Zero Trust Network Model

John Flanigan

December 12, 2018

Abstract

The zero trust network model is a modern alternative to traditional perimeter network security and has been gaining popularity the last several years. Its initial usage was in the technology industry, particularly with Google's BeyondCorp, but it is now being used more widely by traditional corporations. Companies are moving away from perimeter security because of its primary weakness: if the perimeter is breached, then an attacker has easy access to the privileged intranet. The zero trust model solves this weakness by treating all hosts as if they are internet facing and considers the entire network to be compromised. This paper will discuss the advantages and disadvantages of the zero trust model vs other network models and examine potential use cases of the zero trust model.

Table of Contents

1 Introduction

The zero trust network model was originally described in John Kindervag's 2010 paper titled *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. In it, Kindervag cites the need for a new, more flexible network security model and proposes the zero trust model as a solution [1]. Instead of trying to adapt legacy models for the modern world, he suggests a new paradigm of "designing from the inside out." By approaching network security from the inside out, it is possible to optimize network security for future flexibility.

Since this paper was published in 2010, there has been more research and thought given to the zero trust security model. In addition, many companies have already successfully developed and implemented an approach, most notably Google with their BeyondCorp technology.

2 To the Community/Reason for a New Security Model

Because of how quickly technology changes, there is a significant need for an updated network security model. The classic perimeter model grew out of a time when not all of an organization's computers were connected to the public internet.

Today, the network landscape is significantly more complicated and distributed than it once was. Companies now have to account for factors such as remote employees, bring your own device programs, cloud-based applications, etc. when designing their network. In addition, the cost of a security failure can be massive. Companies need to be able to defend against hackers at every layer, not just at the perimeter of their network.

These additional considerations make it much more challenging to apply a perimeter security approach to defend a network. The zero trust model aims to solve this challenge by introducing a new approach.

3 Zero Trust Model

In a traditional network security architecture model, a network is broken into different zones protected by one or more firewalls. Often there will be the outside internet, an exclusion zone (often called a demilitarized zone or "DMZ"), a trusted zone, and a privileged zone [2].

Although the perimeter model is an accepted approach to network security, that doesn't mean there are not alternatives that might be a better solution.

According to Evan Gilman and Doug Barth in their book Zero Trust Networks, a zero trust network is built upon five fundamental assertions [2]:

1. The network is always assumed to be hostile
2. External and internal threats exist on the network at all times
3. Network locality is not sufficient for deciding trust in a network.
4. Every device user, and network flow is authenticated and authorized.
5. Policies must be dynamic and calculated from as many sources of data as possible.

Creating a network that follows these assertions is not an easy task but because of advancements in automation, it is much more attainable than it used to be.

4 Google BeyondCorp

Google's BeyondCorp initiative was one of the first implementations of a zero trust model. It eliminates the privileged corporate network and instead relies on device and user credentials to establish trust [3]. This allows fine-grained access to network resources and entirely eliminates the need for a VPN to gain access to the privileged network. This leads to a better user experience for remote employees [4].

To establish trust, BeyondCorp relies on device and user authentication. To handle the device identification piece, Google tracks managed devices in an inventory database; each device is uniquely identified in this database. Similarly, Google uses a User and a Group database to track and manage users. Through a single sign on system, users can be authorized and granted short-lived tokens that can be used for authorization for specific resources [3].

Another implementation requirement of BeyondCorp was the externalization of internal applications. To achieve this, Google uses an internet-facing proxy to expose its internal applications. The proxy provides common features such as global reachability, load balancing, access control checks, application health checks, and denial-of-service protection [3].

Google's BeyondCorp is a good example of what a corporate network implementation of a zero trust model looks like. It demonstrates what the primary considerations are implementing creating a zero trust network and how Google approached them.

6 Security Considerations

The zero trust model is not without pitfalls and weaknesses. There are some security considerations that are important to understand prior to implementation of such a network model.

Because the zero trust model relies heavily on user and device authentication, identity theft is an important consideration. The model does attempt to mitigate this threat by using user and device authentication in tandem which is more than can be said of other models. This is an issue that is widespread across the industry and many are working to mitigate.

Another consideration is preventing a distributed denial of service (DDoS) attack. Because the zero trust model itself does not provide mitigation against such an attack, additional precautions must be taken to defend against DDoS. Typically, this precaution entails traffic filtering defenses upstream. Zero trust networks work well with traffic filtering because they retain a lot of information about what to expect on the network [2].

Because of the architecture of zero trust models, an attacker can develop a system diagram by monitoring network traffic. The traditional perimeter model prevented this by placing traffic behind VPN gateways. Gilman and Barth argue that network privacy is outside the scope of the zero trust model but if privacy is desired, it can be achieved by using site-to-site tunnels [2].

Although the zero trust model introduces some new security concerns, it resolves many others that exist within a perimeter model.

7 Applications

Although the perimeter defense model has been standard for many years, it is not capable of overcoming to some of the challenges created by remote employees, bring your own device programs, cloud-based applications.

An organization does not need to go to a full zero trust model to see benefits from it however. A hybrid perimeter and zero trust model might be sufficient for many organizations. An organization can start by approaching all new development with a zero trust mindset while maintaining a perimeter model for legacy applications. The principles of assuming external and internal threats exist at all times, network locality is not sufficient to establish trust, and authenticating devices and users can all be applied without going solely to a zero trust model.

Finally, there are many organizations whose business it is to assist with implementing a zero trust network so it is certainly within reach of companies lacking the technical expertise of Google [4] [5].

8 Conclusion

In conclusion, the zero trust network model is a modern network security model that aims to solve challenges introduced by modern technology and workplace structures. It is built around some basic assumptions, the primary of which is that the network is always hostile.

The zero trust model is still relatively new in terms of network security so companies are still working through the implementation details and security concerns. At this point, cutting edge, technology focused companies, Google for example, have already adapted some of the zero trust model principles while others are still catching up. The zero trust model is effective in solving the problems it sets out to. For example, Google has not been successfully phished since 2017 [5].

In conclusion, the zero trust network security model is an important trend in network security to be aware of as it is growing in popularity and more companies continue to implement some or all of its principles.

9 References

1. Kindervag, John. “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture.” http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf. 2010.

2. Gilman, Evan and Barth, Doug. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media, 2017.

3. Beyer, Betsy, and Ward, Rory. “BeyondCorp: A New Approach to Security.” https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf . 2014.

4. “Zero Trust Security.” *Akamai*, https://www.akamai.com/us/en/solutions/zero-trust-security-model.jsp. 2018.

5. Fisher, Nick. “A Brief History of Zero Trust Security.” *OKTA*, https://www.okta.com/security-blog/2018/08/a-brief-history-of-zero-trust-security/. 2018.