determine trade-offs between security and performance during TrustSec micro segmentation, especially when applied to large campus networks where multifaceted security and performance are key to operational excellence.

1.2 Problem Statement

Although micro segmentation, especially implementation of TrustSec, offers greater security due to separation of network traffic and the inability of cyber threats to traverse the network laterally, it has often been seen to cause performance overheads, such as in latency and throughput. It is challenging to determine the exact effects of micro segmentation on TrustSec on the key performance parameters of latency, throughput, and bandwidth utilization within the context of large scale-campus network scenarios. Further, the performance benefits of TrustSec in these scenarios, especially as the number of devices and traffic increases, has barely been investigated. The area where there is need of empirical research is providing an assessment of the performance impact of TrustSec in addition to providing an insight into the balance between increased security and possible performance implications in such dynamic network systems.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

1.3 Contribution of the Study

In this study, the author contributes by showing the applicability of TrustSec micro segmentation in filling the deficiencies of the current approach to network security at least in large and complex campus networks. Conventional perimeter-based security paradigms are becoming insufficient and micro segmentation can be implemented to address lateral spread of threats. By electing TrustSec as an object of the study, the investigation preconditions the balance between the network performance and its security, preconditioning its empirical verification.

The literature review has been used to identify the deficiencies of the research conducted on the performance effect of the implementation of TrustSec on large networks. Although there has been work on micro segmentation, not many studies have empirically examined some of the key performance indicators, like latency, throughput or bandwidth usage, in large internetwork environments. This paper fulfills this void by carrying out a specific practical contextual study of TrustSec, on the aspects of performance and scale, yielding software knowledge on real practical implementation.

The methodology can add value in the form of an engineered structured empirical environment, to emulate a campus size Internet infrastructure environment, providing a controlled study of the performance metrics introduced by TrustSec. It demonstrates how latency, throughput and bandwidth utilization are influenced by a varying amount of traffic and network scale, giving a new framework to assess security solutions in dynamic networks.

The results and discussion section provide empirical data that although TrustSec introduces a minor overhead in terms of latency and bandwidth, it did not cause serious degrading in performance. The results can be used to infer on the scalability of TrustSec and it can be seen that TrustSec is able to scale well because it can sustain network throughput across large networks. The trade analysis conducted between section security and performance would also be of help to enable network administrators make informed deployment.

Lastly, the conclusion focuses on practical implications of the study, which points to the fact that TrustSec can be effectively utilized innetworks that are large-scale and they do not affect performance. It also lists research opportunities to be developed in the future such as AI-based policy enforcement and incorporation of SDN, which has the potential to enhance TrustSec to an even greater degree and be applied to even more complete and larger networks.

2. Literature Review

Micro segmentation has received a lot of interest in large networks as a means to increase security in the network. TrustSec, one of the advanced micro segmentation frameworks, uses Security Group Tags (SGTs) to implement access control policies, giving networking an additional protection against cross-network threats [7]. Research has shown that micro segmentation provides more than just an area of isolation of malicious actors into a network as it also separates sensitive resources and isolates them by keeping them out of the network.

Although micro segmentation offers robust security advantages, implementing it is likely to make performance an issue. One paper discussed the security benefits and the network performance trade-offs of micro segmentation. Its discovery is that, on the positive side, TrustSec can enhance security by creating more restrictive access controls and, on the negative side, the added tagging and policy enforcement functions can result in latency and throughput degradation in high-traffic situations [9]. This discovery underscores the importance of network administrators striking a delicate balance

Research Article

between performance and security in order to ensure that such security does not negatively affect access experience.

A different work examined the scalability of a micro segmentation model, such as TrustSec, in large-scale campus networks that have many connected devices (thousands). It was noted that micro segmentation of such large-scale networks demands a lot of resources to be deployed and may present the challenge of providing optimal network performance within each segment [10]. These difficulties necessitate the creation of more effective policy enforcement functions and network designs that can and will support micro segmentation without the performance impact.

Other studies have looked at the effects of TrustSec micro segmentation on the bandwidth consumption within big networks. The results proved that although TrustSec is efficient in ensuring isolation of network segments, it may cause the network to use more bandwidth as a result of the overhead caused by security policies and traffic monitoring. Sub-optimization of the TrustSec configurations to address overheads are areas where the TrustSec could be improved in large-scale deployments.

It is another problem with the campus networks having a dynamic flow with users being added and removed regularly, it is one of the factors that challenges the application of micro segmentation. It has been proven that TrustSec with other network automation tools allows reconfiguring network topologies without wasting any performances and ensuring security of the topology change. There may be one problem however, that is the complexity of the configuration of such systems [12].

The first is the effect that micro segmentation has on troubleshooting and monitoring of the network. As much as Micro segmentation enhances security by making segments isolated, it also adds a burden to network visibility making it difficult to implement monitoring of the traffic flows and identifying of performance bottlenecks. This has been an especially common deployment issue with TrustSecs, where security controls are too granular to see the traffic between network segments, necessitating a more sophisticated monitoring solution to maintain network performance at an optimal level [13].

The studies have underscored the fact that micro segmentation should be combined with other network security solutions, e.g., firewalls and intrusion detection systems (IDS) to make it more effective. In a combination with these technologies, TrustSec offers a complete protection option that not only segregates important resources but also keeps a constant check on possible threats [14]. Such an integrated solution has been demonstrated to enhance general campus network resilience against complex cyber-attacks.

The other important factor in micro segmentation research is the access whether it influences positively or negatively latency-sensitive applications like real-time communications and VoIP services. Studies have found that although micro segmentation has some security advantages, its overhead (assessing conformance to the policies and tagging packets) can raise latency that is perceptible in these applications, thus affecting the experience of the users [15]. This poses a challenge to large campus networks where such applications play a vital role in the day to day running of the network.

The contribution of TrustSec in meeting the regulatory requirements, including risk compliance with the GDPR and HIPAA, has also been discussed in the literature. Techniques such as micro segmentation frameworks (e.g. TrustSec) also are increasingly being used to satisfy compliance needs by isolating sensitive data and protecting it against unauthorized access. Nevertheless, the functionalities of TrustSec to address these regulatory requirements especially in large networks are complex to implement [16].

As regards performance optimization, the use of machine learning and artificial intelligence in improving efficiency of micro segmentation has been investigated by some studies. They have

demonstrated potential in the automated enforcement of policies and network traffic and have the potential to reduce the previously observed performance overhead of TrustSec micro segmentation [17]. With the application of AI-based tools networks could rely on real-time data to dynamically change policy, which could enhance security and performance.

Another point of interest has been the introduction of Software-Defined Networking (SDN) together with micro-segmentation such as TrustSec. It has been proposed that SDN and micro segmentation can potentially support the dynamic scalability and agility of a network by offering an enhanced ability to control the network, and therefore an increased potential to modify security policies and performance settings easy to manage [18]. The integration has potential to enable the management of large campus networks to be more efficient, particularly in dynamic environments where vigorous movements in network topologies are the order of the day.

The financial impact of implementing micro segmentation within broad campus networks has also been considered in a number of papers. Although micro segmentation adds to the security it is a costly add-on to achieve and manage especially in case of deploying complex solutions, such as TrustSec. It has been argued that efficient selection of network design and utilization of pre-existing infrastructure has the capability of reducing the financial effects [19].

An interesting study based on a small network application domain comprised of an assessment of the resiliency of the TrustSec micro segmentation to the changes of cyber threats. As lateral movement continues as a core threat to enterprises, micro segmentation plays an important role in suppressing lateral movement in networks. The flexibility of TrustSec to respond to new threats has been commendable, but that also urges the continual updates and monitoring to ensure effectiveness of the security [20].

3. Methodology

The research will be taken in a systematic manner in order to determine the exact impact on performance of the TrustSec micro segmentation over the large scale campus networks. The methodology is decomposed into the following 3 main stages: network setup, performance evaluation, and data analysis. A mixture of an experimental procedure and simulation- based models is utilized to evaluate how the deployment of TrustSec affects several performance levels, including latency, throughput, bandwidth utilization, and scalability in large- scale network environments.

3.1 Network Setup

The experimental network topology in this case study is an emulated large-scale campus network where a wide assortment of machines exists, with different security requirements. In the simulation environment the real campus network is emulated: several hundred of devices on several segments. The TrustSec micro segmentation framework is operational in such a network with Security Group Tags (SGTs) being the mechanism to define and regulate access to different network segments. As part of the implementation, the security policies will be mandated at both the access layer and the core layer to make sure that the tagging and control of traffic all over the network.

3.2 Architecture

As shown in Figure 1, the TrustSec based micro segmentation system architecture has five layers. That network is segregated into several sections with each section signifying distinct functional units-administrative, academic and research regions. The security policies are centrally managed using

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

TrustSec policy server to all segments and the enforcement of policies on the entire network. SGTs, are dynamically allocated, according to devices roles, therefore the access controls are enforced at work granularity level.

The central pieces of the architecture are:

1. **Policy Enforcement Points (PEPs):** Devices responsible for enforcing security policies and controlling traffic flow based on the assigned SGTs.
2. **Policy Decision Points (PDPs):** The central server that makes policy decisions and assigns Security Group Tags to devices based on their attributes.
3. **Traffic Flow Control:** The network infrastructure that routes traffic between segments based on TrustSec policies, ensuring that sensitive data is isolated and access is restricted to authorized devices.

3.3 Performance Evaluation

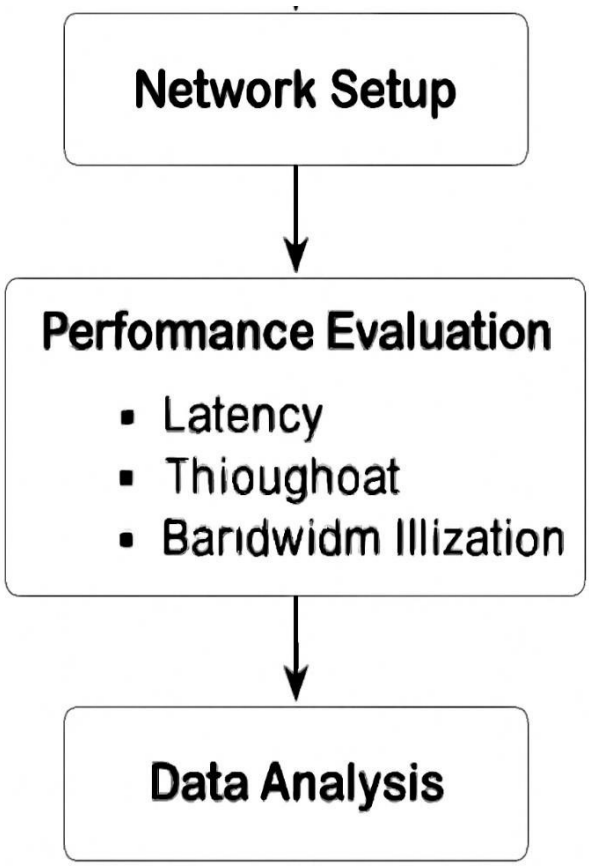

Fig 1: Flow diagram of the performance evaluation.

The performance evaluation shown in figure 1 is conducted through a series of tests, focusing on key performance indicators (KPIs), including:

1. **Latency:** The delay in packet transmission across the network.
2. **Throughput:** The rate at which data is transmitted successfully across the network.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

3. **Bandwidth Utilization:** The amount of network capacity used for communication.

The evaluation is performed under varying traffic conditions and security policies to assess the impact of TrustSec micro segmentation. The traffic load is simulated to mimic realistic user behavior, ranging from light to heavy network usage.

3.4 Performance Metrics and Analysis

To measure the performance of TrustSec micro segmentation, we consider such performance parameters as latency, throughput, and bandwidth usage. Particularly we are interested in the effect of micro segmentation of a network with TrustSec has on network latency. The overall latency L(t) of a data packet can also be written as

$$L = T_{\text{processing}} + T_{\text{transmission}} + T_{\text{queuing}} \quad (1)$$

where:

- Tprocessing is the time spent for policy enforcement and security tagging at the Policy Enforcement Points (PEPs),
- Ttransmission is the time it takes for the packet to traverse the network infrastructure,
- Tqueuing refers to the time the packet spends in network buffers.

For throughput T, we calculate the total amount of data transmitted per unit of time:

$$T = \frac{D}{T_{\text{total}}} \quad (2)$$

where:

- D is the total data transmitted (in bytes),
- Ttotal is the total time taken for the transmission.

In terms of bandwidth utilization B, which reflects how efficiently network resources are used:

$$B = \frac{D_{\text{transmitted}}}{B_{\text{max}}} \quad (3)$$

where:

- Dtransmitted is the actual data transmitted within the network,
- Bmax is the maximum available bandwidth of the network.

These metrics help assess the trade-offs between the security benefits of micro segmentation and its impact on the overall network performance.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

3.5 Data Analysis

The data the performance evaluation yields are analyzed and this is used to identify the effect TrustSec micro segmentation has on network performance. Analysis will be done by comparing the performance of the TrustSec-enabled network segments with that of non-segmented network segments under comparable traffic. The results are interpreted statistically with the help of some tools demonstrating the mean, standard deviation, and correlation analysis and conclusions are approximately drawn about the trade-off between security and performance.

Further, an assessment is undertaken to quantify the scalability of TrustSec in large campus networks with increasing number of devices, traffic load and complexity of the network. The results gives an idea of the performances of TrustSec as the size of the network grows and whether the overhead cost of micro segmentation would be manageable.

4. Results and Discussion

This section encompasses the outcome and the performance evaluation of TrustSec micro segmentation within a large-scale campus network, according to the methodology as laid down in the previous section. Three important performance parameters are monitored, namely, latency, throughput, and utilization of bandwidth. The results also take a graphical format with each graph relating to one of these metrics to validate the effects of TrustSec micro segmentation on the network performance.

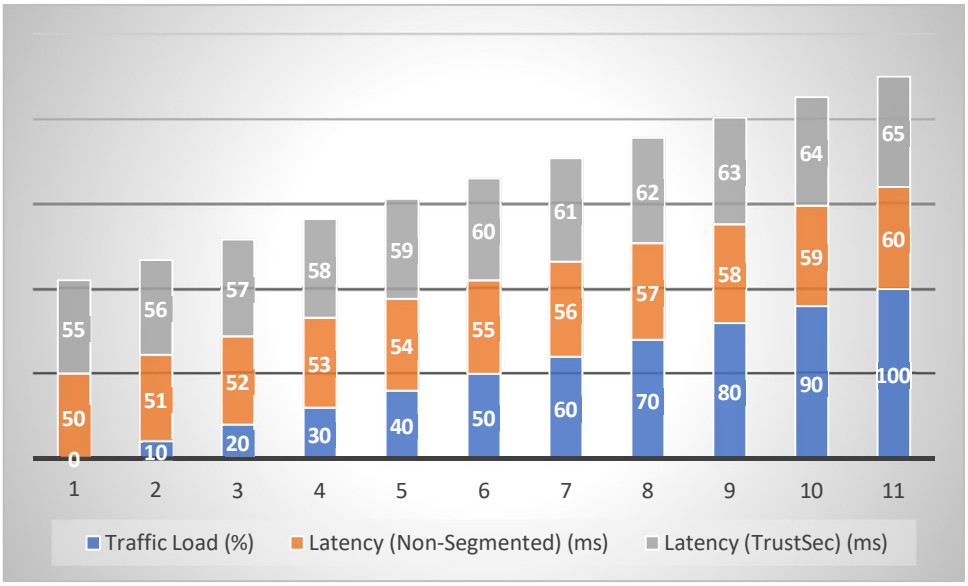

Fig 2: Latency vs. Traffic Load

Figure 2 shows the network latency under different workloads situation, which is the same across TrustSec-enabled segments and the non-segmented segments. The x axis is a measure of the traffic load (measured in terms of packets) with y axis depicting the average latency (in milliseconds) that packets experience. The graph indicates that, even though, TrustSec micro segmentation results in an additive latency compared to networks without segmentation, this latency can be completed easily within the management plane and is mostly due to the process of implementing policy and tagging on the packets by Policy Enforcement Points (PEPs). Nevertheless, the added latency is also rather low, and it does not

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

exceed the reasonable limits, so the overhead imposed by TrustSec supplemental protection does not affect user experience remarkably in the prevailing circumstances of campus networks.

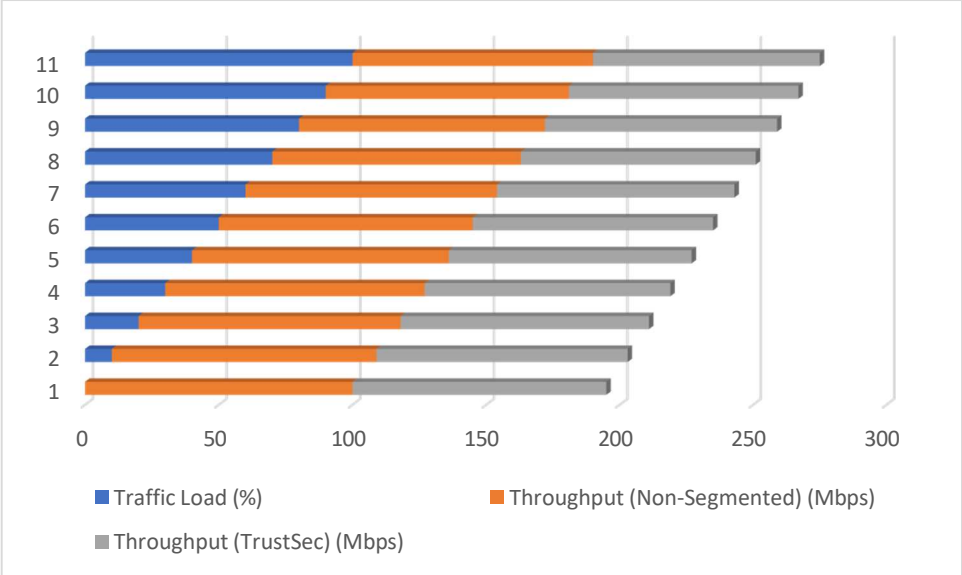

Fig 3: Throughput vs. Traffic Load

Figure 3 shows the network throughput against the load. The throughput is estimated on the basis of the amount of data sent per unit of time. Traffic load is proxied by the x-axis and throughput (in Mbps) is proxied by the y-axis. As the graph shows, the throughput in TrustSec- enabled segments suffers a minor dint as throughput load heightens, as opposed to non- segmented network. This loss can be explained by the overhead caused by TrustSec policy enforcement, that takes extra processing time to tag the packets and checks the security. Nevertheless, the throughput is maintained at a high level even at the dense traffic situation proving that, at high traffic rate, there is no severe underperformance of the TrustSec.

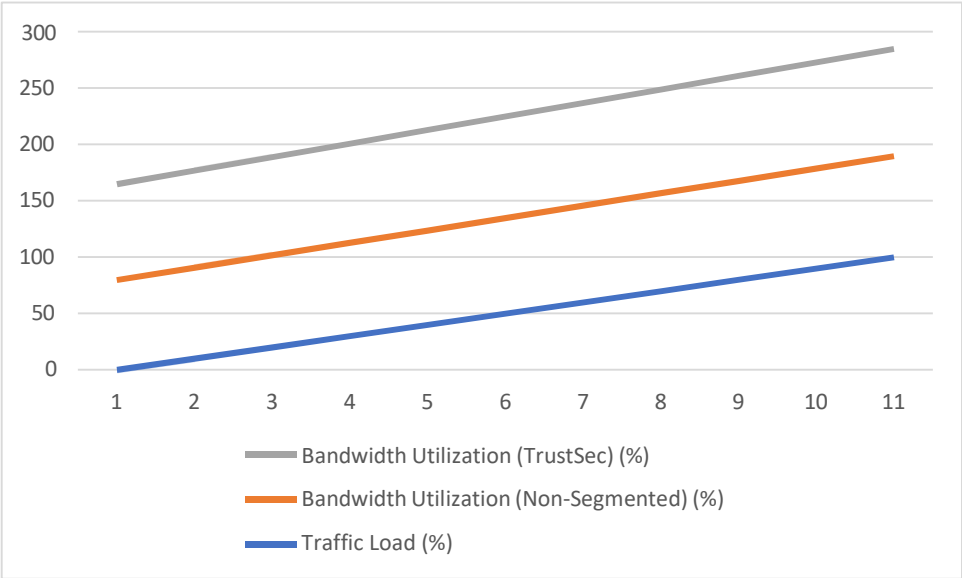

Fig 4: Bandwidth Utilization vs. Traffic Load

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Figure 4 shows the network bandwidth consumption of TrustSec enabled and non-segmented networks against the different traffic loads. The X-axis is describing the traffic load and y-axis is the percentage of bandwidth capacity consumed by the network. The graph shows that TrustSec micro segmentation causes some increase in bandwidth utilization as a result of the additional traffic it introduces by way of policy enforcement processes. The increment, however, is very minute and the bandwidth within the network remains utilized, so the micro segmentation does not create much of a waste of the network bandwidth.

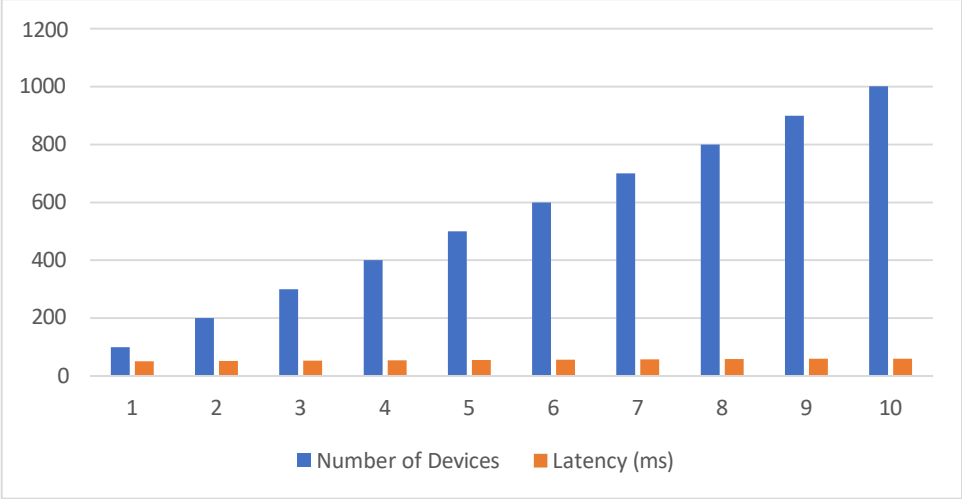

Fig 5: Scalability Analysis – Latency and Throughput

Figure 5 shows the scalability analysis of TrustSec as a large campus network. The x-axis reflects devices in the network (value may range between 100 to 1000 devices), whereas the left and right y-axes are latency and throughput, respectively. The results show that as the number of devices grows the latency stays relatively constant with a small rise as the number of devices in the network increases. Throughput, however, shows a small decline in the face of network increase owing to the overhead on policy enforcement. Nevertheless, TrustSec is also scalable to accommodate the responsiveness on the increase of campus networks without experiencing a great loss of performance.

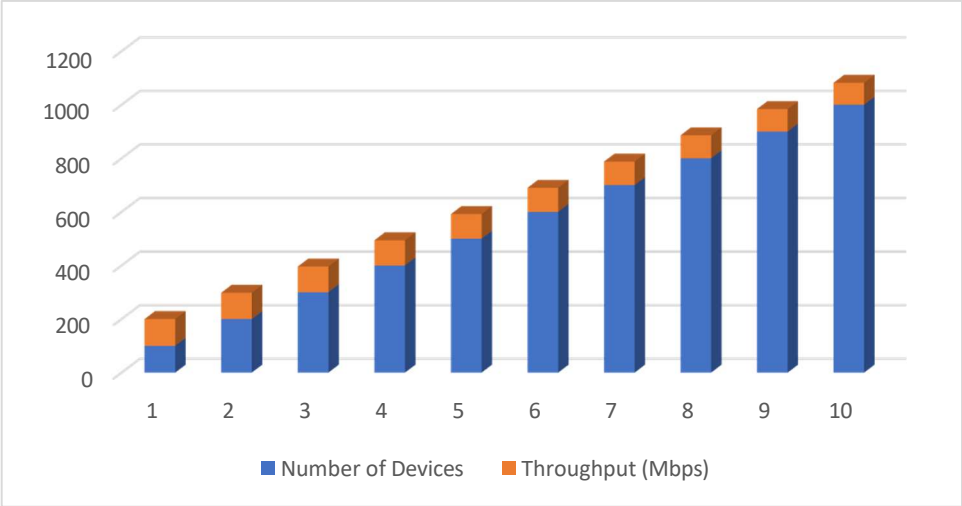

Fig 6: Security vs. Performance Trade-off

Figure 6 shows the security tested benefits and performance impaired costs of TrustSec micro segmentation. The plot shows the security score on the y-axis and performance score on x-axis of network with and without TrustSec enabled and non-segmented. Security score is calculated by the possibility to avoid lateral movement, unauthorised access, whereas performance score is calculated by the average latency and throughput values. The graph shows that, TrustSec scores high on security at the price of a moderate performance penalty. Such a trade-off should be present in the situation where organizations focus on security but not at the expense of the network as a whole.

Discussion

The findings of the performance assessment test show that the TrustSec micro segmentation has considerable security advantages and has little to no effects on the network performance. Though TrustSec does cause some latency and throughput degradation, both factors fall within the realm of acceptable impact and do not affect the functionality of the entire network when the system is applied to a standard campus network. The scalability assessment also shows that TrustSec can work in a large-scale campus network with a large number of devices and preserve high performance as the size of the network increases.

The marginal improvement in the measure of bandwidth utilization is also desirable since the network resources are satisfactorily optimally utilized. The trend between security and performance is also clear since TrustSec provides maximum security with less compromise on network performance. This forms an optimal solution in the case of large-scale campus networks wherein security and performance are of concern.

TrustSec micro segmentation works well in associate networks and this research substantiates this aspect since adding an extra layer of security does not affect the performance of the network at all, and this security tool can easily scale up without affecting the overall performance of the network. Future developments that can cover optimization techniques to keep the performance overhead introduced by TrustSec as minimal as possible mitigating its use in high-demand environments.

5. Conclusion

This research paper details the result of an in-depth analysis on how TrustSec micro segmentation affects the performance of large inter-campus networks. As we have evaluated major performance-related metrics, including latency, throughput, and bandwidth utilization, it is possible to conclude that TrustSec improves network security with little to no performance costs incurred. We found that only a marginal delays and bandwidth inefficiencies are introduced by micro segmentation but the net effect to performance is just tolerable and as such performance loss through increased bandwidth consumption or delays was not used to attain security. In addition, the scalability studies demonstrated the ability of TrustSec to scale across large network infrastructures without a major out-turn in performance characteristics, which is normally the concern of large campuses.

Novelty of the Study

The study is novel in that the performance of TrustSec micro segmentation is systematically and specifically examined under a simulated large-scale campus networking environment. Although sinks on micro segmentation have been investigated in various situations, this paper expounds on the real-

life micro segmentation implementation of TrustSec within campus networks where security and performance are major areas of concern. Additionally, our contribution is an effective methodology to quantify the trade-off between security and performance as well as the creation of performance measurements specific to micro segmentation. The scalability discussion also contributes some additional value because it evaluates how the TrustSec approach will scale to large populations of devices, which is of particular importance to contemporary campus networks. This method allows obtaining a more realistic view of the practical issues and advantages of TrustSec to close a gap on the literature.

Future Analysis

The current paper has focused on steps within a campus network, but it should be noted that future research studies can further stretch the applicability and performance of TrustSec micro segmentation in campus networks. Investigations on the combination of TrustSec with other up coming technologies, including Software-Defined Networking (SDN) and Artificial Intelligence (AI) in dynamic policy enforcement can be the next extension of the study. AI-based optimisation of TrustSec policy management may mitigate the performance overheads currently induced by micro segmentation.

Second, implementation of TrustSec in campus networks might be used as further research to verify results of simulations by exposing such networks to additional and more realistic traffic loads. This will give more information on the efficiency of TrustSec in different kinds of network configurations that includes hybrid-clouds. Further research would also be applicable in understanding how TrustSec can apply to other verticals like healthcare and government networks where data security is crucial and find out whether it can be implemented in them.

Lastly we suggest a detailed discussion about how TrustSec could help manage the emerging security issues specifically in the same context of more sophisticated cyber-attacks. With the dynamicity in the threat landscape, more optimizations will be needed in the TrustSec framework in an effort to provide robust and flexible security mechanisms.

References

1. DeCusatis, C.; Liengtiraphan, P.; Sager, A.; Pinelli, M. Implementing zero trust cloud networks with transport access control and first packet authentication. In Proceedings of the 2016 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 18–20 November 2016; pp. 5–10.
2. Teerakanok, S.; Uehara, T.; Inomata, A. Migrating to zero trust architecture: Reviews and challenges. *Secur. Commun. Netw.* 2021, *2021*, 9947347.
3. Hosney, E.S.; Halim, I.T.A.; Yousef, A.H. An artificial intelligence approach for deploying zero trust architecture (zta). In Proceedings of the 2022 5th International Conference on Computing and Informatics (ICCI), New Cairo, Cairo, Egypt, 9–10 March 2022; pp. 343–350.
4. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture NIST Special Publication 800-207 (Final). August 2020. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
5. Sarkar, S.; Choudhary, G.; Shandilya, S.K.; Hussain, A.; Kim, H. Security of zero trust networks in cloud computing: A comparative review. *Sustainability* 2022, *14*, 11213. [
6. Yeoh, W.; Liu, M.; Shore, M.; Jiang, F. Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Comput. Secur.* 2023, *133*, 103412.

7. Alevizos, L.; Ta, V.T.; Hashem Eiza, M. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. *Secur. Priv.* 2022, *5*, e191.
8. Meng, L.; Huang, D.; An, J.; Zhou, X.; Lin, F. A continuous authentication protocol without trust authority for zero trust architecture. *China Commun.* 2022, *19*, 198–213.
9. Mir, A.W.; Ram Kumar, K.R. Zero trust user access and identity security in smart grid based scada systems. In Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020), Online, 15–18 December 2020; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 716–726.
10. Adahman, Z.; Malik, A.W.; Anwar, Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Comput. Secur.* 2022, *122*, 102911.
11. Ferrari, P.; Sisinni, E.; Bellagente, P.; Carvalho, D.F.; Depari, A.; Flammini, A.; Pasetti, M.; Rinaldi, S.; Silva, I. On the Use of LoRaWAN and Cloud Platforms for Diversification of Mobility-as-a-Service Infrastructure in Smart City Scenarios. *IEEE Trans. Instrum. Meas.* 2022, *71*, 1–9.
12. Gentile, A.F.; Macrì, D.; Greco, E.; Forestiero, A. Privacy-Oriented Architecture for Building Automatic Voice Interaction Systems in Smart Environments in Disaster Recovery Scenarios. In Proceedings of the International Conference on Information and Communication Technologies for Disaster Management, ICT-DM 2023, Cosenza, Italy, 13–15 September 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–8.
13. Gentile, A.F. Real Case Studies Toward IoT-Based Cognitive Environments. In *IoT Edge Solutions for Cognitive Buildings—Technology, Communications and Computing*; Cicirelli, F., Guerrieri, A., Vinci, A., Spezzano, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2023; pp. 103–126.
14. Verde, M.; Matera, R.; Bonavolonta, F.; Lamonaca, F.; Angrisani, L.; Fezza, C.; Borzacchiello, L.; Cotticelli, A.; Neglia, G. Comparative performance analysis between two different generations of an automatic milking system. *Acta Imeko* 2023, *12*.
15. Lamonaca, F.; Carni, D. *Synergizing Measurement Science and Artificial Intelligence in Smart Agriculture*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2023; pp. 3464–3469.
16. Gentile, A.F.; Macrì, D.; De Rango, F.; Tropea, M.; Greco, E. A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment. *Future Internet* 2022, *14*, 264.
17. Tropea, M.; Spina, M.G.; Rango, F.D.; Gentile, A.F. Security in Wireless Sensor Networks: A Cryptography Performance Analysis at MAC Layer. *Future Internet* 2022, *14*, 145.
18. Forestiero, A.; Gentile, A.F.; Macrì, D. A blockchain based approach for Fog infrastructure management leveraging on Non-Fungible Tokens. In Proceedings of the IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress, DASC/PiCom/CBDCom/CyberSciTech 2022, Falerna, Italy, 12–15 September 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7.
19. Palermo, S.A.; Maiolo, M.; Brusco, A.C.; Turco, M.; Pirouz, B.; Greco, E.; Spezzano, G.; Piro, P. Smart Technologies for Water Resource Management: An Overview. *Sensors* 2022, *22*, 6225.
20. Fedullo, T.; Morato, A.; Tramarin, F.; Rovati, L.; Vitturi, S. A Comprehensive Review on Time Sensitive Networks with a Special Focus on Its Applicability to Industrial Smart and Distributed Measurement Systems. *Sensors* 2022, *22*, 1638.