SafeAssign Originality Report

Fall 2019 - Cloud Computing (ITS-532-02) - First Bi-Ter... • Week 5 - Assignment

View Originality Report - Old Design

Chandan Gopu

Total Score: Medium risk 40 %

Submission UUID: 51ee218c-4327-b065-c42d-c639a2ac5cef

Total Number of Reports	Highest Match	Average Match	Submitted on	Average Word Count
1	40 % Microsegmentation and Ze...	40 %	09/27/19 07:13 PM EDT	1,484 Highest: Microsegmentatio...

Attachment 1 40 %

Word Count: 1,484
Microsegmentation and Zero Trust Security.docx

Institutional database (9) 37 %

② *Student paper*
⑩ *Student paper*
⑤ *Student paper*
④ *Student paper*
⑪ *Student paper*
① *Student paper*
⑥ *Student paper*
⑨ *Student paper*
③ *Student paper*

Internet (2) 3 %

⑦ *itworld*
⑧ *softwarestrategiesblog*

Top sources (3)

② *Student paper*
④ *Student paper*
⑥ *Student paper*

Excluded sources (0)

Running head: ① MICROSEGMENTATION AND ZERO TRUST SECURITY 1

② MICROSEGMENTATION AND ZERO TRUST SECURITY 8

Microsegmentation and Zero Trust Security

Chandan Gopu

③ University of the Cumberlands

Introduction

Segmentation has been critical for the ongoing maturity of network environments and architectures. The network architecture has evolved from shared hubs to switches as technology has matured and began to use network virtualization. Over time, network environments have shrunk the collision domain to two main participants (the end node and the switch) and offered a huge jump in performance and capabilities. Organizations are gradually turning away from conventional security models that secure the network perimeter and then trust everyone or everything inside and are instead gravitating towards a Zero Trust Security (ZTS) model to protect sensitive data and resources. The use of microsegmentation and Zero Trust Security have revolutionized the network environments and architectures. Unlike conventional security models that were prone to data exfiltration, ZTS model is typically the best because it prevents cyberattacks and network intruders from exploiting weaknesses in the network/or system perimeter to gain entry, and once inside the network, move laterally to access sensitive data and application. ④ Unlike physical segmentation which is done in a physical network, microsegmentation is executed in an overlay or virtual network that is independent of network addressing or physical architecture. This paper is structured into the analysis of the differences between physical Network Segmentation and microsegmentation, zero trust security (ZTS) vs. conventional security models and offering reasons why organizations should implement ZTS model. Question 1. ⑤ Physical Network Segmentation vs. Microsegmentation

Microsegmentation is a security technique that allows companies to set up granular security policies for users and device access to specific data, applications, and devices. Microsegmentation allows organizations to segment network in a real-time, virtualized manner that is independent of network addressing or physical architecture (Klein, 2019). Microsegmentation was originally used to moderate lateral traffic between servers in a similar segment, but it has evolved to incorporate intra-segment traffic that enables Application A to talk with Host B or server A to communicate to server B. On the other hand, physical segmentation is technique of breaking down a large network into sub-networks or smaller physical components to prevent attackers from attacking laterally once they have accessed the perimeter of the network. Physical segmentation often involves investing in additional hardware such as routers, switches, and access points. ⑥ Physical segmentation mainly involves the use of virtual local area networks (VLANs), firewalls, and access control lists (ACL) to improve the security of the network. ④ Physical segmentation is considered a north-south network traffic control whereas microsegmentation is considered east-west traffic control. Physical segmentation is referred to a north-south because once inside a network's designated zone, users, software, or communication are trusted. Physical segmentation allows an organization to set up course policies whereas microsegmentation allows organizations to set up granular policies. ④ Microsegmentation occurs in overlay or virtual network whereas physical segmentation occurs in a physical network (Conde & Benedetto, 2017). Microsegmentation is done in software whereas physical segmentation is done in hardware. ⑦ The use of software in microsegmentation makes it easier and efficient to define the fine-grained segments. ④ Microsegmentation is workload level/or identity based whereas physical segmentation is network level/or address based. Question 2. ⑧ Zero Trust Security

⑥ Zero trust security (ZTS) is an information technology (IT) security model that demands/require strict identity verification for every device and person trying to access resources on a private network, regardless of whether the person or device is sitting outside or within the perimeter of the network. ⑨ It is a holistic approach to the security of a network that includes several different technologies and principles (Ali et al., 2015). ZTS implies that is no person or device is trusted by default from outside or inside the network, and verification is mandatory for every person trying to gain access to the network's resources. ⑩ The core philosophy behind ZTS is that there are attackers both outside and within the perimeter of the network, so no device, or machines, or users should be automatically trusted. ZTS is based on the assumption that all devices, users, and transactions are already compromised and thus should not be trusted. Unlike traditional security models, ZTS has been proven to prevent data breaches. Conventional security models are based on the castle-and-moat concept whereas ZTS is based on least-privilege access concept (zero trust on users both within and outside the network).

The castle-and-moat concept involves making it hard to access information from outside the network, but every device/machine/or person inside the network is trusted automatically or by default. Basically, Conventional security models trust internal users whereas ZTS does not trust both inside and outside users (Ali et al., 2015). ZTS utilize microsegmentation whereas conventional security models tend to utilize physical segmentation. In cloud computing, zero trust security (ZTS) support ubiquitous security because it thwarts all the threats emanating from within and outside the perimeter of the network. Question 3. Microsegmentation for Zero Trust Security (ZTS) The heart of ZTS model is fine-grained microsegmentation topography. Microsegmentation carves network into smaller granular nodes that are important in the implementation of ZTS model. Microsegmentation provides distinct security segments (micro-segments) for ZTS model. Microsegmentation also protects the east-west traffic and the network perimeter and thus ensuring that the implementation of ZTS is executed properly (Bansal et al., 2018). It also provides a platform for granular enforcement of ZTS model. This is very important ensuring that ZTS model only accepts trusted traffic that are has been verified. Because microsegmentation is based on least-privilege access, it is vital in the implementation of ZTS model because it enhances proper management of traffic both within and outside the network perimeter of an organization. Organizations should implement a Zero Trust Security approach because it reliably prevents the exfiltration of private/or sensitive information and enhances their ability to defend against contemporary cyberthreats. A ZTS approach ensures security and an excellent end-user experience (DeCusatis et al., 2016). ⑥ In the past, organizations have had to make hard tradeoffs between productive user experience and strong security. Highly secure passwords used in the past were unproductive because one could spend a lot of time trying to remember the lengthy passwords. ZTS approach also protects an organization's data and protect customers (Vanickis et al., 2018). With ZTS model, it is very easy to identify services or applications that attempt to access or communicate inside or outside the network. After verifying the authenticity of users, devices, or applications, ZTS allows only those that are trustworthy and valid. ⑥ Therefore, implementing an effective ZTS model ensure that only authorized and authenticated devices and users can access data and application. This assist to prevent and mitigate data intrusion, exfiltration, and many of these negative consequences. Conclusion

⑪ Adoption of microsegmentation and Zero Trust Security (ZTS) help to improve the security posture of any network and attached systems. Organizations that utilize ZTS and microsegmentation stand to benefit a lot because both reduce the risks of attacks, reduce total attack surface of a network security incident, securely isolate applications and networks from each other, and limit the ability to access and expand from a compromised network or systems. Unlike conventional security models that were prone to data exfiltration, ZTS approach is typically the best because it thwarts cyberattacks and network intruders from exploiting weaknesses in the network/or system perimeter to gain entry, and once inside the network, move laterally to access sensitive data and application. When setting a ZTS model, microsegmentation should be enforced in order to provide much-needed granular nodes and distinct security segments for effective implementation. Microsegmentation and ZTS go hand-in-hand so as to provide proper and effective management of east-west traffic and the network perimeter. It is not advisable to use physical segmentation because attackers within the network can exploit weaknesses in the network for their own benefit. Therefore, it is recommended for organizations to have a hybrid or intertwined microsegmentation and Zero Trust Security (ZTS) to their network architectures or environment. References

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). ⑧ Security in cloud computing: Opportunities and challenges. Information sciences, 305, 357-383. Bansal, K., Sengupta, A., Manuguri, S., Krishna, S., & Pereira, J. (2018). U.S. ⑤ Patent Application No. 15/381,123. Conde, D., & Benedetto, F. (2017). Software-defined perimeters: An architectural view of sdp. ② DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M. (2016, November). ② Implementing zero trust cloud networks with transport access control and first packet authentication. In 2016 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 5-10). IEEE. Klein, D. (2019). Micro-segmentation: ② securing complex cloud environments. Network Security, 2019(3), 6-10. Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018, June). ② Access Control Policy Enforcement for Zero-Trust-Networking. In 2018 29th Irish Signals and Systems Conference (ISSC) (pp. 1-6). IEEE

Source Matches (23)

① *Student paper* 100%

Student paper	Original source
MICROSEGMENTATION AND ZERO TRUST SECURITY 1	MICROSEGMENTATION AND ZERO TRUST SECURITY 1

② *Student paper* 93%

Student paper	Original source
MICROSEGMENTATION AND ZERO TRUST SECURITY 8 Microsegmentation and Zero Trust Security	Microsegmentation And Zero Trust Security Microsegmentation And Zero Trust Security

③ *Student paper* 100%

Student paper	Original source
University of the Cumberlands	University of the Cumberlands

④ *Student paper* 66%

Student paper	Original source
Unlike physical segmentation which is done in a physical network, microsegmentation is executed in an overlay or virtual network that is independent of network addressing or physical architecture.	· Physical Network Segmentation is applicable in physical networks, whereas, Microsegmentation is an Overlay network or virtual network

⑤ *Student paper* 100%

Student paper	Original source
Physical Network Segmentation vs.	Physical Network Segmentation vs

⑥ *Student paper* 73%

Student paper	Original source
Physical segmentation mainly involves the use of virtual local area networks (VLANs), firewalls, and access control lists (ACL) to improve the security of the network.	Network segmentation has its security with the assistance of firewalls, virtual local area networks (VLAN) and access control lists (ACL)

④ *Student paper* 92%

Student paper	Original source
Physical segmentation is considered a north-south network traffic control whereas microsegmentation is considered east-west traffic control.	· Physical Network Segmentation is considered as a North-South network traffic control, whereas, Microsegmentation is considered as East-West network traffic control

④ *Student paper* 68%

Student paper	Original source
Microsegmentation occurs in overlay or virtual network whereas physical segmentation occurs in a physical network (Conde & Benedetto, 2017).	· Physical Network Segmentation is applicable in physical networks, whereas, Microsegmentation is an Overlay network or virtual network

⑦ *itworld* 78%

Student paper	Original source
The use of software in microsegmentation makes it easier and efficient to define the fine-grained segments.	Microsegmentation is typically done in software, which makes it easier to define fine-grained segments

④ *Student paper* 76%

Student paper	Original source
Microsegmentation is workload level/or identity based whereas physical segmentation is network level/or address based.	· Physical Network Segmentation is an address based or a network level based in the network, whereas, Microsegmentation is an identity based or a workload level based in the data center or network

⑧ *softwarestrategiesblog* 100%

Student paper	Original source
Zero Trust Security	Zero Trust Security

⑥ *Student paper* 70%

Student paper	Original source
Zero trust security (ZTS) is an information technology (IT) security model that demands/require strict identity verification for every device and person trying to access resources on a private network, regardless of whether the person or device is sitting outside or within the perimeter of the network.	Zero trust security is an IT security model that needs strict identification for each person and device making an attempt to access resources on a private network, in spite of whether or not they are sitting at inside or outside of the network perimeter

⑨ *Student paper* 63%

Student paper	Original source
It is a holistic approach to the security of a network that includes several different technologies and principles (Ali et al., 2015).	It is an all-inclusive approach to network security that includes more than a few different principles and technologies

⑩ *Student paper* 72%

Student paper	Original source
The core philosophy behind ZTS is that there are attackers both outside and within the perimeter of the network, so no device, or machines, or users should be automatically trusted.	The Zero point security model assumes that there are attackers both within and outside of the network, so no users or machines should be automatically trusted

⑥ *Student paper* 66%

Student paper	Original source
In the past, organizations have had to make hard tradeoffs between productive user experience and strong security.	Organizations have had to create tradeoffs between great securities, productive user experience

⑥ *Student paper* 69%

Student paper	Original source
Therefore, implementing an effective ZTS model ensure that only authorized and authenticated devices and users can access data and application.	Implementing an efficient zero trust ensure that only authenticated and authorized users and devices can access applications

⑪ *Student paper* 69%

Student paper	Original source
Adoption of microsegmentation and Zero Trust Security (ZTS) help to improve the security posture of any network and attached systems.	Adoption of Zero Trust and Micro-Segmentation as core design principles can help improve the security posture of network and attached systems

⑧ *softwarestrategiesblog* 71%

Student paper	Original source
Security in cloud computing:	Cloud Computing in Manufacturing

⑤ *Student paper* 100%

Student paper	Original source
Patent Application No.	Patent Application No

② *Student paper* 100%

Student paper	Original source
DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M.	DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M

② *Student paper* 100%

Student paper	Original source
Implementing zero trust cloud networks with transport access control and first packet authentication. In 2016 IEEE International Conference on Smart Cloud (SmartCloud) (pp.	Implementing zero trust cloud networks with transport access control and first packet authentication In 2016 IEEE International Conference on Smart Cloud (SmartCloud) (pp

② *Student paper* 100%

Student paper	Original source
securing complex cloud environments. Network Security, 2019(3), 6-10. Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B.	securing complex cloud environments Network Security, 2019(3), 6-10 Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B

② *Student paper* 100%

Student paper	Original source
Access Control Policy Enforcement for Zero-Trust-Networking. In 2018 29th Irish Signals and Systems Conference (ISSC) (pp.	Access Control Policy Enforcement for Zero-Trust-Networking In 2018 29th Irish Signals and Systems Conference (ISSC) (pp