Johns Hopkins University

Network Security Final Paper

The Future of Firewalls

Student Name: Cheng Xu

Course Name: Network Security

Instructor Name: Seth Nielson

Due Date: 14/12/2018

Table of Contents

1. Introduction

Firewalls have come a long way since its beginning in the late 1980s. The technology has developed greatly since then, and the increased complexity and openness of the network makes the question of security more complicated and various. This paper aims to explore the future of firewalls.

2. Background

2.1. Firewall

“A firewall is a network security system that monitors and controls incoming and outcoming network traffic based on predetermined security rules”[1]. Basically, it helps to create a “wall” between trusted internal network and untrusted external network to controls traffic allowed to enter and exit a point inside a network[2].

2.2. Zero Trust Model

Zero Trust is a security model based on the idea of "never trust, always verify", meaning that an organization should not automatically trust anything inside or outside its perimeters without verifying and granting access at first[3]. Basically, it creates a new type of data-centric perimeter and protects it with strong encryption techniques tied to intelligent authentication.

[1] "Firewall"

[2] "What is a firewall"

[3] "What is Zero Trust".

2.3. Micro-segmentation

Micro-segmentation is a security technique that allows organizations to logically divide the data center into different security segments, down to the individual workload level, and then establish security controls and deliver services for each unique segment. It helps prevent malware from disseminating throughout the data center[4].

2.4. SDN

Software-Defined Networking (SDN) is an architecture that decouples the network control and forwarding functions thus "enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services for applications as SDN cloud computing or mobile networks"[5].

3. Firewall is dying

The traditional firewall is dead or at least dying.

With no doubt, the complexity of networks has increased greatly these years and also perimeters have extended and fragmented a lot. Many businesses have moved to the cloud because of its scalability, efficiency, reliability, etc. Applications can live in cloud and hybrid environments or be delivered via websites by external services providers. Employees and customers often access them via the web, from anywhere, any time, on multiple devices. That means the traditional firewall is "blind". It can't see what's going on. It doesn't know where the connections come from and where they are going to.

[4] "Micro-Segmentation"

[5] "SDN".

Meanwhile, ongoing platform evolution including mobile computing, cloud services, and other trends are blurring the perimeter between internal and external networks is making the perimeter vanishing.

Even though there might be some new versions with next-generation features, breakthroughs are not made on major limitations. Firewalls are still only based on perimeter security and are limited to applying security policies against visible packets that go through them. In short, because of the increasing popularity of the cloud, the vanishing perimeters and the growing volume of data traffic, the traditional firewall is simply no longer qualified for protecting the valuable data of the organization from various potential attacks.

4. Zero Trust v. Perimeter Security

Why is Zero Trust needed? This problem can be answered with a case in which a man called Philip Cummings[6] being involved. Philip Cummings worked on the help desk of a company called TCI, which provided software for credit bureaus. He had access to all of the client passwords and subscription codes because he supported software on all credit bureau networks. During his TCI employment, Philip Cummings sold countless credit reports for the interest of money. The crime continued for years after Cummings was no longer an employee. And the victims were not aware that cybercriminals had infiltrated their network. The financial impact was enormous.

In light of Philip Cummings case, it is clear that the trust is broken once the bad guys get inside. Now it's the time to change the trust model to the Zero Trust model. By applying the Zero Trust Model, it regards all devices, users, and the network as untrusted. It means there is no clear separation between "trusted" and "untrusted" so that to a great extent, the

[6] "World's largest ID theft felon faces 14 years' jail"

internal attack can be prevented. Within the Zero Trust model, security policies should not simply be applied to the environment as a whole or large segment groups of this environment but to everything. Every workload, every application, everything in the network must be protected. In short, perimeter security becomes data-centric security.

5. Micro-segmentation and/or SDN become the norm

Micro-segmentation is the process by which this Zero Trust model is implemented. It effectively makes each virtual machine (VM) their own individual segment. Therefore, each and every virtual machine is protected by their own firewall. If a malicious file did manage a way through the environment firewall and onto a virtual machine, the file can get no further without having to once more pass through a firewall.

Trying to create micro-segmentation manually by dedicating specific physical firewalls and routers to virtual machines or bare-metal servers would be a time consuming and expensive process. However, with SDN solutions like VMware NSX, the environment is virtualized. This enables a network administrator to establish micro-segmentation by creating "security policies" tied to each VM.

Microsegmentation is a powerful strategy for protecting the network. However, there is an ongoing arms race between security professionals and hackers. Microsegmentation is effective now and will one day become as commonplace as the standard firewall but it will never be truly enough. It is only a matter of time before bad guys find a way to crack it. For this reason, network administrators must always be strengthening their network security with the latest solutions.

6. The Future

Although it’s hard to define the future, it becomes the fact that the fundamental problem of the modern network is to trust the internal networks by default. Attackers have repeatedly, and with great success, exploited this implicit trust assumption. And the only solution is to adopt a Zero Trust approach. Vendors have even banded together to create partnerships which essentially offer off-the-shelf Zero Trust solutions. For example, Brocade has partnered with Palo Alto Networks to build an integrated Zero Trust solution for big iron data centers. Meanwhile, VMware built a Zero Trust ecosystem around its NSX network virtualization offering. And it took Google six years to work on BeyondCorp and finally ended up with a lot of high-level components such as Single sign-on, Access proxy, Access control engine, User and device inventory, Trust repository and so on. Now in early 2018, ZTX(Zero Trust eXtended) was introduced.

In short, the idea of Zero Trust is on its way to be adopted by more and more people and more effort will be made on its evolution and application.

Bibliography

Beske, Colin McCormick, Jeff Peck, and Max Saltonstall. "Migrating to BeyondCorp: Maintaining Productivity While Improving Security." (2017): 49-55.

Brocade Communications Systems, “Next-Gen Security Architecture through Brocade Network Devices and Palo Alto Networks Firewall,” http://community.brocade.com/dtscp75322/attachments/dtscp75322/EthernetSwitchesRouters/208/1/Alliances%20Palo%20Alto%20Networks%20-%20App%20Note%20-%20Next-Gen%20Security%20Architecture%20through%20Brocade%20Network%20 Devices%20and%20Palo%20Alto%20Networks%20Firewall.pdf

Kindervag, John. "Build Security Into Your Network's DNA: The Zero Trust Network Architecture." Forrester Research Inc (2010): 1-26.

Kindervag, John. "No more chewy centers: Introducing the zero trust model of information security." Forrester Research (2010).

Osborn, Barclay, et al. "BeyondCorp: Design to Deployment at Google." (2016): 28-35.

Rossi, Ben. “Why the humble firewall still stands strong” *Information Age*, Bonhill Group Plc, 27 November 2014, https://www.information-age.com/why-humble-firewall-still-stands-strong-123458688/.

VMware, “Data Center Micro-Segmentation,” http://blogs.vmware.com/networkvirtualization/files/2014/06/VMware-SDDC-Micro-Segmentation-White-Paper.pdf.

Ward, Rory, and Betsy Beyer. "Beyondcorp: A new approach to enterprise security." login 39 (2014): 5-11.

Wilson, Jeff. "The Future of the Firewall." Business Communications Review 5 (2005): 28-32.