MAZEBOLT

WHITEPAPER

The Right Choice DDoS Mitigation Considerations

Table of Contents

Executive Summary

Every DDoS mitigation system on the market works; it's just a matter of degree. The key is choosing a robust, appropriate solution that can be fine-tuned and hardened for your individual environment.

Before you start examining individual technologies in depth, you need to determine your exact needs. The one-size-fits-all approach is actually the reason that most DDoS protection systems fail almost 50% of the time.

The Big Picture

Strategic Risk

Risk varies greatly by organization and type of business. Acceptable risk needs to be determined on a case-by-case basis. Considerations include downtime, loss of revenue and reputation, network access for remote workers, and more.

A financial institution with a customer base that depends on 24/7 accessibility has a greater need for DDoS protection than a small private hospital with a website serving as an advertisement; its crown jewels, its patient records are not accessible through the Internet.

The Clock

On-Demand vs. Always on Protection

DDoS protection comes in two flavors –

- Always-on continuous protection
- On-demand

The higher your risk, the more likely "*always-on*" is the right solution.

Other technical risk considerations include whether your network is cloud-based, on-premises, or hybrid. Even an on-premises-only network can reduce risk by using a cloud-based, fully managed cloud scrubbing service, which automatically filters suspicious traffic.

To take it a step further, enterprises with multiple branches should be using scrubbing services "close to home" to reduce latency.

Scrubbing centers themselves need to have large enough bandwidths to handle large attacks against multiple clients simultaneously. Check their capacities when comparing scrubbing centers. Terabits per second (Tbps) and gigabits per second (Gbps) are good benchmarks that can be compared to test scalability.

Time to Mitigation

A DDoS attack can take only a few minutes to bring your system down, but it may take hours or days to bring it back up again. Once an attack is detected, you need to know how long it will take for your DDoS mitigation system to respond.

The Equipment

The Basic Features

Every system needs to fulfill the basics:

- Scalability
- Redundancy
- Reliability
- Ease of use

Device Control

As for the complexity issue, the more components within a DDoS mitigation system, the more software and hardware that needs to be kept up to date.

A DDoS mitigation system consisting of a scrubbing service combined with an onsite DDoS mitigation device (CPE) that feeds into network packet brokers requires management of multiple systems, including upgrade management, configuration management, minimizing downtime, and ensuring ongoing compatibility.

The Power of Pass Through

Volumetric attacks – layer 3 and layer 4 attacks – depend on sending high volumes of requests through your network. Your mitigation solution needs to be able to handle this volume without your having to invest in extensive network bandwidth.

If you have an on-premises mitigation system, you are limited to your network's capacity – and during an attack that manages to send traffic higher than your network capacity, your network will come down.

The Mitigation

Types of Protection

During an attack, one of two methods will kick in –

Border Gateway Protocol (BGP), which protects your entire network.

The second is Content Delivery Network (CDN), a DNS-based redirection, which protects only a single server.

If you are an enterprise, a combination of BGP and CDN is probably the setup that will be most effective.

True or False Positive

While volumetric attacks are generally easy to identify, low-and-slow attacks like SlowLoris appear to be legitimate traffic. The mitigation system you choose needs to be accurate enough to ensure that legitimate traffic does get through, while the low-and-slow attacks are stopped.

Extremely short-duration burst attacks can also disguise themselves as false positives, keeping your system busy with analysis, so other threats can more easily pass through to access your sensitive data through another cyberattack vector.

System Flexibility

Not all mitigation systems achieve the same results. A DDoS system deployed on-site (customer premises equipment-CPE) that protects against application layer 7 attacks may not be effective against volumetric attacks. Similarly, scrubbing solutions protect mainly against volumetric attacks.

When mixing and matching DDoS mitigation systems, you need to ensure that the combined result protects against layer 3, 4, and 7 attacks. DDoS attacks come in thousands of flavors but the parent attacks of these variations are actually much lower. While it may be best to test against hundreds or thousands of attack vectors, it's not practically possible to do so, since you would need months of one single continuous 24x7 maintenance period to do so.

Validating your environment against the 18 BaseLine types of attacks will validate much of the implied vulnerability of the hundreds of other vectors and ensure maximum reliability of your DDoS security posture.

The Brains

Intelligence Before the Attack

The ideal mitigation system is one that "learns" from your organization before an attack even becomes a possibility. It examines existing visitor and network behavior to create a normalized profile of the type of traffic your business faces. For example, a financial institution may have more traffic on its online banking software on the first and 15th of the month, while an online retailer may have maximum traffic from October-December 25, with a sharp drop-off until Valentine's Day sales.

A flexible DDoS system will let you define different policies for each service, allowing you to differentiate how each type of message is treated for behavioral analysis and routing.

The Visible, Intelligent System

While you may have control over your onsite systems, is the technology set up to provide visibility? You need transparency; the ability to be able to see "inside" the working mechanisms of the technology deployed assists greatly during an actual attack. Even if you are using an outsourced solution, you need to be sure that you receive as close to real-time-as-possible updates to determine the kinds of risk your network is facing, so you can better prepare yourself if an attack does get through.

You need to be able to see the volume, type of attack, the attack vectors, the source, and the specific areas of your network under attack.

Now, with AI, machine learning, and data science, DDoS mitigation systems are also trying to keep up. The more intelligence you can collect from DDoS attacks,

the better off you are. When your system protects you against an attack, you can see exactly where it succeeded. When it fails, you can see exactly what component went wrong and how to mitigate it for next time.

A more intelligent mitigation system will deliver better results when it comes to accuracy. Systems that rely on threat intelligence can ensure that the latest types of attacks are caught.

Notification

Being the target of a DDoS attack is a "when" not an "if." How will you find out? Ensure your onsite system is set up to automatically send alerts to designated IT team members when the attacks happen. If you are working with an MSSP or scrubbing center, ensure they, too, have an automated alert feature.

The People

The Role of Service-level Agreements

Your scrubbing center or vendor of your onsite system may be promising you the world. However, what are you actually getting? Note the response time requirements, the expected results, and the availability of the support team. Also note the attack types, size, and duration.

Make sure your SLAs are to the highest standards – and then, when you're attacked – ensure they were actually met. If those SLAs aren't met, it's time for a tough call with your vendor.

Team Preparedness

No matter the type of system you ultimately choose, it needs to be managed. Does your team have the capacity to manage the system internally? Should you outsource management?

If you are using a scrubbing center and something goes wrong, how accessible are their personnel?

Are their teams and your teams trained to mitigate zero-day DDoS attacks?

Proper procedures need to be put in place before a catastrophic event to ensure that everyone is prepared for the worst. BaseLine testing not only ensures that the systems are prepared, but also that the people are ready.

The Money

Cost v. Protection

The price of a comprehensive DDoS protection solution for an enterprise can range from the tens of thousands to millions. Regardless of the price, you need to make sure DDoS systems are fine-tuned for your environment. A BaseLine test can determine your true ROI and total cost of ownership (TCO). TCO can be exceptionally high if your system fails; downtime adds up quickly.

Conclusion

When it comes to DDoS protection, even the highest-end DDoS mitigation systems fail. DDoS mitigation appliances come with standard settings that work generally across environments. The operative word here is *generally*. While a financial institution is a financial institution, you have varying types and sizes of financial institutions, e.g. large multinational bank vs. a smaller stock exchange. Each one will vary significantly based on IT infrastructure and services – even the technologies among branches of the same institution can be different.

Once a mitigation solution is chosen, it needs to be tested *in production* to find out what standard settings are appropriate (and not appropriate) for the individual environment.

An important caveat: DDoS attacks are a constant threat – you need to consider how quickly can you get your chosen solution up and running effectively. You also need to consider, how you will maintain such a system.

About RADAR™

Working with any mitigation solution installed, RADAR™ offers superior DDoS coverage and automated DDoS protection. RADAR™ simulates over 100 attack vectors with all public facing IPs 24/7, giving real time visibility to all DDoS vulnerabilities with zero downtime.

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.

