Never Trust, Always Verify: Implementation of Zero Trust Networks

Nicole K. Merritt

Niagara University

Table of Contents

Abstract

Developed by John Kindervag, Zero Trust networks take the trust out of the network and operate on the idea that anyone on the inside or the outside of the firewall is equally as suspicious. This challenges the traditional model of network security – where the network is designed and then security features are added on top. Instead, security is built into the network from the beginning. All traffic is inspected, logged, and treated as suspicious content. The question is not whether an organization should implement a Zero Trust network but rather when. This paper looks at application techniques for legacy networks as well as organizations who are building their network from the ground up with extra attention is given to organizations that rely heavily on cloud computing and Virtual Private Network (VPN) use.

Keywords: Zero Trust Network, Beyond Corp, Insider Attacks, Network Security

Never Trust, Always Verify: Implementation of Zero Trust Networks

Today's corporate network extends far beyond the office walls. It's becoming increasingly common for employees to be accessing sensitive information on their personal devices as well as using a Virtual Private Network (VPN) to do their work remotely. It is no secret that "older, network centric approaches to security no long apply and more applications centric models, with access grounded in identity, are necessary for today's hybrid enterprise" (Centrify, 2017).

For most organizations, the "reality is that they can't just focus on defending the corporate network, because a bulk of their sensitive data now lives in cloud applications and many of the critical operations are performed in the cloud" (Rashid, 2017). Simply protecting the perimeter is not enough anymore considering the amount of work that is completed remotely through VPN's and cloud computing, "with the increased use of [the] cloud comes a slew of risks related to shadow IT. It is important to implement monitors to identify and track the movement of critical data residing in sanctioned IT locations, including on-premises" (Tummalapenta, 2017).

In order to stay competitive and secure, "the modern hybrid enterprise must adopt a Zero Trust security model" (Centrify, 2017). By turning the previous network security strategy on its head, Zero Trust networks "start with the system resources and data repositories that need to be protected as well as the places where we need to be compliant, then build a network from that … building roads is easy. Security is hard" (Kindervag, 2010).

Equally important is the ability for networks to be more "intuitive and inherently secure" while also operating automatically, "automation systems are what allow a Zero Trust network to

be built and operated" (Kindervag,2010). Automation is important because "if policy enforcement cannot be dynamically updated, Zero Trust will be unattainable" (Kindervag,2010).

Literary Review

Perimeter-Centric Security

Perimeter-centric usually operate on the idea that the inside traffic is homogenous, when in fact they "include pockets of users and resources with inherently different levels of trust/ sensitivity, which should ideally be separate" (Paloalto, 2016). Imagine a sort of "castle-and moat mentality" (Pratt, 2018) where an organization is so focused on ensuring that the firewalls surrounding their network is secure. Therefore, they end up assuming that anything that is already inside the network was supposed to be there and did not pose a threat.

Previous models of perimeter-centric security lack tiered trust, this lacked of tiered trust allows malicious users to gain sensitive information easily through even low level employee accounts. One of the biggest threats to the perimeter-centric security model is the careless insider. Willfully ignorant employees can prove disastrous to traditional security models. With stolen credentials a malicious user can gain access to privileged information. Zero Trust minimizes access, theoretically closing the roads to access sensitive data. The less pathways there are the easier it is to monitor.

The main issues with perimeter-centric security is that "it relies on the assumption that everything on the internal network can be trusted" (Tummalapenta, 2017). This cannot be the assumption anymore due to the fact that companies have "remote employees, mobile users, and cloud computing" that "blur the distinction between internal and external" (Tummalapenta, 2017). Employees bringing their own devices creates a large risk to security. Authorized users

are no longer all “housed within a defined and trusted corporate network perimeter” (Tummalapenta, 2017) which means IT managers can no longer solely focus on simply protecting the perimeter.

What is a Zero Trust Network?

A Zero Trust network assumes anyone trying to access the network is untrustworthy until proven otherwise. Would you assume that someone you don’t know is authorized to be in your home just because they found a way to get inside? This is the same sort of logic zero trust networks aims to address. The key to the Zero Trust network model is understanding that we can “no longer assume devices, applications, or user credentials and access are trustworthy simply because they are inside the perimeter” (Sverdiove, 2017).

A home intruder does not attempt to get in your house just to see if it’s possible. Once inside, they will begin to move around, take stock in what you have, and start stealing your valuables. Similarly, once the attacker is inside the network, they will begin to cause havoc, “some of the most egregious data breaches happened because the hackers, once they gained access inside corporate firewalls, were able to move around through internal systems without much resistance” (Pratt, 2018).

The never-ending landscape of high-profile insider attacks and data breaches demonstrate that traditional approaches to network security are no longer adequate. These breaches can prove costly for organizations and with the General Data Protection Regulation (GDPR) coming into effect in May it can become extremely expensive for organizations to be lax on security. To put this into monetary terms, “for a breach that results in less than 10,000 records being compromised, the average total cost is $1.9 million, but for 50,000 or more that rises to $6.3

million" (Drolet, 2018). Beyond cost, organizations risk damaging their reputation when breaches occur, which could spell the end of their business.

Zero Trust networks specifically aim to reduce the risk of insider attacks, which experts at Intel have reported are the cause of 43% of data breaches (Mello, 2017). The "malicious insider reality demands a new trust model" and the Zero Trust network provides just that with a "willingness to set aside preconceived notions about what the network should be and think about what the network could be. By taking the network down to the trust level, we can create the Zero Trust network" (Kindervag, 2010).

Trust Zones

Trust zones are a critical component to of Zero Trust architecture, a trust zone is a "distinct pocket of infrastructure where the member resources not only operate at the same trust level but also share similar functionality" (Palalto, 2016). The key here being that by sharing functionality, "such as protocols and types of transactions" (Paloalto, 2016) it provides the ability to "minimize the number of allowed pathways into and out of a given zone" and in turn "minimize the potential for malicious insiders and other types of threats to gain unauthorized access to sensitive resources" (Paloalto, 2016).

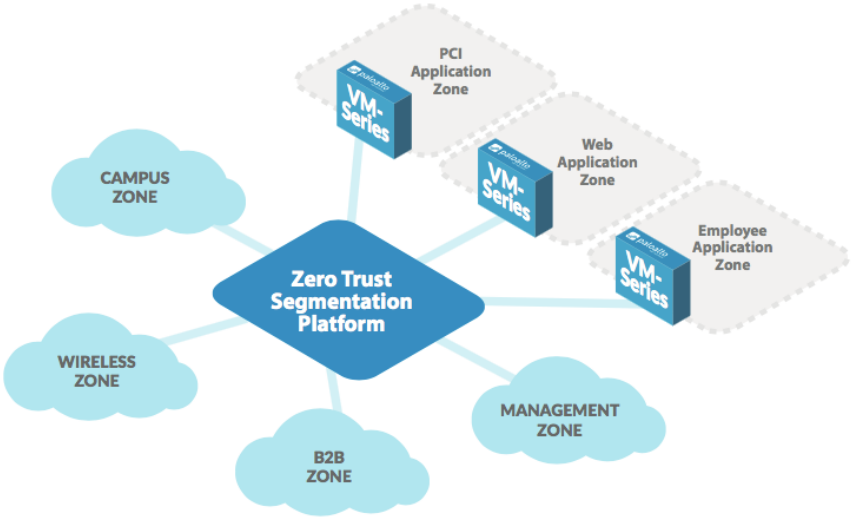

Figure 1. Trust Zones (Paloalto, 2016).

Figure 1 depicts an example Zero Trust segmentation. Trust zones are used to define and differentiate the internal boundaries within the network. In order to operate as Zero Trust is intended "the network would be configured to ensure that ALL communications traffic – including that between devices in the same zone – is intermediated by corresponding Zero Trust segmentation platform" (Paloalto, 2016). The above example shows a single component in a single location when "an effective implementation is more likely to entail multiple instances distributed throughout an organization's network" (Paloalto, 2016).

Google Application: Beyond Corp

Initiated by the 2009 "Operation Aurora" attack, Google's Beyond Corp is a "Zero Trust security framework that shifts access controls from the perimeter to individual devices and users". In a transition away from traditional perimeter security models, the Beyond Corp approach deploys all applications "to the public internet, accessible through a user and device-centric authentication and authorization workflow" (Beyond Corp, 2018). The result is the ability

for employees to “work securely from any location without the need for a traditional VPN” (Centrify, 2017).

Beyond Corps model relies heavily on a tiered access approach “which looks at the user’s individual and group permissions, the user’s privileges as defined by their job role, and the state of the device being used to make the request” (Rashid, 2017). Meaning that once successfully authenticated, a user is only able to access the amount of information that their job entails. Authentication is also dependent on the state of the user’s device. If said device does not have the latest security and application patches installed it will not be allowed to access the internal system regardless if the user is supposed to be accessing the data or not.

Requests to access are evaluated on a per request basis through an Access Control Engine. “The authorization decision is based on assertions about the user, the group to which the user belongs, the device identity, and the attributes of the device from inventory systems” (Beyond Corp, 2018). Google has a “culture of innovation that requires the freedom and flexibility to connect many different devices to many different assets and services. Tiered access was implemented in order to provide an access model appropriate for this very heterogeneous environment” (Google, 2017). The tiers allow Google owned android devices more access to sensitive data verses employee owned devices (BYOD) which are only given access to the lower trust tiers, “Tiered access de-emphasizes traditional passwords in favor for a more flexible and accurate means of providing identity” (Rashid, 2017).

	Examples of services accessible
Untrusted	• No Google data or corporate services (in general)
Basic Access	• Services with limited Confidential and Need-To-Know data exposure (e.g. campus maps and bus schedules) • HR data for the requesting user
Privileged Access	• Services with Confidential but not Need-To-Know data (e.g. bug tracking) • HR data with manager level access
Highly Privileged Access	• Access to all corporate services, including those that contain Confidential or Need-To-Know data. * Note that further authorization checks for this class of resources occur at the service and data levels as well

Figure 2. Beyond Corp Trust Tiers (Google, 2017)

Implementation into Legacy Networks

While it is easier to build security networks from the ground up, it is possible to use "zero trust to redesign legacy networks into modern networks so that they are compliant, secure, effective, and cost-effective". Implementation can roll out at a pace the organization is comfortable with, in fact "one of the great advantages of a Zero Trust architecture … is that it is conducive to progressive implementation" (Paloalto, 2016). Implementing the Zero Trust model into legacy network can be extremely daunting, "it forces you to unwind legacy infrastructure, legacy workflow and legacy processes that have been around for decades, in some cases". The fact of the matter is the larger your organization is, the more complex this process becomes and the "amount of legacy workflow, processes and systems that you have to account for" as well as the "flexibility of your organization to adapt to change, are all obstacles to implementation" (Carder, 2018).

While adapting the Zero Trust model into legacy networks can be difficult, there are ways to make the transition easier. James Carder, during the process of implementing Zero Trust into his company has identified six key steps for implementing Zero Trust into legacy networks:

1. Identify your sensitive or toxic data sources.
2. Identify roles and assign people to a single role.
3. Map transaction flows regarding the toxic data.
4. Architect a Zero Trust network based on the toxic data sources and the way they are used transitionally.
5. Write rules on your segmentation or policy gateway based on expected behavior of the data.
6. Monitor the network; inspect and log the traffic; and update rules based on your behavior analytics.

Adopting Zero Trust "principles at concepts at major access points to the internet also makes sense" however, "will probably require replacing or augmenting entrenched legacy security devices with a Zero Trust segmentation platform to obtain all of the requisite capabilities" (Paloalto, 2016). This gradual application can start with "low-impact, cost-friendly projects, such as software defined wide area network solutions, to encrypt and securely transmit data over a network" (Tummalapenta, 2017) and while "you can't go out and simply buy a Zero Trust network, you can use the architectural design components of Zero Trust to help you get past today's biases about how we should build networks" (Paloalto, 2016).

Management

As outlined by the creator of Zero Trust networks, John Kindervag, an "essential concept of Zero Trust is that you must inspect and log all traffic". If you're not analyzing the activity on your network there is little point to have any sort of security. There are however ways to make this analyzing process easier through the implementation of a Data Acquisition Network (DAN), "a DAN facilitates the extraction of network data … to a single place where you can then inspect and analyze it in near real time" (Kindervag, 2010).

Centralized management is a key factor for the Zero Trust network. This management provides "efficient administration and ongoing monitoring, particularly for implementations involving multiple, distributed Zero Trust segmentation platforms". It is critically important that network logs are inspected, "by forwarding all session logs to a data acquisition network, this data can then be processed by any number of out-of-band analysis tools and technologies … to further enhance network visibility, detect unknown threats, or support compliance reporting" (Paloalto, 2016).

Findings

Challenges of Implementation

All aspects of the organization need to be on board in order for a Zero Trust network to be successful. This is not an installation that can occur within one department, but rather a company-wide shift in network security. Certain aspects of legacy network security theory still apply. For example: it is important for department managers and Human Resources to be in constant contact regarding changes in employment status such as promotion and termination of employees. This information affects the users tiered trust level and should be kept current.

If an organization is operating in a virtualized network then scalability can be a challenge. If operating a large network, an organization may find its cost prohibitive to adapt the Zero Trust framework or face the issue that "stretched VLANs across data centers may add inefficiency or cost to the design" (Townsend, 2015) .

Beyond scalability, cost can play a factor in general implementation. From example in order to get the network running it "requires a large number of man-hours ... as well as to maintain going forward" (Mello, 2017). Due to the fact that implementation can be extremely costly an organization may need to adapt to the new model in stages. This can be done by conducting a risk assessment to identify "high-risk areas where permissions have been historically lax" (Mello, 2017).

Benefits of Implementing a Zero Trust Network

Zero Trust networks can help with compliance, and can scale with your business as it grows and the needs of the organization change, "one of the great advantages of a Zero Trust architecture … is that it is conducive to progressive implementation" (Mello, 2017). In practice this means that the Zero Trust model does not need out be rolled out at once, but can be added gradually as an organization grows and their needs change.

The Zero Trust model "tests and validates a user and device before allowing them on the network, which is different approach from Transmission control protocol/ Internet Protocol (TCP/IP protocol)" (Mello, 2017) which allows the network to ensure that the user is supposed to access the network before granting them permission to be there. TCP/IP "is the basic communication language or protocol of the Internet … when you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other

computer that you may send messages to or to get information from also has a copy" (Tech Target, 2014). Furthermore, TCP/IP "allows a packet to traverse into a network segment, shake hands with an application, and then present credentials. That's the equivalent of TSA letting you get on an airplane, letting the plane take off, and then asking you for ID and checking you for weapons" (Mello, 2017)

While it can be costly to set up and monitor, organizations can see costs cut in other aspects of their IT department. For example, "after Google deployed its zero-trust system, called Beyond Corp, across the company, it noted a 30% reduction in IT support tickets" which can be attributed to "improvements in security hygiene" as well as providing people with more intuitive messages as to "why a requested has been blocked and can deliver that message to the user in a more friendly manner" (Mello, 2017). Furthermore, organizations can start to see savings in regards to employee productivity. Considered a "natural by-product of Zero Trust networks" organizations can expect to employees to have a better "security posture" and being more aware of the things they are doing on the network (Mello, 2017).

Trust zones within Zero Trust networks isolates the traffic flow from one zone to another. These zones are compartmentalized, being authorized in one zone does not grant you access to the others. Similar to the water tight compartment on ships, if water enters one compartment it does not sink the ship. Therefore, "an intruder penetrating your wireless LAN would be limited to access defined for wireless users. If the rules prevent wireless access to the servers there would be no danger of a data breach from this zone" (Convington, 2015).

Recommendations

Experts stress that "it is important for IT security managers and architects to realize that it is not necessary to instigate or wait for the next comprehensive overhaul of their organization's network and security infrastructure" (Paloalto, 2017), there are ways organizations can make small tweaks to their existing system. One of the great things about Zero Trust networks is that it can be rolled out at the pace the organization is comfortable with and can scale along with you as you grow. If choosing to roll out a Zero Trust network slowly then the key becomes to assess what is most important to the organization and start the implementation process there.

Robert C. Covington presents the idea of "Zero Trust Lite" based on an understanding that the full implementation of the Zero Trust model is "complex and expensive, and thus beyond the current reach of much of the business world". Zero Trust Lite requires organizations to define the network into segments, dedicate one or more network switches to each of the newly created segments, use a full-featured firewall at the core connecting all of the segments, and implement tools to insure access controls and least privilege (Covington, 2015). This lite approach allows organizations of all sizes to move towards a Zero Trust architecture within a budget they are comfortable with while still benefiting from the enhanced security it provides.

It is abundantly clear that if an "organization [is] looking to substantially improve their defensive posture against modern cyber threats and more reliably prevent the exfiltration of sensitive data should consider migrating to a Zero Trust security architecture" (Paloalto, 2016).

Organizations attempting to implement Zero Trust networks today have the benefit of using Google's implementation as a model for a successful rollout. The success of Beyond Corp relied on multiple teams, "at a large enterprise scale, it is impossible to delegate the entire transition to a single team. The migration will likely involve some backward-incompatible

changes that need sufficient management support" (Gilman & Barth, 2017) The extensive use of "sandboxes" allowed developers to test how advanced scenarios would affect the network before being fully implemented.

Future Research

Further research should still be conducted on the ability for large scale organizations to successfully adopt Zero Trust networks into their legacy network architecture. Google had a lot of time and resources at their disposal in order to make the transition a success. Research focusing on non-technology sector business adapting to the Zero Trust model would be beneficial.

Conclusion

Introduced in 2010 and now fully implemented by Google, Zero Trust Networks can prove to be the perfect solution for organizations trying to stop the bleeding of sensitive information. While Zero Trust networks are not completely hack proof, this new take on network architecture provides a tiered access model which can help organizations ensure that sensitive information is only accessible to employees who are required to use it.

In order to "fulfill expectations of the future, networks need to be simpler and easier to manage [as well as] become more intuitive and inherently secure" (Kindervag, 2010). Employees accessing sensitive data from places they should not be and on devices that are not secure is going to continue to be a problem in to the foreseeable future. While it can be difficult to control behavior, organizations can control access. It is wise to trust as little as possible because once trust is built into a network, it can be very hard to remove it (Gilman & Barth, 2017).

References

Carder, J. (2018). How to approach a zero trust security model for your enterprise. *CSO*. Retrieved from https://www.csoonline.com/article/3253571/endpoint-protection/how-to-approach-a-zero-trust-security-model-for-your-enterprise.html

Centrify. (2017, November 27). Centrify innovations embrace zero trust security. Retrieved April 7, 2018, from Centrify Business Wire website: http://www.businesswire.com/news/home/20171127005105/en/

Covington, R. C. (n.d.). Throw out the trust, and verify. *CSO*. Retrieved from https://www.csoonline.com/article/2944794/network-security/throw-out-the-trust-and-verify-everything.html

Drolet, M. (2018). What does stolen data cost [per second]. *CSO*. Retrieved from https://www.csoonline.com/article/3251606/data-breach/what-does-stolen-data-cost-per-second.html

Gilman, E., & Barth, D. (2017). *Zero trust networks: Building secure systems in untrusted networks*. Sebastopol, CA: O'Reilly.

Google. (2017). *Mobile best practice: Tiered access at google*. Retrieved from https://lp.google-mkto.com/rs/248-TPC-286/images/eBook%202%20-%20Tiered%20Access_v5%20-%20Google%20Cloud%20Branding.pdf

Kindervag, J. (2010, November). *Build security into your network's DNA: The zero trust network architecture*. Retrieved from http://www.ndm.net/firewall/pdf/palo_alto/Forrester-Build-Security-Into-Your-Network.pdf

Mello, J. P., Jr. (2017). Is the key to bulletproof security zero-trust networks? *Tech Beacon*. Retrieved from https://techbeacon.com/key-bulletproof-security-zero-trust-networks

Paloalto. (2018). *Getting started with a zero trust approach to network security*. Retrieved from https://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwjcsK-Fn6baAhVEja0KHSCWBS8QFgh1MAQ&url=https%3A%2F%2Fwww.paloaltonetworks.com%2Fapps%2Fpan%2Fpublic%2FdownloadResource%3FpagePath%3D%2Fcontent%2Fpan%2Fen_US%2Fresources%2Fwhitepapers%2Fzero-trust-network-security&usg=AOvVaw3sT23ryr6hPGdWqAWe0gPi

Pratt, M. K. (2018). What is zero trust? A model for a more effective security. *CSO*. Retrieved from https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html

Rashid, F. Y. (2017, April 25). Google zero-trust security framework goes far beyond passwords. Retrieved April 10, 2018, from Infoworld Tech Watch website: https://www.infoworld.com/article/3192244/security/google-zero-trust-security-framework-goes-beyond-passwords.html

Sverdiove, H. (2017, November). Edgewise networks founder & CTO to speak at O'Reilly security conference on zero trust networking. Retrieved April 7, 2018, from Business Wire website: https://www.businesswire.com/news/home/20171030005135/en/

Tech Target. (2014). Understanding TCP/IP. Retrieved April 14, 2018, from https://searchnetworking.techtarget.com/tutorial/Understanding-TCP-IP website: https://searchnetworking.techtarget.com/tutorial/Understanding-TCP-IP

Townsend, K. (2015). Don't implement zero-trust security in a virtualized network without reading this overview. *Tech Republic*. Retrieved from https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html

Tummalapenta, S. (2017). A zero trust model for living in a hacked world. *Security Intelligence*. Retrieved from https://securityintelligence.com/the-zero-trust-model-for-living-in-a-hacked-world/