A Zero Trust Approach to Network Security

Pedro Assunção

University Lusofona of Porto Porto, Portugal
pedroj_9@hotmail.com

Abstract. In the last years, we have seen an increase in the use of wireless networks due to new forms of communication. The online security has become a hotly debated topic in the community. People want to have access to all of your applications and resources anywhere, anytime. With the increase in the use of Cloud computing and IoT, the number of connected devices increases that consequently also increase the targets of cybercrime. A simple change of mentality can help protect data and the entire network. This paper describes what a Zero Trust Network is and show some concepts behind this architecture/philosophy. Zero Trust is an architecture that has a principle that everything inside or outside the network is not reliable until verified.

Keywords: Cybersecurity, Business Security, Zero Trust Network, Google BeyondCorp.

1 Introduction

Cybersecurity is a hotly debated topic today because of the breach large amounts of sensitive information from large companies. Which has caused a big question on who we can trust our data.

So, the IT Landscape has changed, and the use of networks substantially have risen. The users want to access applications everywhere, every time and with this, we have a great amount of sensitive data on these networks/applications that cybercriminals want to be able to profit with. So, the security models have to support this evolution to keep user data safe.

According to the authors [1], the conventional model normally used has in mind build a wall between trusted and untrusted resources, local network and the internet for example. And according to the Computer Security Institute (CSI), approximately 60 to 80 percent of network misuse incident is originated inside the network [2].

With these needs come a security architecture called “Zero Trust” that was developed by John Kindervag of Forrester Research [1].

Zero Trust, unlike the conventional model, has as its principle "never trust, always verify," where both internal and external networks cannot be trusted. This principle is the basis for reducing the risk of attacks not only external but also internal.

This model brings new concepts on how to design a corporate network such as segmentation gateway, which allows increasing the micro-segmentation of a network with the aim of having more visibility over all traffic by inspecting all types of users and devices that connect in the

10.11228/dpsc.01.01.007

network. BeyondCorp is an example of a zero trust architecture designed by Google that allows employees to work more securely in any location without the need for a traditional VPN.

2 Network Landscape

Initially, with the appearance of the first computer systems, companies would be more "isolated" which mitigated the number of attacks focusing on their efforts to restrict access only within the company by hierarchical levels. Since these days the safety models developed have focused on separating the "trusted resources" from the "untrusted resources" using layers of protection to build digital perimeters. The according to the author [3] the traditional perimeter security depends to the firewalls, VPN's and web gateways who has to deal with employee's skill shortages, overloaded, and an ever-expanding number of cloud apps and mobile devices which leads to an increase in the attack surface of cybercriminals. The growing of cloud computing and the internet of things have caused these perimeters to be eliminated. What can we say that the conventional model is no longer functional. With that model as much as we invest in cybersecurity of our company, new and more sophisticated attacks are launched against our defenses, so we must look at cybersecurity not as an investment but as a necessity over time. According [4] it is estimated that cybercrime targets increase considerably due to the existence of an ever-growing universe of connected people (figure 1).

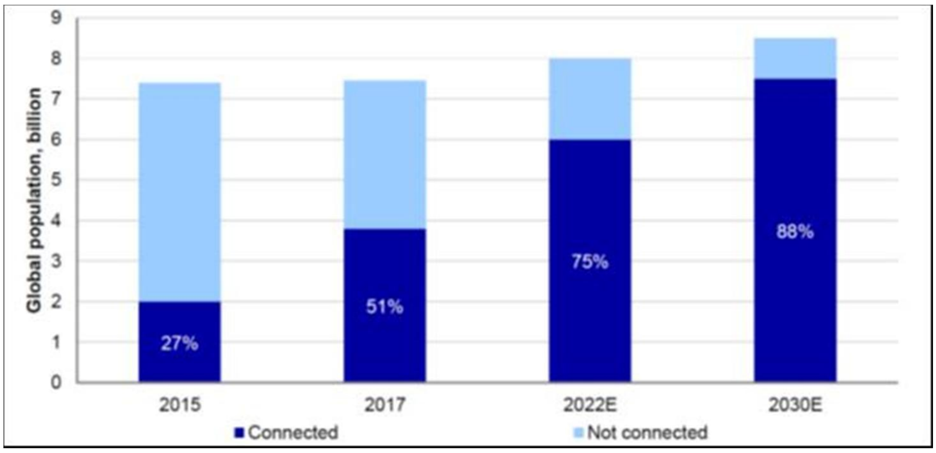

Fig.1. Growing of connected people [4]

2.1 Impact of Cybersecurity

With the increase in the number of devices connected to the Internet and consequently more attack area for cybercriminals, the monetary values involved in cybersecurity has been increasing [4].

Cybersecurity is about protecting information and cyber threat systems. Threats can be used as malware (malware, ransomware, phishing, worms) these weapons are increasingly sophisticated and automated and can be purchased at low cost.

With this, companies have a "punctual products" approach to combat these threats, which we will see later in this article that this is not viable because this model is expensive and complex.

The cybersecurity market is expected to reach 170 billion by 2020 [5].

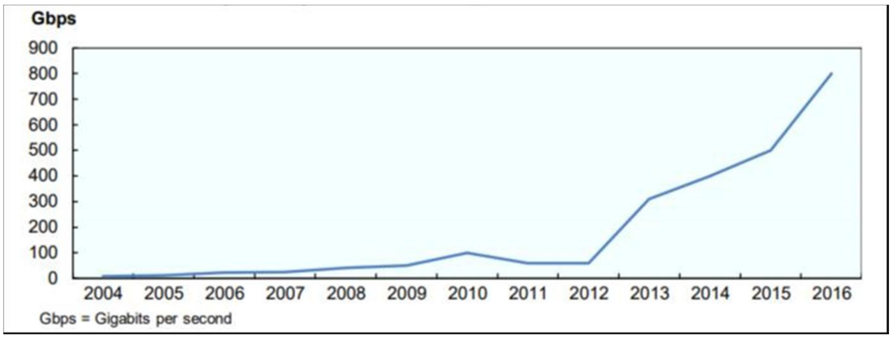

Fig.2. Evolution of bandwidth used for major DDoS [4]

3 Zero Trust Fundamentals

As the conventional model is not more functional, we cannot let the security of our organization be relied upon purely on a firewall or intrusion prevention system.

The Zero Trust is a security model developed by John Kindervag at Forrester research which has the principle of "never trust, always verify,", This architecture is designed to mitigate threats within the network-specific data or assets so that more granular rules can be applied.

According to John Kindervag [6], Zero Trust is not making networks, clouds, or endpoints more reliable; is to eliminate the concept of trust from digital systems, Trust is binary, it’s on or off which is different from the real world interacting with people.

So Zero trust is all about how you think and there is no single formula for implementing this type of architecture. When building a network with zero trust DNA you need to keep in mind the following topics: [6]

- Ensure all data are securely accessed based on user and location
- The use of access control is strongly advised/required
- Inspect de log’s of all traffic

This is important in a world where mobility is more dominant with tablets, smartphones, laptops, and IoT devices accessing the internet. These devices need to access these resources in a secure way.

3.1 Zero Trust Architecture

With this we can say that no longer exist a trusted interface in our devices, no longer exist trusted network, no longer exist trusted users and this is an important concept when we need to move packets from one place to another. If we look at the traditional model (figure 3) we have several layers of the network that we put several layers of security devices. This eventually making the network heavy, unmanageable, hard to keep safe and always invest in new devices over time.

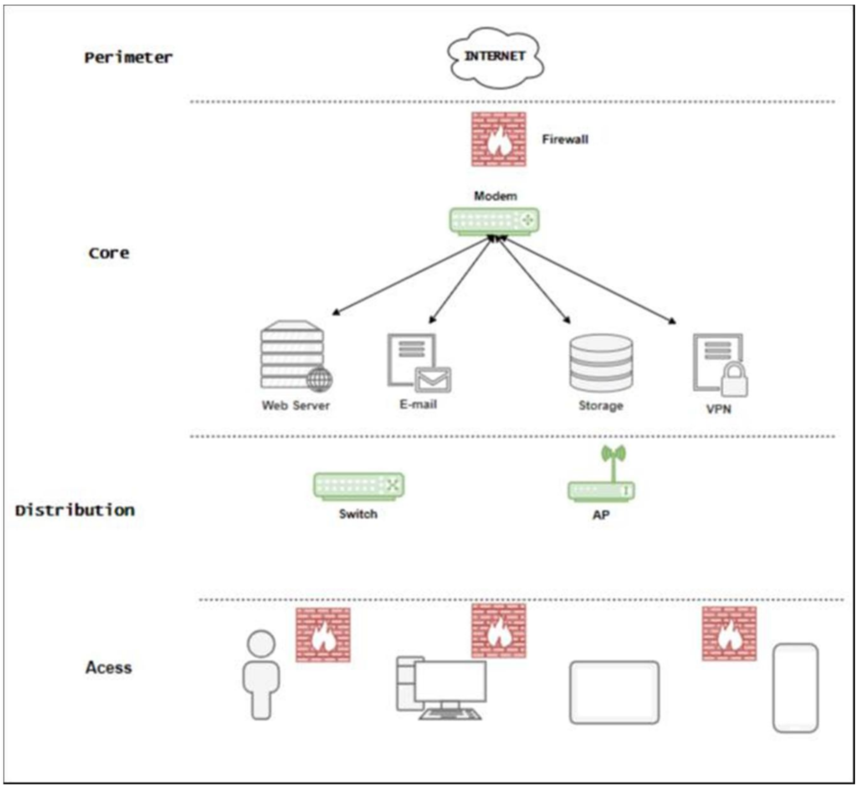

Fig.3. Traditional Architecture base on [6]

So zero trust model redraws the network and creates a new idea of segmentation gateway. This concept is built to concentrate all the resources that are used in a modern network like, content filtering, access control, firewall, cryptographic engines, package forwarding.

This type of segmentation is used in a modular way, is scalable and can adapt to any type of business, without having to restructure the entire network structure. But if a company has to structure the network, it has to do from the inside out, what will allow having a network that adapts and evolves with a security ADN where all packets can be delivered in a secure way.

This segmentation gateway model is considered by [7] as a next-generation firewall, since it is developed to increase the micro-segmentation of the networks, becoming quite versatile in terms of being scalable, adapting to all types of business and virtualization-friendly.

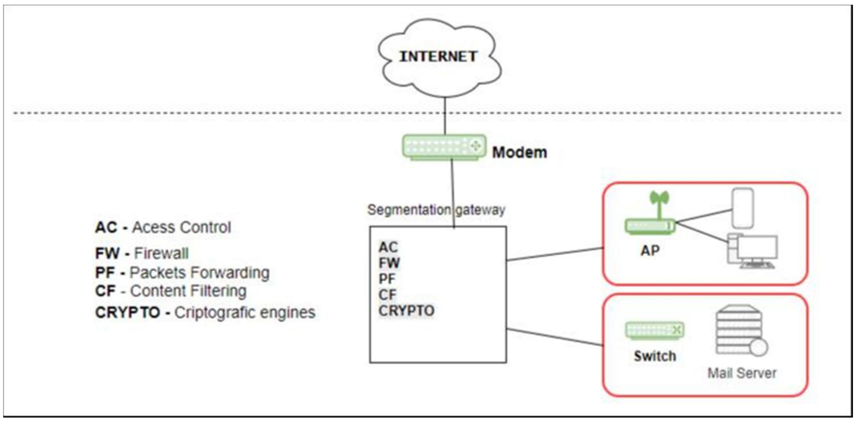

Fig.4. Zero Trust Architecture based on [6]

In the figure above it is represented a segmentation gateway in a basic way making the separation in micro-segmentation (MCAP) so that it is easier to inspect all the traffic of the network.

So, with the segmentation and next-generation firewalls, we can control who, what, where and when someone gets connected in the network. After a user is authenticated, the privileges must be tightly managed.

The thinking behind this is to prevent lateral movement inside the network after being compromised this reduces the range of damage caused. The term firewall, in this case, cannot be confused with the fact that we want to place near the perimeter of the network because the segmentation gateway must be placed in the center of the network.

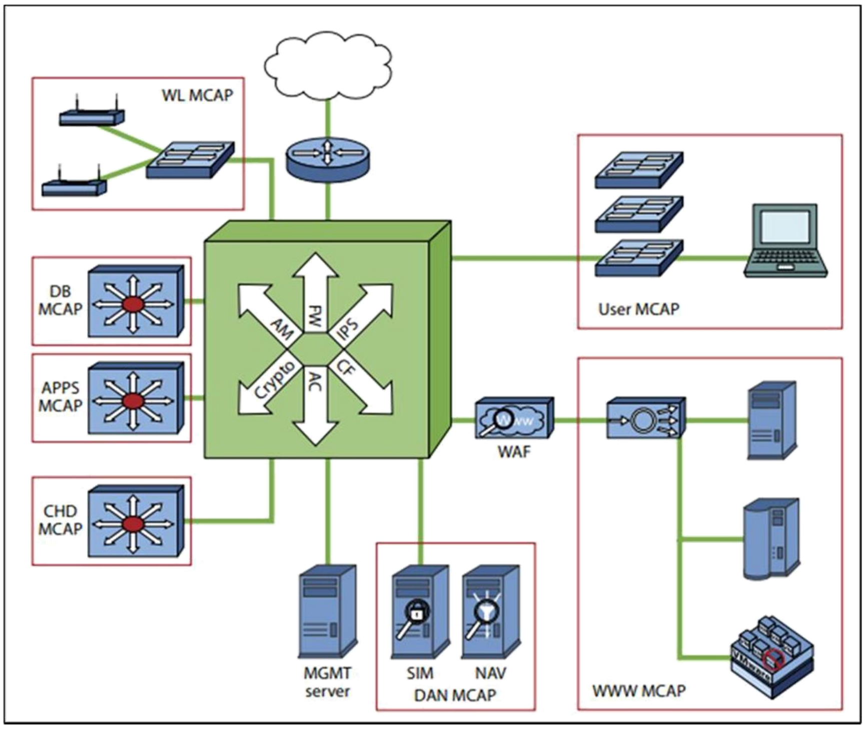

Fig.5. Extensible network architecture [6]

This is an example of a network that is scalable and can be augmented in any way we want or need.

3.2 Security benefits of Zero Trust

Zero trust is a philosophy that brings innumerable advantages in several levels to the company. So, I believe that the future of cybersecurity goes through this model.

According to [8] Zero trust delivers security and impressive business results. This model delivers a considerable business value like greater enterprise visibility protecting your customer data and business. In a "front-end" perspective Zero trust avoid financial costs in security audits, maintaining a good reputation towards other companies. In a "back-end" perspective we have reduced time to breach detection and get visibility into all your corporate traffic by inspecting the user request, devices, and data. Reducing the complexity of the security stack is a great support for the network maintenance team to deliver security and excellent end-user experience.

With this, we can be completely rested? Of course not. Some attacks against Zero Trust networks are well mitigated, while others we can only detect the attack. No model is perfect and 100% effective but we can reduce the impacts caused by any type of attack.

4 BeyondCorp by Google

BeyondCorp is a business security model of building zero trust networks in Google. By changing network perimeter access controls for individual devices and users, BeyondCorp allows employees to work more securely in any location without the need for a traditional VPN.

Basically, according to [9] Google BeyondCorp is a new model that excuses privileges in the corporate network, instead, access only depends on the credentials of the user and the device. whether it is in a home network, a hotel or a coffee shop. All access to enterprise resources is fully authenticated, fully authorized, and fully encrypted based upon device state and user credentials. BeyondCorp can enforce fine-grained access to different parts of enterprise resources

BeyondCorp consists of many cooperating components to ensure that only appropriately authenticated devices and users are authorized to access the requisite enterprise applications (figure 7).

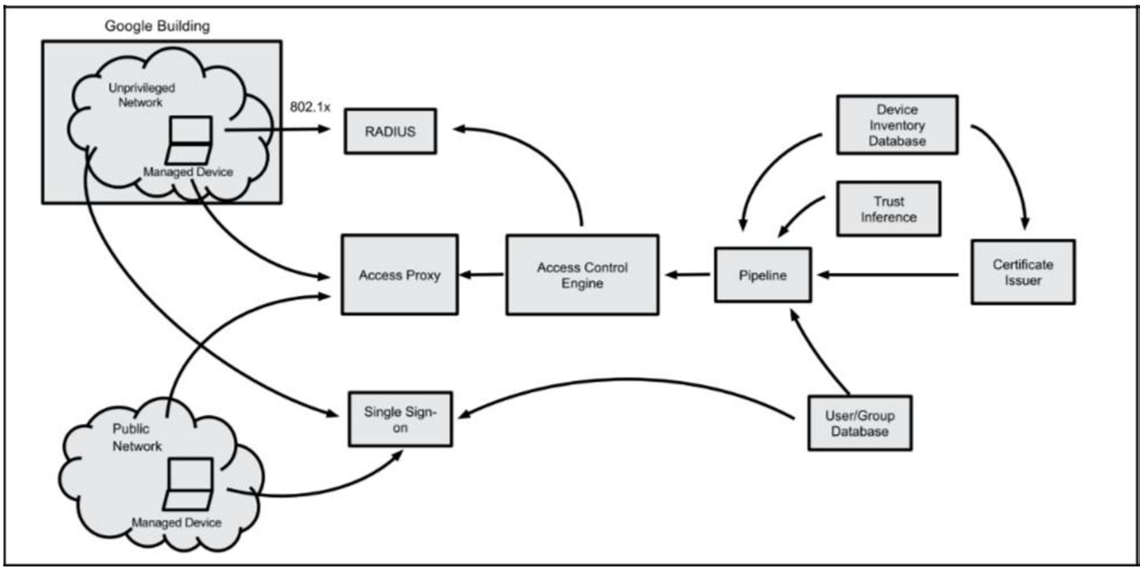

Fig.6. BeyondCorp components and Accessflow

In this model, all the devices normally used by the user are stored in a device inventory database in order to have better visibility of all the devices that are used in the network. All such information collected about devices and users is needed to understand what applications are used internally and what security policies should be applied in each application. It is necessary to understand the roles of the position and decide who has access to specific services in order to have effective access control.

With this, BeyondCorp brings many benefits to corporate network security by keeping the business consistent.

BeyondCorp benefits

- Keep devices up-to-date with the latest software
- Maintain an inventory of employee devices
- Monitor all endpoints & log all traffic
- Only communicate over fully encrypted channels
- Incorporate multi-factor AUTH
- Eliminate Static credentials

But not all models are 100% efficient there are also some difficulties that may appear in the implementation of this type of model. These difficulties may vary depending on the area of activity of the company itself. Depending on the area of the company, some vendors need network access inside the enterprise in order to maintain installed products or provide direct services, making access management difficult.

5 Conclusion

Cybersecurity is an area of emerging security that has been felt in recent decades as an exponential concern since the number of devices connected to the Internet is increasing dramatically, with almost 90% of the world population expected to be connected to the Internet by 2030.

And with this, traditional security models are becoming increasingly impractical due to the increase in the sophistication of the attacks and the elimination of the perimeters of computer networks.

With this scenario, there was a need to have another type of mentality and approach on data protection.

Zero trust arises from the need to simplify data security. In the absence of a simple implementation formula, this philosophy is based on "never trust, always verify". This is the beginning of the change of the mentality eliminating the trust of our network. Zero Trust segmentation platform is the basis of any Zero Trust initiative that allows us to break the network into micro-segmentation, giving us the ability to adapt our needs without restructuring our entire network.

Nowadays we have already seen several companies following this type of model because they bring many advantages. One of these cases is Google BeyondCorp.

BeyondCorp is the Google-designed business solution that allows users to work anywhere without VPN.

References

1. Gilman E., Barth D.: Zero Trust Networks, O'Reilly, (2017)
2. Sivaraman R.: "Zero Trust Security Model". S3tel Inc, White Paper (2015)
3. Williams C.: Zero Trust Security, Centrify Special Edition. John Wiley & Sons, Inc., Hoboken, New Jersey (2019)
4. Osorio de Barros G.: "A Economia da Cibersegurança", Gabinete de Estratégia e Estudos, Ministério da Economia(2018)
5. Morgan S.: "Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020", Forbes (2015)
6. Kindervag J.: Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Forrester (2010)
7. Kindervag J.: Clarifying What Zero Trust Is and Is Not (2018)
8. Akamai: "The 6 Business and Security Benefits of Zero Trust." White Paper (2018)
9. Ward R., Beyer B,: "BeyondCorp A New Approach to Enterprise Security". Usenix, vol. 39:6 (2014)