International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov-2017 www.irjet.net p-ISSN: 2395-0072

Enhanced method of Micro segmentation based on provisioned application in Data Centers

Mrs. Pradnya Patil

Assistant Professor, Department of CSE, TKIET-Warananagar, Maharashtra, India

---

Abstract - *Micro segmentation is technology these days used in recent days to prevent lateral movement of threats within cloud data centers. Data centers are under attack and it is easiest way to attack multiple servers or machines since they tightly interconnected and use shared resources. Hardly a day goes by without some kind of hack being uncovered. Intellectual property is stolen, cash ripped off from bank systems, websites brought down and millions of identities stolen. So organizations are in search of ways to more efficiently and securely use IT resources to increase innovation and minimize cost. Micro-segmentation is a data center security technology that supports this need in cloud, virtual, and physical environments. A secure network design that focuses on micro segmentation can slow the rate at which an attacker moves through a network and provide more opportunities for detecting threat movement. In fact, the effort extended in learning, classifying, and segmenting the network adds value and strengthens all of the organization's controls.*

Key Words: Micro Segmentation, Data Centres, Application Provisioning, Network analysis, Correlation

1. INTRODUCTION

Micro-segmentation enables organizations to logically divide the data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment. This restricts an attacker's ability to move laterally in the data center, even after the perimeter has been breached — much like safe deposit boxes in a bank vault protect the valuables of individual bank customers, even if the safe has been cracked. Micro-segmentation of the data center network restricts unauthorized lateral movement but, until now, hasn't been operationally feasible in data center networks.

The burden of security management increases exponentially with the number of workloads and the increasingly dynamic nature of today's data centers. If firewall rules need to be manually added, deleted, and/or modified every time a new VM is added, moved, or decommissioned, the rate of change quickly overwhelms IT operations. It's this barrier that has been the demise of most security teams' best-laid plans to realize a comprehensive micro-segmentation or least privilege, unit-level trust strategy in the data center.

Unfortunately, data center network segments are often far too large to be effective and traditional processes for defining and configuring segmentation are time consuming and prone to human error, often resulting in security breaches. There are two key operational barriers to micro-segmentation using traditional firewalls: throughput capacity and security management.

Limitations on throughput capacity can be overcome, but at a significant cost. It's possible to buy enough physical or virtual firewalls to deliver the capacity required to achieve micro-segmentation, but in most (if not all) organizations, purchasing the number of firewalls necessary for effective micro segmentation isn't financially feasible.

2. LITERATURE SURVEY

By micro segmenting the network, an organization creates boundaries that the attacker has to cross before gaining access to another subset of data. These boundaries are created in a way that only allows the minimum necessary services through. These services are then closely monitored to detect any unauthorized use. Physical security can play a role in determining if another segment is needed. For Example, imagine an office building with 100 identical workers spread across two floors. The bottom floor is in an area with access to the public. The top floor only allows employee access. The information on all 100 systems has the same value and security needs. However, the additional risk presented by the physical access to the systems on the bottom floor means that additional controls are necessary.

Network segmentation should be one of the controls considered. Wireless should be considered another segmentation qualifier. Due to the fact that it is nearly impossible to physically secure a wireless network, they should be segmented on a private VLAN. On a private VLAN, attached devices are not able to directly communicate with each other. This helps prevent compromised systems and rouge users from spreading to other systems on the wireless network.

Security is a significant challenge to hyper-consolidation. When an IT organization wishes to consolidate workloads with differing security needs, such as a production environment with a test environment, a new approach to data center security is needed. Micro-segmentation enables this to happen by creating the ability to enforce security

policies around each individual workload in the environment. By placing security controls next to the workloads themselves, security policies become asset-specific - for example, controlling communication between two workloads in the same subnet or on the same hypervisor, regardless of location, infrastructure-type, or workload-type. As a result, workloads at different security levels can now share common infrastructure, enabling much greater consolidation and agility.

Security vendors can take advantage of the network virtualization platform to trigger advanced security service responses from a completely different security vendor's technology solution — an innovation that's simply not possible without network virtualization. Ability to provide fine-grained security with enforcement distributed to every hypervisor in the data center micro-segmentation. To understand micro-segmentation, we first need to understand Virtual LANs (VLANs). VLANs are a way to simulate separate physical networks without actually having to physically wire up separate networks Virtualization, arguably describable as "software-defined workloads," has become inextricably intertwined with both Software-Defined Storage (SDS) and Software-Defined Networking (SDN). The past decade had storage wars that redefined the IT landscape, and the upcoming one looks to see networking do the same. One term that will soon become commonplace for all virtualization administrators is micro segmentation.

Network segmentation has long been a security best practice, based on hardware-bound zones of firewalls and/or VLANs inside the data center. These segmentation technologies remain rigid, complex, and slow to change, even though the data centers they are protecting have become dynamic, fast, and integrated with cloud services.

3. PROPOSED METHODOLOGY

This chapter discusses about the proposed methodology of doing micro-segmentation in public, Private cloud or in on premise organization network. Micro segmentation suggest to administrator different best practices or recommendation by which the machines or servers in the cloud network configured in way that lateral movement of threat can be minimized to minimal level. In the proposed method there different flow of operations:

1. **Collection of Assets and related inventory**: In first step the proposed system will collect all the assets (servers/machines) details into system with their all details like OS, version, hardware information and different application installed in the server within data center. All of this inventory of servers are stored in database in relation with application installed on each of servers

2. **Collection of network logs/VPC logs**: Once all the inventory about the serves in imported then in next action system will collect all the network and VPC logs to system. The network logs contains all of the traffic of server to server communication and with other information about the network micro segmentation. This operation also collects details about network topology like details about :

   - Virtual LAN's
   - Virtual Switches
   - Different subnets defined on each of LAN's and their IP configuration

3. **Classification of applications and correlation with servers**: As next step system will classify all of the collected information about different application installed within organization. This will mainly classify application into Servers and Desktop application. The most server side application are distributed in nature and contains multiple components like Application server, Database, Console and Load balancer. So accordingly this operation will classify the application and correlates to on what server this application or its role is installed.

4. **Classification of network/VPC logs:** Once application classification is completed then system will process all of the imported network and VPC logs to get all the communication traces between the applications. As first phase system will gets all of machine IP those are communicated with each other within organization and its ports number on which communication happening. The processed data is stored in to DB with machine IP as primary key with association with port number it is communicating.

5. **Correlation between Application and Network**: In this activity all the application related information correlated with details with network log extracted. This is first step towards establishing the IP to Application correlation, this done in multiple steps as per the different server roles for each of application. For each application how many IP's are association gets calculated and based on Network reference map is created to summarize second level of correlation between application and IP. In the next phase for each IP in pair with application the port number is associated to get determine more detailed level of summarization.

6. **Segmentation based on summarized data:** This is final step where proposed system will suggest segmentation in the scoped data center. For each application gets details on how many different IP's are active in the cross component communication on which port. As summarization for each application list of IP and their port number gets associated. In case where application is interacting with internet then separate port mapping done with respect to the application. As output of proposed system there will be recommended

segmentation for each application installed within scoped data center and details about:

- Server group recommended within subnet
- What all firewall port should be open
- Security group
- Access control list

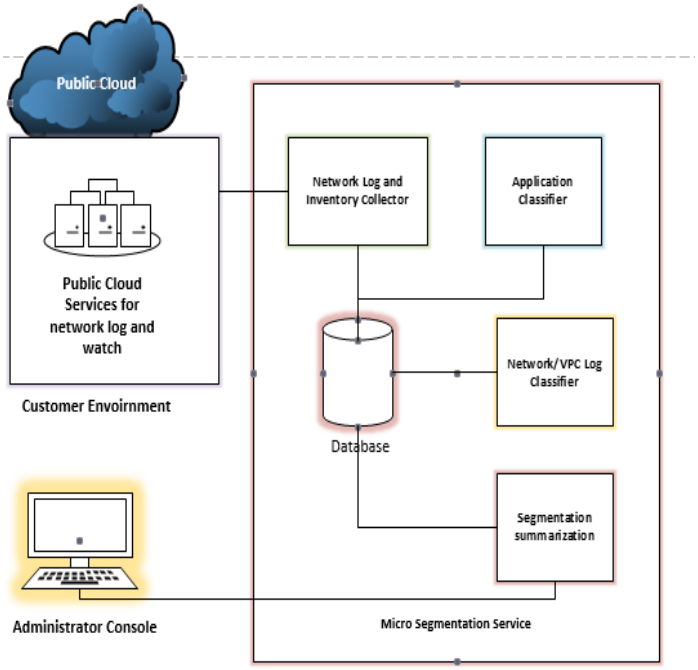

Fig. 1- Architecture of Micro-segmentation service

4. RESULTS AND CONCLUSIONS

As discussed in with designed and developed system prototype we observed that micro-segmentation in public, private or hybrid cloud data centers the application based segmentation can be recommended to system administrator for better security of the data center in any space. Generally application based segmentation can be implemented per application deployed as per the requirements, we observed for large scale multi-tier system application can be successfully segmented with the analysis of network or VPC logs in summarization with application communication logs. In our research done in private cloud based on VMware NSX we observed that three trier systems can segmentation recommended with suggestions of different firewall ports should be open, what are different Access Control list should be configured and configuration of different security groups. In future this proposed system can be enhanced with adding more real time network traffic analysis and understand detailed level of communication with the provisioned systems. Also the proposed system can be also enhanced to provide micro-segmentation based on application user permissions assigned, so that in future which user should have what rights can be also recommended.

REFERENCES

[1] Technical White Paper Micro-Segmentation For Cloud-Scale Security vArmour 2015.

[2] VMware-micro-segmentation-for-dummies by VMware Special Edition Published by John Wiley & Sons, Inc. by Lawrence Miller, CISSP,and Joshua Soto

[3] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutionbrief/partners/intel/vmware-micro-segmentation-builds-security-into-your-data-centers-white-paper.pdf

[4] Data Center Micro-Segmentation A Software Defined Data Center Approach for a"Zero Trust" Security Strategy, Published by VMware.

BIOGRAPHIES

Pradnya Patil is currently working as Assistant Professor at Department of Computer Science and Engineering, TKIET Warananagar. Completed Master of Engineering from Savitribai Phule Pune University, Pune and research areas are Cloud Computing, Computer Security and Data Analytics.