Segmentrix: A Network Visualization Tool to Develop and Monitor Micro-Segmentation Strategies

Aditeya Pandey* Northeastern University
Larry Chan† Illumio Inc.
Raven Gao‡ Illumio Inc.
Joy Scott§ Illumio Inc.
Brian Staats¶ Illumio Inc.

Abstract

Micro-Segmentation enables organizations to logically divide the datacenter into distinct security segments down to the individual workload level, and then define security controls for each unique segment. Micro-segmentation allows flexible organization of network assets into meaningful groups. For example, workloads in a network can be divided into production and development environments, and policy can control communication between the environments. Network visualization plays a critical role in the development and maintenance of segmentation. In an unsegmented network, a network visualization of workload communication can help domain users assess dependencies and create segmentation policies. Whereas, in segmented networks, the visualization of traffic between individual workloads and segmented groups can be essential for monitoring security compliance. We present a systematic overview of micro-segmentation visualization goals and use the goals to develop Segmentrix a novel tool which aids organizations to segment and monitor their networks.

Index Terms: Human-centered computing—Visualization—Visualization techniques—Adjacency-Matrix; Human-centered computing—Visualization—Visualization design

1 Introduction

Micro-segmentation is an emerging security practice of applying security controls to the datacenter and cloud assets that have an explicit business purpose for communicating with each other. Micro-segmentation is built on the principle of flexibility, which makes it different from traditional network segmentation and firewall implementation. Flexibility expresses security policies in abstract but meaningful concepts (such as web, application, and database tiers) rather than in terms of network constructs (such as IP addresses, subnets, and VLANs).

Visualization plays a crucial role in the development and analysis of segmentation strategies [1–3]. Previously, adjacency matrices have been used to visualize network segmentation with constructs like IP addresses [2, 3]. Kim et al. [2] justify the use of matrix based on three parameters: scalability with data, readability of nodes, and visibility of links. These factors also extend to the micro-segmentation goals. More specifically, readability and visibility of the network are essential for developing segmentation strategies. Readability ensures the users have context when analyzing nodes, like information about the critical nodes, and visibility of links reduces the chances of missing vulnerable connections [4] while writing security policies.

We contribute a systematic overview of micro-segmentation visualization design goals. And use the goals to develop Segmentrix: a novel network visualization that supports development and monitoring of micro-segmentation strategies.

*e-mail: pandey.ad@husky.neu.edu
†e-mail: larry.chan@illumio.com
‡e-mail: raven.gao@illumio.com
§e-mail: joy.scott@illumio.com
¶e-mail: brian.staats@illumio.com

2 Domain Goals

We discuss micro-segmentation domain goals from the context of development of strategies and monitoring of network post-segmentation.

Develop: To develop micro-segmentation strategies, users need visibility of their network and an interface to write security policy to establish communication protocol. Therefore, we identify two tasks a visualization tool should support for development of micro-segmenation strategies: **Goal 1**: Visualize dependencies and traffic flow between workloads. **Goal 2**: Segement(divide) the network into groups and write security policies.

Monitor: Segmentation is a manual task, to support post-segmentation validation and monitor strategies, we recognize that a visualization tool should support the following tasks. **Goal 1**: Visualize connection between segments. **Goal 2**: Drill down on segments to analyze them in isolation. **Goal 3** Update Policies.

3 Data and Visual Encoding

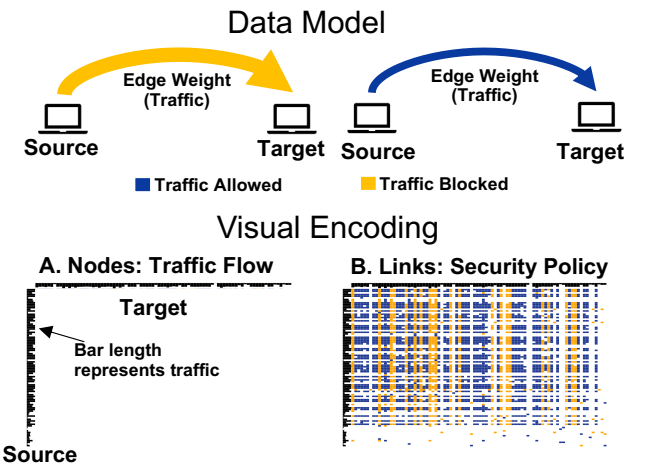

Figure 1: Micro-segmentation uses network data, where nodes represent workloads and a connection has two attributes traffic and policy. For the visualization, source node and target nodes are placed separately on the vertical and horizontal axes. The bar length encodes traffic between the source and target nodes. Further, the security policy is represented by the color-coded cell in the matrix.

Data Model: Datacenter network is a directed network. In the directed network, a workload(source node) requests a client(a target) for information. The client responds based on the established security policy. In Fig. 1: Data Model, a link in the network encodes total traffic flow and the state of the policy (Fig. 1: Data Model).

Visual Encoding: In Fig. 1: Visual Encoding, we explain the mapping of network data to an adjacency matrix. Nodes are explicitly represented on the vertical(source) and horizontal(target) axes, and each node represents the total number of requests as the bar

length. Matrix cell encodes the policy decision set by the security analyst.

Data: In the poster abstract, we use randomly generated data.

4 SEGMENTRIX

Segmentrix is a network visualization tool that supports micro-segmentation task. The tool supports exploration of the network, segmentation of the workloads into meaningful groups, defining security polices and analysis of segments using filtering and interaction.

Fig. 2 shows a typical workflow adopted by a Security Analyst in developing segments and writing security policy. The task involves three main activities, exploring the network, grouping of workloads and writing security policy. Segmentrix uses an adjacency matrix to show the network. Interaction in Segmentrix allows exploration of links and traffic. Users can order nodes based on attributes like traffic. Segmentrix supports sorting of nodes by traffic, moving the most connected nodes to the top and left corner of the interface (Fig. 2 B). After, analyzing the network users can segment or divide the nodes into meaningful groups (Fig. 2 C). For example, all the workloads which store credit card information can be placed in one group and isolated with security policies from the rest of the network. For grouping and policy writing, Segmentrix allows users to define labels for nodes and policies for links. Segmentation and policy implementation can also be done outside the tool with advanced segmentation softwares.

Figure 2: Develop Segmentation Strategies: Sub-Fig. A shows an unsegemented network, in Sub-Fig. B nodes have been sorted by the traffic volume for each node. In Sub-Fig. C, we demonstrate logical segments created by the security analysts. And in Sub-Fig. D we show that security analyst secures communication between workloads based on network segments.

Post segmentation, analysts can use Segmentrix dashboard to validate and update their security policies. Sometimes analyst may want to explore the topology of the network. To ease the visualization of topology, we display a node-link visualization of a selected segment in the adjacency matrix. In Fig. 3, the highlighted source workloads, and all the connected target workloads are displayed as a node-link visualization in the linked widget.

A crucial task in monitoring of network is the ability to drill down on data and analyze segments of interest. Segmentrix allows users to filter the data by grouping label, for example in Fig. 4, the user has filtered all the source workloads which were grouped as 'Production'. The filtered view can useful for anomaly detection. As the analyst is dealing with a smaller focused group of workloads, they can look for patterns that may have been missed in the overview mode of Segmentrix.

Figure 3: Segmentrix supports interaction to analyze segments. In this figure, the user has selected a segment to analyze. The selection highlights the source segment and all the connected target segments. For context, we also display the node-link visualization of the selected segments.

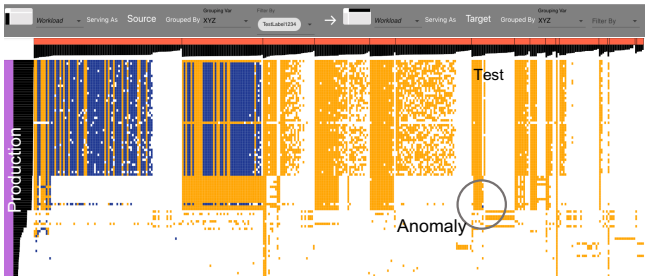

Figure 4: Segmentrix allows filtering data to analyze segments in isolation. The navigation bar at the top shows the label XYZ as the grouping variable. Further, the user has filtered out TestLabel1234 from the dataset to analyze in isolation. After filtering, we notice an anomaly, where all but one connection is allowed between segments TestLabel1234 and Test.

5 CONCLUSION

We present an overview of micro-segmentation visualization goals and the corresponding network definition of the datacenter. We developed Segmentrix, a novel adjacency matrix-based tool for developing and monitoring micro-segmentation strategies. This representation is scalable, readable, and provides visibility into the datacenter network of large organizations. The ability to visualize all the network level dependencies in one view makes it an essential tool for developing segments in the datacenter. To support monitoring of the network, we provide a linked interactive dashboard with functionalities like data filtering. As the size of datacenter grows and networks become more flexible, the need for micro-segmentation will rise and thus we expect to see more work in the domain in the near future.

REFERENCES

[1] J. Friedman. *The Definitive Guide to Micro-Segmentation*. 2014.

[2] H. Kim, S. Ko, D. S. Kim, and H. K. Kim. Firewall ruleset visualization analysis tool based on segmentation. In *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 2017. doi: 10.1109/VIZSEC.2017.8062196

[3] H. Koike, K. Ohno, and K. Koizumi. Visualizing cyber attacks using ip matrix. In *IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05).*, 2005. doi: 10.1109/VIZSEC.2005.1532070

[4] Y. Liu and H. Man. Network vulnerability assessment using bayesian networks. In *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005*. International Society for Optics and Photonics, 2005. doi: 10.1117/12.604240