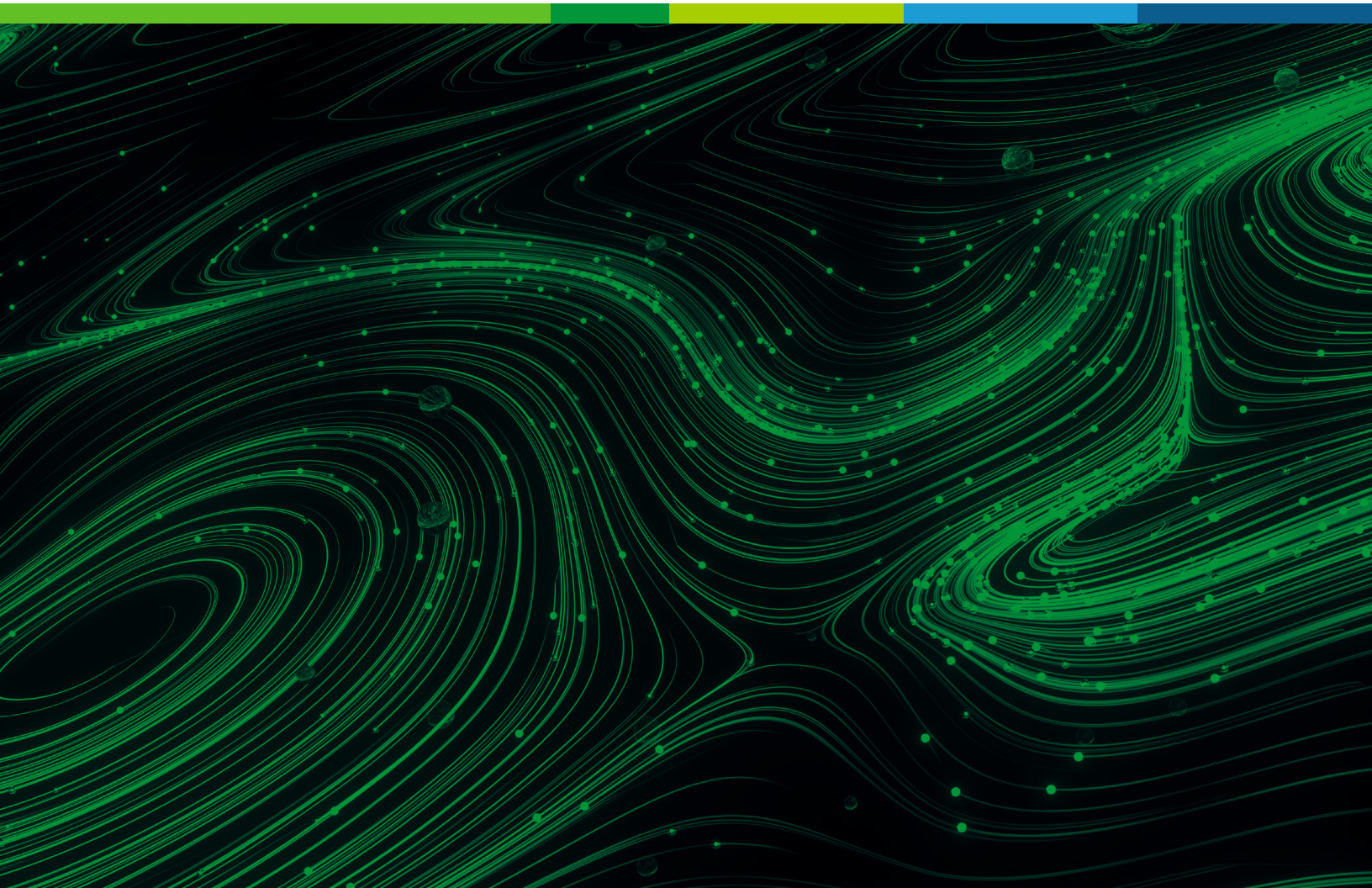
NGINX
Part of F5

WHITEPAPER

Securing Modern Apps Against Layer 7 DoS Attacks

By the security experts at F5 NGINX



Introduction

Application development and delivery are changing rapidly in the face of digital transformation. And the global COVID-19 pandemic is quickening the pace of change – accelerating it by months if not years – affecting the way we live, work, and do business.

But the impetus driving transformation initiatives remains unchanged: **Speed is key if you want to survive (and thrive) in the future.**

Modern organizations inevitably focus on improving development speed as they seek to improve how quickly they can adapt to disruption and other unforeseen challenges. More agile development delivers many benefits: faster time to market, optimal performance that drives better customer experiences, and quicker problem resolutions that reduce operational costs.

MALICIOUS ATTACKS ON DIGITAL ASSETS ARE BECOMING COMMONPLACE

According to F5's State of Application Strategy 2021 report, the number of organizations modernizing applications increased by 133% in the last year alone. Unfortunately, the increasing importance of modern apps and APIs at the core of many organizations also makes them attractive targets for bad actors. Malicious attacks on digital assets are becoming commonplace and securing modern applications is a monumental task.

So, are security teams keeping up? At most companies, the answer is no.

The Quest for Speed Puts More Pressure on Security

Organizations are working overtime to transform their technology stacks. They are moving to the cloud to provision and scale infrastructure on demand and deploy resources globally. They are adopting microservices and containers to give developers more freedom and autonomy to build faster. They are embracing DevOps practices and implementing continuous integration and continuous deployment (CI/CD) pipelines to keep users engaged by releasing more features faster.

Unfortunately, the same environments and technologies that help organizations entice customers also introduce new vulnerabilities and opportunities for exploitation. Online criminals are wasting no time exploiting them, either – organizations suffered 218 security incidents per day in 2020 alone, and cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025.

As companies adopt new modern technologies and migrate to the cloud, they become prime attack targets for cybercrime – especially if their security policies lack consistency and effectiveness.

With security teams stretched thin, cybercriminals are upping the ante and becoming more sophisticated in the ways they abuse applications for financial gain. To avoid becoming prime attack targets for cybercrime, organizations need consistent, effective security policies and tools.

Consider the following scenario:

Emma enjoys shopping for furniture on her favorite e-commerce website – your website. One day, Emma notices your website is loading very slowly and pages are unresponsive. Over the next week, every time she visits your website to shop or search for products, it's sluggish. Emma becomes frustrated and eventually decides to stop coming back. Instead, she goes to your competitor to make her purchase.

Beneath the surface, a likely cause of Emma's poor user experience is a denial-of-service (DoS) attack. In a typical DoS attack, a bad actor floods a website or application with so much traffic that the servers become overwhelmed by all the requests, causing them to stall or even crash.

DoS attacks are designed to slow or completely disable machines or networks, making them inaccessible to the people who need them. Until the attack is mitigated, services that depend on the machine or network – such as e-commerce sites, email, online accounts, and others – are unusable.

DoS ATTACKS NEGATIVELY AFFECT USER EXPERIENCE AND THEY ARE ON THE RISE

DoS attacks negatively affect user experience and they are on the rise:

- DoS attacks are among the most popular in part because of the proliferation of APIs.
- Layer 7 attacks have increased by 20% in recent years, and the scale and severity of their impact has risen by nearly 200%.
- The digital shift prompted by COVID-19 was accompanied by a surge in distributed DoS (DDoS) attacks to over 10 million attacks in 2020.

But a DoS attack isn't the same as a compromised system where an active attacker is stealing gigabytes of sensitive company and customer information, right? Not exactly, but the impacts of DoS attacks might surprise you.

What's So Bad About DoS Attacks?

The most obvious problem caused by DoS attacks is that they make it difficult for companies to do business, bogging down all the processes that may rely on the use of the network. With the targeted web application or website slowed by fake traffic, normal workflows cease until the attack subsides – and this is where the real risk lies. A single negative experience can be all it takes for a customer to abandon your brand forever.

As we saw with Emma's experience, DoS attacks can severely affect the customer experience of a website or application. Imagine that poor performance being experienced by tens, hundreds, thousands, or even millions of users. Whether the attack comes from a competing business, hacker, or any other source, website availability has a material impact on business operations and carries other non-financial costs, such as decreased customer satisfaction and reputational damage to brand.

THE AVERAGE COST OF DOWNTIME PER MINUTE IS $5,600

It's hard to pin down the exact costs of these attacks as the impact varies greatly depending on the size of the company, what's targeted, how long the attack lasts, and the long-term indirect consequences. In 2014, Gartner estimated that the average cost of downtime per minute is $5,600, which translates to around $336,000 per hour. A 2017 survey from Kaspersky found the average cost of a DDoS attack ranged from $120,000 for small to medium-sized businesses, up to over $2 million for large enterprises.

When you consider that DoS attacks are becoming more sophisticated and pervasive, the average cost is doubtless much higher in 2021. And these amounts are just the direct costs, not accounting for the indirect losses caused by a website or application outage.

What Do Modern DoS Attacks Look Like?

DoS attacks have been around for decades. Typically, they take place over various layers of the Open Systems Interconnection (OSI) model.

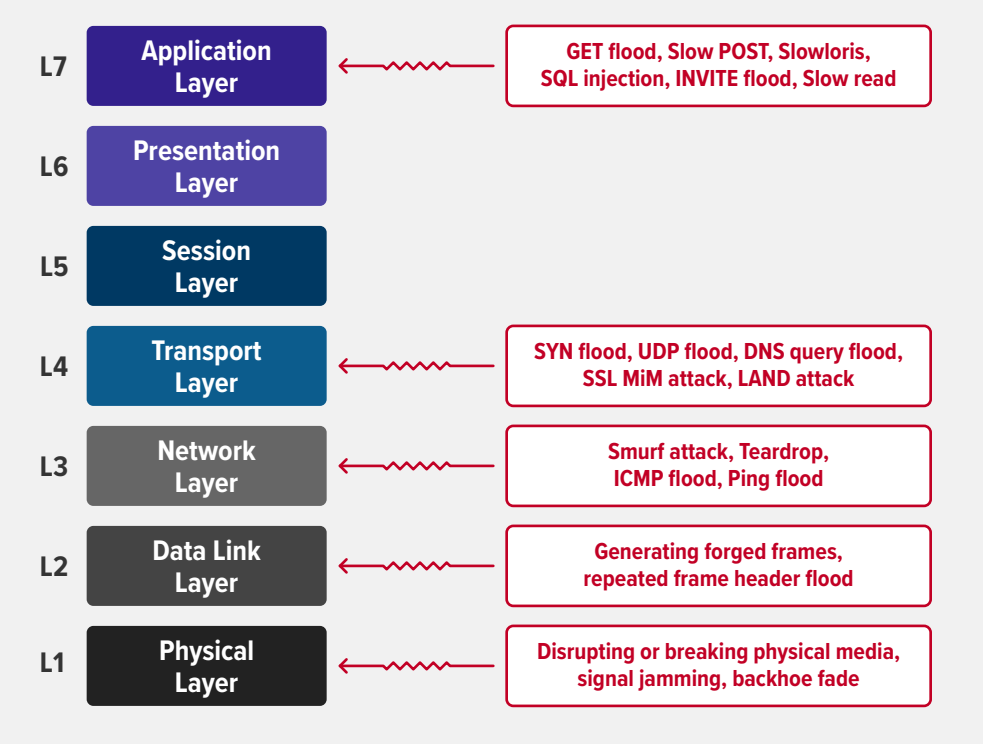


Figure 1: The OSI model

Traditional DoS attacks primarily employ traffic-flooding techniques that overwhelm the server with connection requests at the network and transport layers (Layers 3 and 4). However, these so-called *volumetric attacks* – UDP reflection, and ICMP and SYN flooding, among others – are not as prevalent as they used to be.

Bad actors have also moved away from using a single machine to flood a server. Now, they can launch distributed DoS (DDoS) attacks, yoking together thousands of devices and machines into a botnet that sends requests. With DDoS attacks, not only is the possible number of requests greater, but the distributed nature of the attack makes it that much more difficult to figure out the source of the requests and block them.

Increasingly, DoS attacks are using HTTP/HTTPS requests or API calls to attack at the application layer (Layer 7), in large part because Layer 7 attacks can bypass traditional defenses that are not designed to defend modern application architectures.

Why the switch from volumetric attacks to Layer 7 attacks? Attackers are following the path of least resistance. Infrastructure engineers have spent years building effective defense mechanisms against Layer 3 and Layer 4 attacks, making them easier to block and less likely to be successful. That makes such attacks more expensive to launch, in terms of both money and time, and so attackers have moved on.

LAYER 7 DoS ATTACKS ARE RELATIVELY CHEAP TO LAUNCH, EVEN FOR LOW-SKILLED CYBERCRIMINALS

By comparison, Layer 7 DoS attacks are relatively cheap to launch, even for low-skilled cybercriminals. According to Digital Shadows, DDoS-for-hire services charge an average of just $7 to disrupt any target the buyer chooses.

One of the reasons attacks are getting cheaper and easier is the proliferation of smart devices. Omdia estimates that the number of Internet of Things (IoT) devices will reach nearly 28 billion by the end of 2021. Unfortunately, security controls are often (and notoriously) overlooked on IoT devices, meaning it's easy for hackers to take control of them and exploit them in botnets, often without the owners of the devices even knowing.

New sophisticated DoS attack types include:

- **`GET` and `POST` flood attacks (HTTP/HTTPS)** – The attacker tries to overwhelm the server or API with large numbers of requests, rendering it unable to respond to real users.
- **"Slow" attacks (HTTP/HTTPS)** – "Slow-and-low" attacks tie up server resources, taking them away from actual users. There are three main types of slow attacks:
  - **Slowloris** – The attacker connects to the server and sends partial request headers at a slow pace. The server keeps the connection open while waiting for the remainder of the headers, exhausting the pool of connections available to actual users.

  - **Slow read** – The attacker sends a well-formed HTTP request, but then reads the response at a sluggish speed, if at all. This has the cumulative effect of consuming server resources, thus preventing legitimate requests from going through.
  - **Slow POST** – The attacker sends legitimate HTTP POST headers to the server, complete with correct specification of the size of the message body that will follow. It then sends the message body very slowly. Because the message seems valid, the server keeps the connection open waiting for the complete body to arrive. A large number of slow POST attacks exhausts the pool of connections available for actual users.

- **Distributed variations of the preceding attacks** – Obviously, enlisting multiple computers makes it easy to send a larger number of simultaneous requests. Further, the traffic volume from each computer can be relatively low, making it resemble a regular user. Computers can also drop out of the attack pool and then rejoin, putting the set of source IP addresses in constant flux. These traffic characteristics make traditional mitigation techniques like rate limiting, IP address denylisting, and geo-blocking less effective.
- **Challenge Collapsar attack/random URIs** – In a Challenge Collapsar (CC) attack, the attacker sends frequent requests that are normal except that the requested URIs require execution of complicated, and thus time-consuming, algorithms or database operations, which can exhaust resources on the targeted server. The attacker can also randomize URIs and other HTTPs parameters in a way that defeats legacy mitigation tools like static rules.
- **Hiding behind NAT** – The attacker uses encryption or network address translation (NAT) to evade detection. Trying to detect attacks by tracking only the source IP address is ineffective because it treats all NAT users as attackers even if only one user is attacking.
- **Targeted SSL/TLS attacks** – The attacker abuses the SSL/TLS handshake protocol. One popular approach is to send garbage data to the target SSL/TLS server. It's just as computationally expensive to process an invalid message as a legitimate one, but without a useful result. Most firewalls don't help in this case because they can't effectively distinguish between valid and invalid SSL/TLS handshake packets and implementing decryption on a firewall is cost-prohibitive.

THE EXPLOITATION OF EXISTING AND NEW TECHNOLOGIES AT SCALE HAS BECOME TOO EASY FOR ATTACKERS

The exploitation of existing and new technologies at scale has become too easy for attackers. With bad bot traffic stealthily hiding among legitimate customer traffic, Layer 7 attacks create a new challenge.

These developments also make Layer 7 DDoS attacks much more difficult to detect because bots and automation allow attackers to disguise themselves as legitimate traffic, especially when they're using sophisticated security penetration tools.

Why Your Traditional DoS Protection Can't Stop Layer 7 Attacks

You may be thinking, "But I already have a security solution in place to help me detect DoS attacks. Why won't that work?"

LAYER 7 DoS ATTACKS LOOK LIKE LEGITIMATE TRAFFIC, AND TRADITIONAL WAF DEFENSES CAN'T EFFECTIVELY DETECT THEM

Traditional DoS mitigation includes limiting the number of requests accepted from a given source IP address during a certain time. Since requests that are part of a Layer 7 DoS attack may be under this limit and look like legitimate traffic, traditional web application firewall (WAF) defenses can't effectively detect them. Moreover, attackers continue to leverage new technology like machine learning and AI to make DoS attacks more sophisticated and evasive.

Other reasons why traditional DoS protection falls short include:

- **Security teams can't keep up with the constant maintenance and dedicated analysis**
  Static rule-based security requires continuous maintenance of thresholds to keep up with changes and updates in the modern app landscape. Missing an update can lead to a false positive that blocks legitimate traffic to your website or application. Also, when most attacks target the application, you need regular insight into the application's behavior to establish baselines that determine whether or not traffic is malicious. This stretches the limits of already overburdened security teams struggling with the demands and complexity of modern app development.
- **Traditional DoS protection can't stop unknown unknowns**
  No matter how robust your security is or how thorough your security team is, there will always be new attack types and techniques. Cybercriminals are constantly increasing the frequency, size, and sophistication of attacks, so what you successfully blocked today might look totally different tomorrow. Unlike other attack vectors, DoS attacks don't typically occur because of a vulnerability or insecure coding. DoS mitigation is reactive by nature: teams must first detect attacks and then successfully identify the source to block them. Traditional DoS protection solutions rely too heavily on blocking vectors they recognize and know, making them less effective against new zero-day attacks.
- **Long delays from attack reporting to attack blocking**
  Mitigating an attack can be a complex and lengthy process. Detection and response teams are typically alerted to suspicious behavior, which must be analyzed and assessed. Once you recognize that you are under attack, you must monitor it manually to understand the pattern, and develop a method for successfully blocking it. This can take anywhere from a few hours to several days. Meanwhile your website or application might be down and unavailable for your customers.

With the increasing scale and sophistication of DoS and DDoS attacks, only organizations with defenses made for modern landscapes can defend against attacks that evade traditional network and web defenses.

Modern Problems Require Modern Protection

So, what is the ideal solution for stopping Layer 7 attacks?

On a basic level, you need tools that recognize when your website or application is under attack because they're able to distinguish between the "good guys" (legitimate traffic) and the "bad guys" (malicious traffic). As we mentioned above, malicious application-level requests often look the same as legitimate ones. Even worse, HTTP attacks at Layer 7 can be damaging at a much lower rate and volume of requests than at Layers 3 and 4.

To be effective, Layer 7 DoS protection must satisfy a completely new set of requirements and be able to:

- Distinguish attacks from regular traffic patterns
- Evaluate server health under load
- Determine when an attack started and whether it's over
- Mitigate attacks without affecting legitimate users
- Determine whether changes in app behavior are due to attack or updates to app functionality
- Survive a prolonged attack without loss of detection efficacy

A NEW APPROACH IS NEEDED, ONE THAT IS AS ADAPTIVE AND DYNAMIC AS THE MODERN ENVIRONMENTS IT PROTECTS

On top of that, solutions must be able to do this in both traditional, "monolithic" environments and modern, distributed app architectures employing microservices and Kubernetes. A new approach is needed, one that is as adaptive and dynamic as the modern environments it protects. Today's attackers are constantly changing their strategies, so attack-prevention mechanisms must be able to observe changing user and service behavior and adapt continuously in response.

Teams need adaptable and powerful protection with the following key features:

- **Seamless integration**
  Enabling strong security controls that integrate seamlessly into modern infrastructure architectures is key. Security teams need a solution that reduces complexity by consolidating the set of tools needed to safely deliver modern apps from code to customer across clouds and architectures.
- **High performance**
  A solution's performance impact on customer experience and the application itself must be minimal, both under normal conditions and during an attack. Customers don't care if you're under attack; they care about their own experience. So, users must be able to access the application without hindrance or adverse performance, even while your teams are actively fighting an attack. Continuous monitoring and real-time signatures with zero-day attack protection ensure both optimum application performance and effective attack mitigation.

- **Agile security**
  To operate effectively at the breakneck pace of today's digital world, a solution needs to be integrated into continuous integration and continuous development (CI/CD) pipelines. Automatically baselining and entering mitigation mode once new code is deployed reduces operational inefficiencies that cause friction between security and development teams. A modern solution needs to enable "security as code" integration with DevOps tools so protection becomes automatic without slowing down app innovation.
- **Attack prevention**
  Cyber attackers may adjust their tactics. To combat this, a dynamic solution with embedded tools for learning from user and service behavior is needed. Layer 7 security must react to attackers before any significant damage is incurred, without immediate human intervention. This means mitigation deploys automatically in response to detected behavior anomalies, and is then measured for effectiveness. An unsupervised capability creates an automated feedback loop with multilayer defense, enabling security remediations to move at the same speed as app evolution.
- **Reduced-cost speed**
  Traditional security solutions can slow down DevOps workflows. CI/CD takes the deployment burden off developers so they can focus on delivering features, fast. It also gives emerging DevSecOps teams a way to integrate security into automated app delivery. With this streamlined workflow, no-touch configuration enables cost-effective protection at scale for distributed app and API environments like microservices and removes friction between DevOps and SecOps teams.

With all of the above in mind, we built NGINX App Protect Denial of Service to deliver protection built to endure every digital shift, so your website stays accessible, fast, and safe.

NGINX App Protect DoS Adapts to Stop Attacks Automatically

NGINX App Protect DoS is a new lightweight dynamic module for NGINX Plus, built on F5's market-leading WAF and behavioral protection. Designed to defend against even the most sophisticated application-layer DoS attacks, NGINX App Protect DoS uses adaptive technology to construct and deploy dynamic signatures and mitigate attacks automatically.

NGINX APP PROTECT DoS USES UNIQUE ALGORITHMS TO CREATE A DYNAMIC STATISTICAL MODEL THAT PROVIDES THE MOST ACCURATE POSSIBLE PROTECTIONS

NGINX App Protect DoS uses unique algorithms to create a dynamic statistical model that provides the most accurate possible protections. It continuously measures mitigation effectiveness and adapts to changing behavior or health conditions. These features enable NGINX App Protect DoS to block DoS attacks where each attacking request looks completely legal, and a single attacker might even generate less traffic than the average legitimate user.

NGINX App Protect DoS uses a multistep process to detect and mitigate Layer 7 DoS attacks.

STEP 1

Capturing Typical Behavior in a Statistical Site Model

The first step is to create a statistical site model which captures a baseline of typical behavior when your website is not under attack. NGINX App Protect DoS tracks 320 user and app metrics for a comprehensive view of your app deployment, dynamically updating the model as it observes traffic. This frees you from the need to adjust system thresholds manually, while also guaranteeing that NGINX App Protect DoS takes into account the changes in traffic patterns that inevitably occur over time.

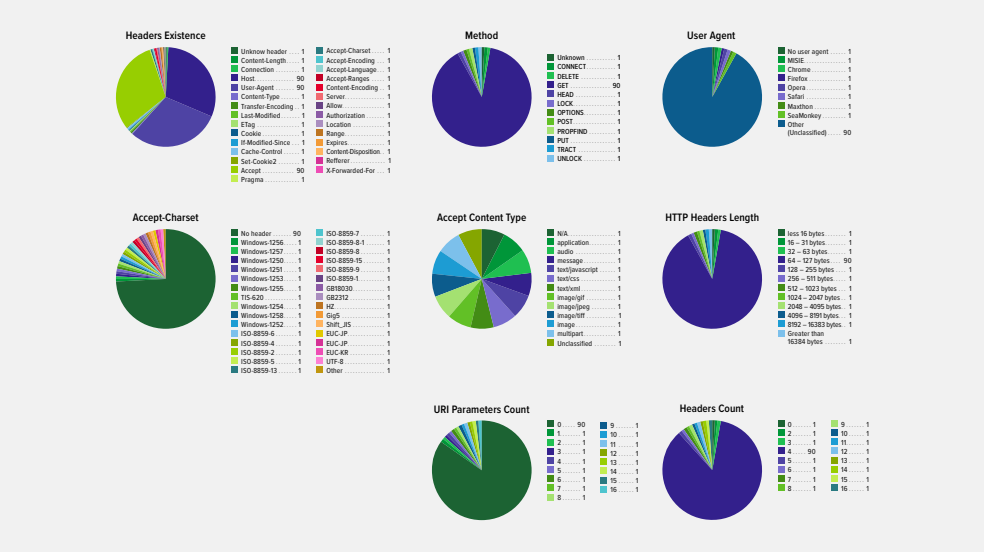


Figure 2: Metrics for tracking HTTP request characteristics

STEP 2

Checking Service Health

MANY LAYER 7 DoS MITIGATION TOOLS ONLY FOCUS ON CLIENT TRAFFIC PATTERNS

Many Layer 7 DoS mitigation tools only focus on client traffic patterns. For superior attack detection, you can configure NGINX App Protect DoS to actively check service health as well. It tracks multiple server performance metrics, such as response time and the proportion of dropped requests. Worsened values for any metric indicate server stress that might be caused by an attack. Once NGINX App Protect DoS determines an attack is in progress, tracking server metrics and response patterns to health checks can also help shed light on when the attack started.

STEP 3

Identifying Malicious Actors and Request Patterns

NGINX App Protect DoS then kicks off two procedures that run in parallel:

- **Analyzing the behavior of individual users to detect who created or contributed to the anomaly**
  NGINX App Protect DoS initially treats all users as suspects and analyzes their behavior. It's unlikely that every user is an attacker but measuring the behavior of all of them enables NGINX App Protect DoS to create a statistical picture that reveals who did and did not contribute to the attack. Detected bad actors are identified by their IP address or the `X-Forwarded-For` header in their requests.
- **Generating a list of rules to describe attack traffic without blocking legitimate users**
  NGINX App Protect DoS generates real-time signatures for zero-day attack protection, which can be reused. Attack signatures are rules or patterns that identify attacks. In the same way a personal signature can identify a person, attack signatures identify bad traffic and block an attack attempt.

This generated attack signature identifies HTTP attributes associated with an attack:

```
http.request.method eq GET and http.user_agent contains Chrome and
http.uri_parameters eq 6 and http.accept_header_exists eq false and
http.headers_count eq 7
```

STEP 4

Mitigating the Attack with a Multilayer Defense

The primary goal when defending against a Layer 7 attack is to catch it before it can do any damage. As shown in the following diagram, you can configure either a conservative or standard mitigation strategy:

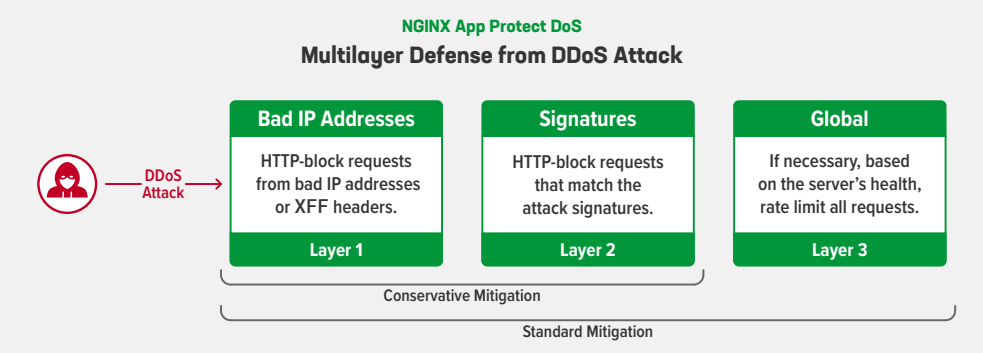


Figure 3: The conservative and standard mitigation strategies in NGINX App Protect DoS

With both strategies, the first layer of defense is to block requests from the malicious actors who were identified by IP address and `X-Forwarded-For` header. The next layer of defense blocks requests that match the signatures generated in the previous step.

Finally, if you've configured standard mitigation, and NGINX App Protect DoS finds the first two layers of defense are insufficient, it applies global rate limiting for a short period.

STEP 5

Minimizing False Positives During Attack Mitigation

Global rate limiting always carries the risk that legitimate users get blocked due to false positives. To reduce false positives, instead of imposing a global rate limit, NGINX App Protect DoS "challenges" requesters with a response that web browsers can properly handle but a script run by a botnet controller (that is, malware on infected computers) typically cannot. Specifically, it returns an HTTP redirect and a snippet of JavaScript code for processing. If the requester cannot respond correctly, NGINX App Protect DoS concludes it is not legitimate and blocks subsequent requests.

We understand that some users have concerns about relying on adaptive learning because of the potential for large numbers of false positives. Still, it's the most effective way to mitigate Layer 7 DoS attacks. NGINX combines multiple approaches – analyzing user behavior, checking service health checks, and measuring the effectiveness of mitigation tactics – to reduce the chance of false positives.

Is Layer 7 DoS Protection Needed When My WAF Already Protects Against Bots?

While Layer 7 DDoS attacks usually employ bots, their purpose differs from other bot activity. Bots typically try to scan for application vulnerabilities or use previously compromised data in credential stuffing attacks, whereas service disruption is the main goal of Layer 7 DoS and DDoS attacks.

In addition, standard anti-bot tools focus on distinguishing "good bots" from "bad bots" using human supervision to minimize false positives. NGINX App Protect DoS focuses on distinguishing attackers from legitimate users based on behavior, regardless of the attack mechanism. As a result, it generates fewer false positives than standard anti-bot protection.

Four Real-World Scenarios Where NGINX App Protect DoS Saves the Day

Now that you understand how NGINX App Protect DoS works, let's take a look at the concrete advantages it brings to security teams on a daily basis.

Scenario 1: Detecting Low-Volume Attacks on Apps Deployed in the Cloud

Example: E-commerce application running on Amazon Web Services
Problem: Slow HTTP attack from a single machine consumes all concurrent connections

A slow-rate attack uses a tool like Slowloris in an attempt to exhaust the pool of available concurrent connections so that real users can't establish connections. If, for example, a server at an e-commerce website can handle a maximum of 200 concurrent connections, the attacker sends 200 partial HTTP request headers to the server one at a time. Each time a connection to a legitimate customer is closed, Slowloris establishes a new connection and sends a partial HTTP request header. The server waits patiently for the rest of the data to show up so it can process the request and close the connection, but the data never comes and the connection remains open.

Once 200 connections are consumed, legitimate users can't establish a connection until the server times out and even then Slowloris simply sends another connection request. If undetected and unmitigated, Slowloris attacks can last a long time. Many tools, such as Amazon's managed DDoS protection service, AWS Shield, can't mitigate these attacks because they don't recognize the low volume of traffic as an attack.

The result? Real customers experience extremely slow page load times or are unable to load a page at all.

The NGINX difference:
NGINX App Protect DoS can discover attacks and block them before users – or even your security team – notice anything is wrong. When traffic patterns are normal, NGINX App Protect DoS establishes a baseline of application behavior. It constantly monitors service health and automatically switches into mitigation mode as soon as it detects any degradation in performance or service health.

Scenario 2: Automatically Suppressing an Internal DoS on a Microservices Application

Example: Newly transitioned shopping cart microservice
Problem: Request loop from an automation script bug causes self-inflicted volumetric attack

When talking about DoS and DDoS attacks, we typically focus on bots and hackers trying to take applications offline. But for many organizations, the self-inflicted DoS attack is far more common.

Microservices architectures allow DevOps teams to develop pieces of independent functionality in parallel, embrace a common toolset, and streamline processes. Further, many teams introduce automation tools to monitor and analyze key elements of a microservice by collecting usage data and generating data points.

Imagine a developer writes an automation script to periodically monitor the performance of a newly introduced customer shopping cart microservice. Accidentally, the developer has the script ping the microservice for performance status continuously on a loop, instead of every 60 seconds. This generates significantly higher traffic than planned and the shopping cart stops working for customers.

While traditional DoS protection probably detects this type of problem eventually, it still takes time to identify and resolve it – valuable minutes, hours, or even days where the shopping cart microservice isn't working and shoppers can't make a purchase.

The NGINX difference:
NGINX App Protect DoS detects that a microservice has stopped responding and begins defending. It identifies the specific tool causing the loop and blocks the traffic coming from the script so that the shopping cart remains available to real customers. While this approach prevents the automated tool from gathering information, it guarantees that the user experience is protected at all times.

Scenario 3: Rate Limiting Caused by Out-of-Date Thresholds on a Website

Example: Online news website
Problem: Rate-limiting thresholds are never updated to reflect changing traffic patterns

Modern infrastructures are moving faster than ever, and changes need to be applied rapidly. Traditional DoS protection involves estimating and manually imposing thresholds to trigger mitigation. As a website evolves and attracts more traffic, those thresholds need to be regularly updated.

Let's say a site administrator who's launching an online news website configures thresholds for concurrent connections and requests per second. Over the next month, the website gains popularity, and then a particular headline goes viral, driving huge amounts of new traffic as more people share the story and readers head to the news site.

Unfortunately, even if the thresholds have been adjusted as traffic increased over the past month, the sudden traffic spike exceeds them. The traditional DoS protection tool goes into gear, imposing rate limits and triggering false positives that block real readers from reaching the website.

The NGINX difference:
NGINX App Protect DoS offers zero-touch configuration. Since it is constantly learning and dynamically updating the baselines for service behavior, you don't have to manually maintain thresholds.

Scenario 4: Responding Quickly to Changing Attack Patterns

Example: Online shoe store

Problem: Sneaker bot adjusts traffic pattern, circumventing blocks set by site administrator

Attackers are hard to outsmart. Cybercriminals are launching new attack vectors faster than security teams can configure new HTTP attack signatures or update lists of known bad IP addresses.

Online shoe stores and other e-commerce sites, for instance, are locked in a battle of wits with sneaker bots – automated bots that everyone from collectors, resellers, and more nefarious actors use to scoop up limited-edition inventory. Sneaker bots aren't limited to footwear. They can be used for everything from consumer electronics, hotel rooms, and other high-demand items like hand sanitizer and vaccines.

Even when a site administrator configures recognized malicious subnets and HTTP signatures with expected attack patterns, perpetrators can adjust the pattern and relaunch. In the face of advanced technologies and a thriving bot ecosystem, site administrators have no chance of keeping up if they depend on manual prevention methods.

NGINX APP PROTECT DoS AUTOMATICALLY GENERATES ATTACK SIGNATURES AND DETECTS BAD ACTORS BASED ON BEHAVIOR ANOMALIES – WITHOUT HUMAN SUPERVISION

The NGINX difference:
NGINX App Protect DoS automatically generates attack signatures and detects bad actors based on behavior anomalies – without human supervision. Instead of painstakingly detecting new attack vectors and updating configurations manually, site administrators can simply configure the resource they need to protect and leave the rest to NGINX App Protect DoS's adaptive technology.

Conclusion

For effective Layer 7 DoS protection, organizations must leverage flexible and adaptive products built for modern, ever-changing landscapes. Security professionals and developers alike need dynamic solutions that offer robust protection without slowing down release velocity.

NGINX App Protect DoS enables security, development, and DevOps teams to:

- **Combat a new generation of DoS attacks**
  Secure your modern, distributed apps and APIs against hard-to-detect Layer 7 DoS attacks through automated user and site behavior analysis, proactive health checks, and no-touch configuration.
- **Reduce complexity while securing apps**
  NGINX App Protect DoS can be deployed anywhere NGINX Plus is deployed, delivering consistent security and control everywhere you need them – apps, APIs, and operating environments. At the same time, seamless integration with NGINX minimizes costs, reduces latency, and accelerates performance.

- **Deliver security as agile as your apps**
  NGINX App Protect DoS helps align security and development teams by automating protection through a continuous feedback loop. It also facilitates “security as code” integration with DevOps tools with a lightweight software package that makes it easy and fast to deploy.

NGINX App Protect DoS provides the comprehensive and coherent defenses that can withstand today’s threat vectors – and the ones still to come.

Learn more at www.nginx.com/products/nginx-app-protect/denial-of-service/

NGINX
Part of F5