ZIVARO
BRILLIANT IT

Modernizing Enterprise Networks to Exceed Compliance Outcomes

Cliff Flowers
EVP Engineering Services

INTRODUCTION

Companies desire solutions to maintain confidentiality, integrity, and availability of their data as well as the data of their customers as part of their overall information technology approach and to maintain a robust security posture. In regulated industries, cybersecurity compliance is often mandated and must be recertified on a regular basis, typically annually. This need for tighter security is increasing and many companies are approaching security from a “*we’ve already been compromised*” perspective. Increasing sensitivity[1] to public criticism resulting from a breach is a major contributing factor in awareness. The negative public image can culminate at the highest offices of the country and published in reports such as the “Committee on Oversight and Government Reform – The Equifax Data Breach”[i] . This awareness is resulting in more discussions and requests on how to implement Zero Trust solutions which appropriately limit access to resources to only those with a “need to know.”

BACKGROUND

The need for a systematic approach for security compliance across an organization’s infrastructure is more critical today than ever before. Compliance historically has come with some negative connotations. In the earlier days of IT security compliance it was more common for organizations to ‘check the boxes’ on compliance requirements rather than fully defending their environments while maintaining compliance. A focused and strategic effort, regardless of industry, has become more than just the next “bolt-on” security tool and has become a core component in IT roadmaps. In the Department of Defense, the Risk Management Framework is the clear guide for not only security controls required for implementation, but also for continuous monitoring throughout any system’s lifecycle. In the Commercial market, a holistic review of a Cybersecurity Framework determines the applicable controls. This framework has additional requirements in submarkets whether that’s HIPAA requirements for Healthcare, PCI DSS, FFIEC, 23 NYCRR 500 requirements for the Financial Sector, or very specific American Water Works Association J100-10 Risk and Resilience Management of Water and Wastewater Systems requirements dictated by the Environmental Protection Agency to critical utility infrastructures.

Although specific regulations or compliance guidance may differ by industry, each approach is either directly, or indirectly, in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework or other cyber standards documented by that organization. As companies continue to migrate to an “access by exception” security approach, an access control methodology across the infrastructure that includes training for personnel and process improvements supported

[i] U.S. House of Representatives, Committee on Oversight and Government Reform, The Equifax Data Breach - Majority Staff Report, 115th Congress December 2018

by technology evolution become the focus for an improved security posture.

One key evolution of the cybersecurity world in support of compliance is the rise of Zero Trust security. Zero Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the Internet) or based on asset ownership (enterprise or personally owned).[ii] Part of implementing a zero trust architecture is enabling a robust Authentication, Authorization, and Accounting (AAA) implementation within a network.

Zero Trust is exactly what it sounds like – nobody, no software, no device or endpoint trusts any other - or at least almost nobody else. Not only that, but trust needs to continuously validated. Networks over the years have evolved. Not too long ago – and in many networks today still - the internal and external networks were well defined and relatively easily controlled. You had a firewall with an inside interface with all your hosts that you trusted and an outside interface where, everything was suspicious, distrusted, and needed to be closely monitored if not blocked altogether. If and once you were connected to the inside network you had nearly free access to anything and everybody on the network.

PROBLEM STATEMENT

With the explosion of security malware/worms etc. that easily propagate from host to host, traditional approaches to compliance have largely become untenable architecture. In order to significantly improve an organization’s security posture, a zero trust architecture demands that no host may communicate with any other host without specific security controls and proper AAA implementations. For example, there is typically no need for end user workstations to communicate with each other. For the sake of simplicity and manageability many times these user networks are lumped into one extensive subnet with no East-West controls. Similarly, while IP phones will have a need to communicate with each other and often with a workstation, especially for advanced integrations, this communication happens on specific ports. Implementing zero trust demands that East-West traffic, e.g. workstation to workstation, IP phone to phone, workstation to phone, workstation to printer, etc. be blocked or strictly limited to specific channels and it should be monitored for suspicious behavior. This type of requirement maintains NIST compliancy and supports the implementation of most security controls.

“Zero trust is a strategic approach to security that centers on the concept of eliminating trust from an organization's network architecture. Trust is neither binary nor permanent. We can no longer assume that internal entities are trustworthy, that they can be directly managed to reduce security risk, or that checking them one time is enough. The zero-trust model of security prompts you to question your assumptions of trust at every access attempt.” [iii]

i. https://csrc.nist.gov/publications/detail/sp/800-207/final

SOLUTION

Zivaro recently was tasked with implementing a robust AAA solution for one of our clients in the defense industry. We started by assessing the businesses current AAA standing and found it to be severely lacking in the Accounting section. Our next step was to view all applicable regulations. After review we found that this business was required to adhere to all Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs) and that their security scans showed quite a number of vulnerabilities related to missing 802.1X and AAA commands in their network devices. We worked with the technical team to determine the best solution to meet their business needs, and implement a zero trust architecture to align with their AAA requirements. Ultimately, the best solution that met all requirements was Cisco's Identity Services Engine (ISE) because it has the total package. After reviewing their operations forecast we came up with a plan to roll out the full implementation in pieces in order to minimize downtime and meet regulatory requirements as soon as possible. We gracefully failed-over from their old solution to ISE after updating all switch configurations within hours of standing-up the ISE server. The business went from no accounting to a full ISE accounting solution in less than a day with no downtime. Due to operational constraints, we planned the 802.1X roll out for early 2021.

*"With the zero-trust model, you gain better visibility across your users, devices, containers, networks, and applications because you are **verifying their security states with every access request**. You can reduce your organization's attack surface by **segmenting resources** and **only granting the absolute minimum access needed.**"* [iV]

There is an extensive solution set available for implementing zero trust in the Cisco portfolio, in the spirit of great security and superior compliance. It should also be stated that any path to zero trust is a journey and not a project based set and forget style deployment. Cisco is a solid leader in Zero Trust ecosystem and received top scores both with respect to current product offering as well as its overall strategy[v] . Cisco distinguishes its solution portfolio between **Workforce**, **Workload**, and **Workplace** focused. The applicable solution portfolio includes the following:

Cisco Duo, a fairly recent acquisition by Cisco, provides multifactor authentication (MFA) across various systems for the **Workforce**. Duo is extremely user (and admin) friendly and allows MFA using smart phones, SMS, flip phones, land lines, or email with the smart phone app of course being the easiest and most user friendly. Overall Duo is simple to deploy and can authenticate users across multiple platforms. It can provide MFA for VPN users, AD/Desktop logins, Office 365, and dozens or hundreds of other applications. Quite frankly, there is really no excuse for not implementing full MFA as part of your Zero Trust architecture with a product as easy to deploy and use and cost effective as Duo.

Tetration is the Cisco solution for Zero Trust architecture for **Workload** protection and is designed to support both on prem and cloud based workloads. Tetration uses machine learning, behavior analysis, and algorithmic approaches to offer a all-inclusive workload protection strategy. Tetration allows one to contain lateral traffic movement by implementing operational microsegmentation, dynamic identification of security incidents utilizing behavior analysis, and reduction of the attack surface by identifying software-related vulnerabilities. Tetration uses software agents on servers (virtual machines, bare metal, or containers) to collect telemetry data and to enforce a consistent, distributed zero-trust policy at scale. Tetration also integrates with Cisco AnyConnect and Cisco

[iv] https://www.cisco.com/c/en/us/products/security/zero-trust.html

Identity Services Engine (ISE) to bring user and endpoint context into the segmentation policy. The Tetration system uses an allow-list security model which provides more front-end protection: no waiting for malware to be identified before you can list the name and then avoid it. A zero-trust model requires an allow-list policy. The Tetration platform of course provides flexible on-prem deployment or software-as-a-Service (SaaS) options.

Software-Defined (SD) Access, finally provides a software-defined approach for network segmentation extending the Zero Trust architecture to the **Workplace**. SD Access is not a standalone application but rather encompasses a set of components including DNA Center, Identiy Services Engine (ISE), and Wired and wireless networking infrastructure. Within SD-Access, DNAC provides visibility into what's on the network using AI endpoint analytics while ISE provides Network Access Control (NAC) which in turn forms the foundation of a zero-trust implementation. Within DNAC and ISE, TrustSec with Security Group Tagging (SGT) provides a quantum leap in simplifying network segmentation. Rather than rely on VLANs and ACLs on switch ports, endpoints are profiled and tagged with a SGT, a logical policy grouping, at ingress and traffic flow can be managed centrally managed using matrix style permissions across classes of traffic.

So, does this all sound complicated and expensive? In short, yes and no. Rarely should or will zero trust be deployed as a single project or initiative. A zero trust architecture comprises multiple components that work harmoniously together to provide a tighter, more secure infrastructure and better security posture. A "divide and conquer" approach is all but necessary. The key is twofold. One is to prioritize based on busisness needs – ROI applies to security as with anything else but that's another topic. The second is to keep forward momentum. Many organizations get bogged down in daily operations and struggle with the required lift of adding security related architectural components. There is some "low haning fruit" so to speak with respect to zero trust however. With respect to **Workforce**, Duo is quite easy to deploy (and free trials are available) and the security posture improvements are substantial. Tetration, on the **Workload** side, can be deployed as SaaS making it quite easy to stand up even if an initial limited proof of concept. Concerning **Workplace**, ISE is natural starting point providing any combination of profiling, NAC, guest access control, TACACS+, etc. but again, should be tackled in phases. Finally, on the cost front Cisco provides attractive Enterprise Licensing which benefits customers using more than two or three of Cisco's solution set.

CONCLUSION

Compliancy requirements are driving business decisions across industries not only to increase infrastructure security postures, but to drive standards in regulated markets. Specific compliancy standards vary from industry to industry and are often expanded upon beyond just the NIST-based standards. Networks that lack a good cybersecurity solution lack the situational awareness required to ensure compliance, network security, stability, and overall health in protecting the business and customers from malicious actors and data loss. Cisco's ISE solution has everything required for a comprehensive zero trust solution that supports AAA meeting any business's compliance requirements. Beyond Cisco ISE, there are other market-leading solutions from Cisco that help fill out a robust security architecture including Duo and Tetration. Staying compliant with NIST and other standards, regardless of the industry, will pay for itself over time by helping protect networks from malicious activity and keep organizations healthy from an ever-evolving threat landscape.

v. The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020