MAZEBOLT

WHITEPAPER

Why Zero Trust Cannot Prevent DDoS Attack

Table of Contents

Why Zero Trust Cannot Prevent DDoS Attacks

Introduction

`When there is a need, a solution arises' is the principle governing most innovations. As is with the Zero Trust framework or process that is an outcome of the vulnerabilities in networks and VPNs. In most cases, prophetic innovators sense the problem even before it becomes a problem. So too, in the case of network security over a decade ago, John Kindervag, an industry analyst at Forrester, reinitiated an old concept called 'Zero Trust'. The philosophy of Zero Trust is that assumptions of trust can prove to be disastrous for enterprise security and even a small error, or mistake can lead to security breaches, data loss and ultimately, revenue, customers, and ultimately business loss.

Zero Trust, as discussed in detail in this whitepaper, has gained large-scale recognition and is being widely adopted by enterprises across the world to ensure network security. It is also a fact that Zero Trust has proven security benefits but there needs to be more clarity on how well equipped it is to prevent DDoS attacks. This question is highly pertinent in today's world for the following reasons:

a. The strong security challenge that DDoS attacks pose to enterprises.
b. The depth of damage that these attacks can cause to these enterprises.

This whitepaper delves into VPNs and their vulnerabilities, Zero Trust and its strength to protect networks, and finally an understanding of its uses and ability to prevent DDoS attacks.

Virtual Private Networks (VPNs) – An Overview

Virtual Private Networks (VPNs) are private networks that are linked to the public internet, and work through private circuits which reside on top of the existing networks. VPNs are more trusted than Wi-Fi hotspots as they ensure greater privacy and security. VPNs encrypt data to secure services enabling people to access their official emails, on-the-go, without having to worry about data leakages. The process of encryption involves scrambling data making it difficult to intercept.

Gartner describes a VPN as

> `A system that delivers enterprise-focused communication services on a shared public network infrastructure and provides customized operating characteristics uniformly and universally across an enterprise.'

VPNs are largely used by enterprises, over the years, to empower remote employees to access folders and files wherever they are. An example of its usage would be sales professionals on the field who need to access RFPs, invoices, and other documents to close sales deals without delay. VPNs would also help sales professionals to forward documents to concerned departments by email on-the-go. VPNs would therefore help reduce dependency on being in the office to access applications and data, and instead provide flexibility to employees to access these anywhere and everywhere securely. VPNs have always been extremely useful for offices to ensure connectivity amongst employees no matter where they are without having to worry about security issues.

VPNs provide users, once connected, access to the network, critical applications, and infrastructure. This keeps the internal systems wide open for security breaches simply because of the access it provides. An analogy would be a bank's safe room which has complex digital locks at the entrance, but once these locks are opened, the entire contents of the safe lie open. Despite this security handicap, VPNs have always been used by enterprises to provide remote access to employees and business partners, the reason being their advantages far outweighed the limitations.

VPNs Come to The Forefront During the Pandemic

That is until the emergence of the COVID-19 pandemic. During peak phases in from 2019 to 2021 when governments worldwide enforced lockdown, organizations across the world moved from office settings to work-from-home models, to ensure business continuity. As a result, CISOs and IT professionals began scaling up their remote access services to support their entire employee base, so business continuity is not impacted while employees work from home.

But many of them were not prepared for the challenges that would ensue. According to a study by OpenVPN conducted in 2019, 24% of companies had not updated their remote work security policy in over a year, and 44% say their IT department did not lead the remote work security policy plan.

One of the primary concerns that organizations face with VPNs is tied to security and ensuring ongoing security of their applications, infrastructure, and data. This sudden enhanced dependency on VPNs needed IT teams to scale up security measures. This would involve a wide range of possible activities from defining permissions, security, expanding infrastructure to setting up remote access for most employees who usually do not need it. Combine these with the fact that enterprises only saw the VPN as a standby for remote workers that constitute a small percentage of their entire workforce and one can see how the VPN has opened a pandora's box of challenges for these companies.

Unsecure VPNs and Networks Pave the Way for Zero Trust Networks

The primary and most significant challenge with VPNs lies in the fact that users, once signed in, have access to the entire network, applications, and infrastructure. There is no real way to monitor what goes on once a user has logged in. This is a huge internal security threat. This weakness has been exploited by malicious attackers who have managed to penetrate VPN protocols with the intention of causing security breaches. This is the external threat faced by VPNs. This threat is further magnified by the number of users having access to the VPN. The more users, the less control that the IT team has over its security.

The limitations of VPNs as well as the fact that enterprises offer full freedom to users to their network and applications, once logged in, has been a growing concern for enterprises. with VPNs or secure networks, it is challenging to gain access from outside, but once users log in, have access, they are all trusted by default, and they have access to everything within.

The significance of this phrase needs no examples or proof. Governments and enterprises of all sizes have fallen victim to different forms of exploits and cyber-attacks. As a result, Zero Trust takes greater significance and implies that no one, not a single person should be trusted from inside or outside a network. To ensure that the weaknesses in existing VPN and network access is overcome, Zero Trust policy requires additional authentication and is limited within the network, depending on the individual, his function, and his requirements.

A simple example, and to go back to the earlier sales analogy, refers to which parts of the network, an application or data source would a sales manager need access to? Would he need to access the entire network or to certain folders and applications? With Zero Trust, he will have access, after logging into the network, only to those sources of data or application that he needs to access. Utilizing a policy called 'micro segmentation' Zero Trust breaks up larger chunks into small zones that require separate access.

Zero Trust controls user access by requiring multiple authentications for different accesses, such as, the first authentication to enter the system, another authentication to access a folder and so forth. Along with this user control, enterprises also ensure device control by monitoring the different devices used to access a system. An example of this is when one tries to access emails from a friend's system by entering username and password, an immediate alert is set off, to the user, the current system and sometimes system admin requesting confirmation that it is the same individual and not a breach.

An easy way to relate to Zero Trust is, instead of securing endpoints, access to endpoints is limited. If this is understood, then Zero Trust can be understood.

Zero Trust has proved to be extremely useful during the unsecure COVID-19 pandemic phase for businesses. It has managed to deal with the vulnerabilities posed by insecure VPNs and complex networks. To explain, larger the network, higher the vulnerability when all users gain access through single authentication. Controlled access has helped to reduce vulnerabilities and helped to ensure higher levels of security.

Gaps in Zero Trust when it comes to DDoS protection

It is virtually impossible for any enterprise to eliminate cyber risk, however when you follow Zero Trust diligently it can help bring the risk factor down. But, in some cases, such as DDoS, Zero Trust may not be useful to either predict or prevent attacks. The reason for this is that Zero Trust is a framework; it is not a tool or an application. It defines security policies that will help prevent breaches. To maximize its uses, enterprise IT teams must take the framework, customize it for their own unique requirements, roll it out, and periodically review the entire process to ensure it is up to date. To a large extent the entire network or framework is under the control of the Zero Trust policy maker. If access to the network or Policy Maker's entrance point is attacked, and denied access, the entire operations under the policy maker's control will be affected. It is like taking down the King in a game of chess. If the king is down, the game is over and so too if DDoS attackers go after the policy maker's network entrance point and attack it, then the entire network's internal controls come to a halt.

One way to avoid going down fully, would be to have the Zero Trust policy replicated and in different places so if one point is attacked then another can take over. But this is also not fool-proof and it helps to lower risk but does not completely eradicate risk.

This is the larger picture but as explained earlier, when a user gains access to a certain application after authentication, there is still no way to monitor the user's activities. The framework does not assure additional visibility into the network or how information is stored. Since the framework largely focuses on internal security, external threats such as DDoS can continue to pose challenges to enterprises. There is also the possibility that a user's account could be used to launch an attack against the Zero Trust policy maker, denying further access and thereby affecting all the points under his control.

Count on Zero Trust for Internal Security Not DDoS Protection

Zero Trust as a framework can help prevent internal cyber breaches, but it is not meant to prevent attacks coming from outside. The solution is to follow Zero Trust for internal security and adapt DDoS protection for network security from external forces. Enterprises should invest in DDoS mitigation solutions to complement their Zero Trust networks to ensure complete DDoS protection.

It is also important for Zero Trust policy makers to have a complete understanding of the DDoS threat landscape as Zero Trust can create a false sense of security. DDoS risk today is not a static but a dynamic challenge. The DDoS threat landscape is continuously shifting with new threats, new vulnerabilities, and new forms of attacks emerging almost on a day-to-day basis. For businesses, the impact of DDoS attacks is substantial both in the short and long terms. Short-term damages are costs associated with downtime/latency, and loss of immediate revenue, personnel costs associated with mitigating attacks. The long-term impact would be customer churn, regulatory repercussions, and compromised data. The blog `Calculate the Cost of DDoS Attacks' explains in detail the repercussions of DDoS attacks for enterprises.

Can DDoS Mitigation Be the Answer?

To some extent mitigation along with Zero Trust could provide an answer to worried policy makers. However, even with the most sophisticated DDoS mitigation and testing solutions deployed, most companies are left with major DDoS vulnerabilities. DDoS Mitigation security policies do not adapt to dynamic changes happening in the network, leaving around 50% of DDoS vulnerabilities undetected and therefore unprotected. Furthermore, mitigation solutions & infrequent Red Team DDoS testing are reactive, rather than automatically and continuously detecting and closing vulnerabilities.

The inherent shortcomings in mitigation solutions are visible to all and can be seen in the DDoS attacks that continue to cause severe damage to businesses worldwide. In May 2021 a large-scale DDoS attack was the cause of several sections of Belgium’s internet going down. Several organizations in Belgium, including the government and parliament, were affected by this DDoS attack that overwhelmed them with bad traffic.

There were several more attacks, and they are captured monthly here. All if not most of the enterprises that were attacked had mitigation solutions in place. Despite this, massive attacks continue to occur with the intention of taking businesses, enterprises, governments, and sometimes entire countries offline. For many such companies, disruption of information technology (IT) services can directly correlate to lost revenues. Finally, customer expectations have increased, and there is an expectation of `always-on connectivity, which means that businesses cannot afford any downtime whatsoever.

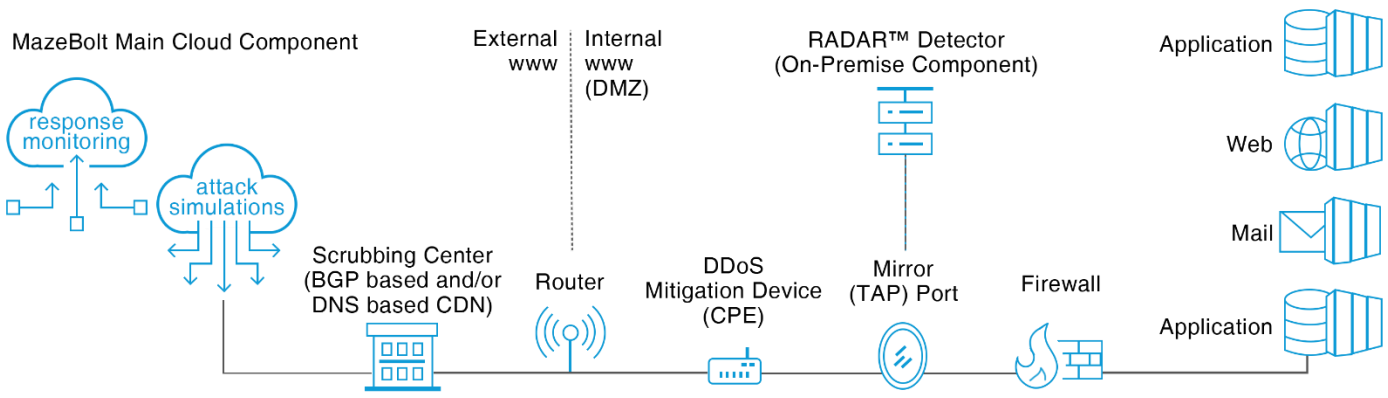
Simulate DDoS Attacks with no Downtime!

1. Enterprises should remain convinced about the urgency to manage the threat landscape and invest in innovation by adopting technology solutions that provide DDoS protection. Protection instead of mitigation is key to ensuring DDoS protection irrespective of changes to the network or new DDoS threats.
2. To effectively block complex and intermittently changing threats, enterprises should continuously validate and remediate the entire DDoS protection posture regularly, fix known areas of weaknesses proactively as there is no time to do this when an attack starts.
3. Break complex attacks into individual attack vectors to ensure protection automatically against mixed vector attacks.
4. Start at a low rate and increase attack simulation to identify new potential targets that are susceptible to attacks from external attackers.
5. Monitor all simulated traffic downstream from the DDoS mitigation device or scrubbing center on a mirror port during simulation to detect attack leakages instantaneously and remediate them on-the-go.
6. And, following the Zero Trust framework maintain good DDoS mitigation posture, i.e. no disruption or downtime.

Introducing MazeBolt's RADAR™ Technology - Simulation Without Disruption:

RADAR™, MazeBolt's new patented technology solution, is the only 24/7 automatic DDoS attack simulator on a live environment with ZERO downtime/ disruption. It automatically detects, analyses, and prioritizes the remediation of DDoS vulnerabilities in any mitigation system. RDAR™ raises the efficiency of your mitigation solution, delivering the ultimate DDoS protection.

The DDoS RADAR™ Network Setup



This new technology allows you to address the two gaps discussed above through:

RADAR™, MazeBolt's new patented technology solution, is the only 24/7 automatic DDoS attack simulator on a live environment with ZERO downtime/ disruption. It automatically detects, analyses, and prioritizes the remediation of DDoS vulnerabilities in any mitigation system. RDAR™ raises the efficiency of your mitigation solution, delivering the ultimate DDoS protection.

Vulnerability identification across the complete attack surface, automatically discovering the attack surface, running thousands of non-disruptive smart attack simulations against protections in place to identify the entire vulnerability landscape.

Guided Remediation Process and Revalidation of specific network vulnerability intelligence collection throughout the process creates a prioritized remediation plan, guiding customers in closing vulnerabilities in the most accurate and effective manner.

Finally, the system immediately revalidates the protection level, ensuring the highest level of protection is achieved.

Learn how RADAR™ Simulates DDoS Attacks And Protects Live Environments

About MazeBolt

MazeBolt introduces a new standard in DDoS coverage, automatically detecting, analyzing, and prioritizing remediation across the network, doubling coverage, and virtually eliminating DDoS exposure without shutting down organizational operations. MazeBolt's continuous defense supercharges the performance of CISOs as well as the mitigation service provider.
.

For more information, please visit: http://www.mazebolt.com or e-mail: info@mazebolt.com