INDUSFACE™

WHITEPAPER

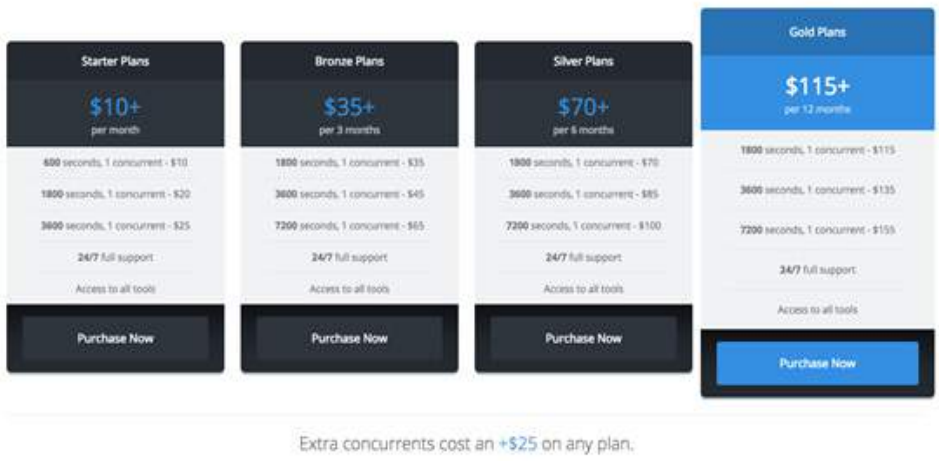
Comprehensive Un-Metered Managed Application **DDOS Protection**

One of the biggest challenges of moving business digital is it exposes business to new threat around security and availability. The new post-pandemic world is going to be lot different from what it was when it went into pandemic. Many organizations have adapted to the new need and have moved critical applications over internet which they were resisting in past. Digitalization of organizations is on steroids, but this also opens new challenges on the cyber security front. With these applications available from anywhere it is also available to hackers readily. One of the biggest challenges that organizations face is how they are going to ensure availability of critical applications and key piece to address this is the DDOS mitigation plan that organizations have in place.

Denial of service (DOS) attacks are attack made on applications to make it unavailable. These attacks are done by sending requests at high volume to the servers serving the application exhausting the resources available and ensuring the legitimate requests do not get any share of resources rendering the application inaccessible. Difference between DOS and DDOS (Distributed denial of service) is based on how attack is launched, if distributed nodes are used to launch DDOS attacks whereas DOS attacks are launched using single resource.

With the advent of IOT, DDOS attacks are becoming more prominent and are becoming more sophisticated, hard to predict and ever evolving. These attacks are done for varying reasons ranging from cyberbullying, extortion tactics to some form protest. Within days after DreamHost rejected request from Department of Justice to diverge visitor data for an anti-Trump website, the company has reported DDOS attacks. At times DDOS attacks are also state sponsored with widespread allegation of such DDOS attacks being done from China & Russia.

Whatever may the reason behind the DDOS attacks, the reality is with the cost of launching DDOS attacks coming down, these attacks are here to stay and almost anyone can become victim of DDOS attacks. Nowdays, DDOS attacks are available as an service, which can be ordered online. When you dig deeper and look at the DDOS services available, you will feel like you are ordering for some legitimate SaaS service with various plans ranging from free to premium service.



These attacks can be launched without actually having any direct contact of attackers and payment can be made using cryptocurrencies like Bitcoin. There are even review sites available for the same.

Such services are dime a dozen and buyers of these services completely understand the efficacy of such attacks. A cost to launch a 5 minutes attack is less than $5 but 5 minutes loss of service could be multi-fold for large organizations. We can only guess how many customers an online store loses if an attack lasts the whole day. For example, amazons loss for 40 minutes downtime was estimated to be around $4.8 million dollars. Bottom line is DDOS attacks are are very cheap, easy to organise and without proper defence pretty effective. Every organizations should look at ways to protect against DDOS attacks.

Type of DDOS Attacks

There are different kinds of DDOS attacks that can be launched to bring down the application. Two major classification of DDOS attacks are Network layer attack and Application layer attacks.

Network Layer Attack:

Network layer attacks are DDOS attacks that are done on Layer 3 and Layer 4 of OSI Model. Mostly in this layer the attacks are done by exploiting weakness of protocols in this layer. Some of the well-known network layer ddos attacks are

Reflection and Amplification Attacks:

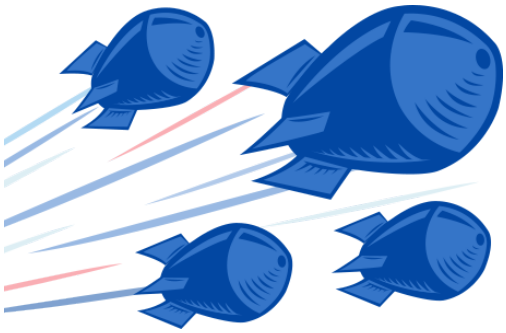
These attacks exploit the inherent connection less nature of protocol like UDP and trick servers to bombard victim with large requests. In such attacks the attacker sends request to servers masquerading with victims IP. The server not knowing that it is a request from an attacker ends up sending response to victims' server bombarding the victim server with unwanted requests rendering it unavailable to legitimate requests. Attackers like such attacks as they have to send relatively small requests to server which would in turn attack the victim server. The resources spend by attackers are very less in such attacks. Attacker generally exploit unattended/orphaned servers which is exposed over internet and weaponize them, most common of these exploits are exposed Memcached server because of the huge amplification potential that these servers possess.

ACK Attacks:

Ack Attacks are DDOS attacks where attacker floods the victim server with lot of ACK packets. ACK is part of the 3 way handshake that happens as part of TCP protocol. During TCP handshake the connecting machine sends a SYN packet to the target machine which in turn sends SYN/ACK message to which the connecting machine sends back ACK (Acknowledgement) packet to complete handshake and establish connection. ACK packets are also sent to tell if packets are received in order. Since ACK packets are a flag set in packets , it can be sent as part of other messages. In case of attack attacker sends large number of ACK packets to victim server, since the server cannot differentiated between legitimate ACK packet vs attack packets, it will end up processing all requests resulting it getting overloaded and running out of resources

Flood Attacks:

SYN Flood attack is one type of DDOS attack where attacker sends multiple sync requests to all ports open on the server. As server wont know that it is an attack processes the SYNC request and opens connection and sends back SYN/ACK. The attacker now ignores the SYN/ACK or delays the ACK packet. The server keeps waiting for the ACK packet until it times out keeping the connection open, the attaker may send a SYN packet just before the request times out, ensuring there are lot of connections kept open in the server making the server open new connection for legitimate requests



Application Layer Attack:

Application layer DDOS attacks are more tricker, these are attacks done on Layer 6/7 and looks pretty much like legitimate attacks making it harder to detect or prevent. Some of the common Layer 7 DDOS attacks are Reflection and Amplification Attacks:

SlowLoris:

Slowloris are a special type of attack, where partial http requests are send to server , as the name suggests these attacks are methodical and slow in nature. Attacker sends partial but legitimate requests to the server. The server inturn opens up connection and keep it open waiting for rest of the request which never comes. Even when the connection times out another partial request is sent opening up new connections until server is overwhelmed and unable to handle any new requests.

Slow Read Attack:

In this type of attack, attacker sends a request to server for large response and then reads slowly sometimes one byte at a time. This means the server keeps the connection open as it is never idle but the read is so slow that it takes a long time to close the connection. If multiple such requests are done and connection left open, server soon runs out of connection pool and strats dropping legitimate requests.

Slow Post Attack:

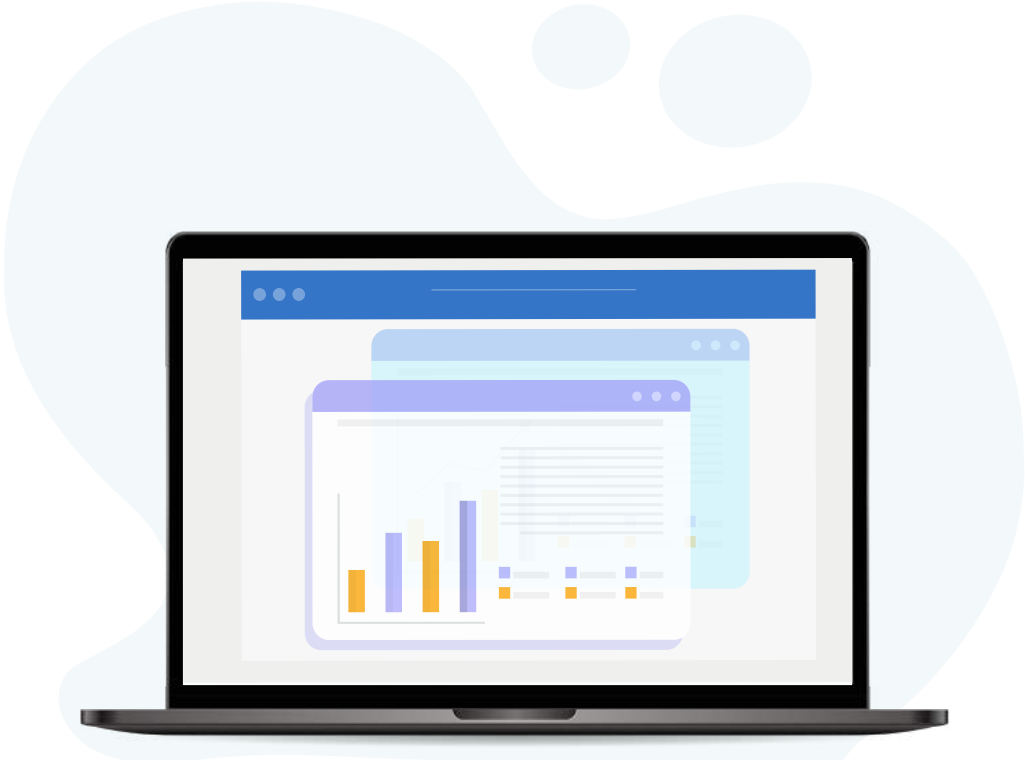
This is similar to Slow read attack but in this case , attacker says to server that there is POST request of x length but then sends the request at very slow rate as slow as 1 byte in a minute, this again means the resources on the server are rapidly consumed making the server unavailable for legitimate request.

HTTP Flood Attacks:

These attacks as the name suggests are flood of GET/POST requests send to server overwhelming the server. In case of GET it might be requests from multiple IPs for a large image , video file etc. In case of POST attacks multiple post requests are made with large payload which makes the server to process and generally send the POST request to persistence layer like database, consuming lot of resources eventually making the server unresponsive. These attacks are sometimes made with only few requests from each IP easily bypassing the rate limiting rules making detection and protection of such attacks complex.

Large Payload Attacks:

Large Payload Post DDoS attacks occur when web services use a DOM parser to create an in-memory representation of the SOAP message. During this process, the SOAP message size can double, or in some cases, grow as much as 30 times larger. The resulting large documents result in memory exhaustion. Variations of this attack can include over-sized content contained in the header of the SOAP message, in the SOAP body, or in SOAP envelope but outside of the SOAP header and the SOAP body.



AppTrana – Comprehensive DDOS Protection

DDOS protection is complex, as explained it is of varying nature and very potent . AppTrana is the only solution in the market that provides a completely managed un-metered DDOS protection for Applications. It provides complete protection against all types of DDOS vectors protecting the application end to end.

Under the Hood:

AppTrana's DDOS protection starts immediately once a site in onboarded behind AppTrana. It is inbuilt and enabled from day zero with little configuration from customers end. Once customer makes DNS change, all the traffic to the application is passed through AppTrana infrastructure and DDOS protection starts immediately.

Built for Scale:

First step of any DDOS protection is ability to observe large volume of requests. No matter how good the defense are these defenses won't work if the solution is not able to observe huge volume of attacks, for any processing and identifying ddos attacks those requests need to be observer and pattern identified, for this these requests need to be accepted by the solution, making scalability a primary requirement for any DDOS solution. This is one of the major reasons that On-premise solutions are not very effective against DDOS attacks as the limits to which they can scale and observer requests are limited and provisioning huge capacity is very cost prohibitive.

AppTrana is built bottom up for scale on AWS. Leveraging the highly scalable, multi-regional cloud offering of AWS. AppTrana scales seamlessly to huge variance in load without running out of resources. Built with multiple redundancies and aggressive tracking of requests on the infrastructure, AppTrana constantly monitors the load on the infra and based on various lead indicators scales up the resources to meet any demand. AWS infrastructure is known to block large attacks upto 2.3 Tbps and 700k requests per second, which speaks volume about the scalability at its disposable. AppTrana leverages this scale effectively to provide cost effective DDOS protection to its custoemrs.

Multi-Layered Defense:

Key to AppTrana's defense is the multi-layerd architecture, each playing a key role in protecting against various form of DDOS attacks.

Origin Protection:

Once an application is bought under AppTrana protection, AppTrana infrastructure becomes the front face for the application, any hacker trying to resolve and identify the IP of the application will be shown the IP of AppTrana.

So, any attack launched directly on the application will first hit AppTrana infrastructure which monitors the requests and passes only the legitimate request to back end. This does not mean that origin is automatically protected from all attacks, hackers can get hold of origin IP through DNS cache etc and launch attack directly on the origin. To avoid this as part of onboarding AppTrana provides set of IPs that has to be whitelisted on application infra and only requests from these IPs should be accepted blocking all other requests. This is provided as part of our basic protection without any additional cost unlike many other vendors.

Content Delivery Network:

Any traffic to the application first hits the edge network which caches the application. Traffic reaches the edge which is nearest to your visiting users. Traffic hits these edge no matter if you are data is cached or not, such an architecture is built to make the solution resilient to DDOS attacks. The Edge is equipped to accept only well-formed requests which automatically protects against volumetric DOS attacks like TCP flood , ACK attacks etc. As mentioned before any requests to application will now hit Apptrana first, so any network attacks will and can be launched at only the AppTrana infrastructure. Since all edeges are equipped to handle and block these network attacks, any network based DDOS attacks are blocked automatically. Since origin accepts request only from AppTrana IPs , any network based attacks directly on the Origin will be automatically protected providing a comprehensive protection. CDN is also enabled to find the optimized route to Origin through AppTrana's WAF layer effectively accelerating the site performance even if no caching is done as part of onboarding.

Highly Scalable WAF layer:

Traffic through CDN if not cached reaches the WAF layer.

WAF layer is equipped to protect against application layer DDOS attacks. In order to protect against these attacks, it is important the WAF infra scales to observe high load. WAF layer built on AWS monitors load on various parameters and has multiple lead indicators to anticipate increase in load and scales up immediately to observe any amount load. WAF layer also is equipped with various rules like rate limiting rules, IP reputation rules , rules to protect against Slowloris attacks by controlling the minimum rate of bytes transferred etc..

IP reputation checks: By default, AppTrana checks the reputation of the request IPs and blocks anything that is marked malicious in our Database. Our database is constantly updated from various sources including threat intelligence we gather from protection hundreds of sites.

BOT Pretender Policies: These are checks to see if there are any BOTs that is pretending as good bots. For example, there could be a bot which may masquerade as Google bot. AppTrana checks for these bots and block them.

Rate Limiting Rules: AppTrana comes with inbuilt with AppTrana where number of requests that can be made to the application can be controlled. These can be quickly changed from AppTrana portal and propagation happens within seconds.

Anomaly Detection Layer.:

All DDOS attacks cannot be automatically blocked by default rate limit rules or controlling timeout/byte transfer rates. Many application layer attacks mimic browser behavior which means they do not have any specific characteristics on how they send request to identify and block them. They are just huge volume of requests but each request when looked at isolation looks legit.

Basic rate limiting rules are not sufficient in such attacks as they might be sophisticated in nature ensuring it adjusts the rate of requests well below the rate limits set but send requests from multiple sources. Such attacks can only be identified and blocked by monitoring the behavior of requests across time and identifying anomalies. All Traffic is passed through anomaly detection layer that constantly monitors the behavior of request patterns and block malicious requests. Malicious behavior is identified through sophisticated machine learning that monitors traffic and identifies requests from bad reputation, malformed user-agent etc..

DDOS Protection Details :

Attack Vectors	Details	Protection Type	Visibility
	Network Layer Attacks		
Reflection Attacks	Spoofing IP to make legitimate 3rd party to send request to Victim	Default Always On - Infrastructure Level	Since protection is at Infra level, site level visibility is not possible
SMURF Attacks	Vulnerability in ICMP protocol exploited to make network inactive	Default Always On - Infrastructure Level	
ACK Attacks	Overloading Server with TCP ACK	Default Always On - Infrastructure Level	
Flood Attacks (UDP/ TCP/ICMP)	Flooding Server with requests to exhaust resource and make server unavailable	Default Always On - Infrastructure Level	
Network Port scanning	Port scans done to exploit vulnerabilities found	Default Always On - Infrastructure Level	
	Application Layer Attacks		
Slowloris	Send partial HTTP request to Server. Server keeps waiting for rest and gets exhausted	Default Always On - Infrastructure Level	Since protection is at Infra level, site level visibility is not possible
Slow Read attacks	Sends a request to server but does not read in timely manner from the server	Default Always On - Site Level	Attacks are shown under DDOS Category
Slow POST attacks	Says to server there is POST request of x length but does not send it or sends it slow	Default Always On - Site Level	Attacks are shown under DDOS Category
HTTP Flood (GET & POST Attacks)	Requests are sent from zombie armies few request at a time. Hard to detect they remain below threshold	Default Always On - Site Level	Attacks are shown under DDOS Category
Resource Exhaustion	Identity resource that can be exhausted and attack it. For example memory exhaustion, connection pool exhaustion	Default Always On - Site Level	Attacks are shown under Rules that block exploit of vulnerabilities leading to resource exhaustion
Brute force attacks	Trial and error method to decrypt sensitive data	Default Always On - Site Level	Attacks are shown under DDOS Category
Large payload POST Attack	Oversize payload attack where DOM Parser payload is increased to cause memory exhaustion	Default Always On - Infrastructure Level	Since protection is at Infra level, site level visibility is not possible
SSL exhaustion	Garbage data to SSL server to exhaust SSL pool	Default Always On - Infrastructure Level	Since protection is at Infra level, site level visibility is not possible
Mimicked User Browsing	Requests mimicking normal user behaviour exhausting server	Default Always On - Site Level	Attacks are shown under DDOS Category
Database connection pool exhaust	Send queries that keeps DDOS connection open and exhaust	Default Always On - Site Level	Attacks are shown under Rules that block exploit of vulnerabilities leading to resource exhaustion

Unmetered DDOS Protection:

With AppTrana customer need not worry about being penalized for DDOS attacks. The DDOS protection we that AppTrana provides is unmetered/uncapped. This means no matter how huge the DDOS attack that the application receives, customer will not be penalized. Customer will be continued to be charged for legitimated requests i.e.) the requests that is passed on to the origin after processing and marking them legit.

Instant Visibility and Sophisticated Controls & Managed Protection:

AppTrana provides complete visibility into attack that matters. Network attacks as explained before are protected at infra level at various layers. Since this protection is at global level, visibility into the attacks protected in the site level is not provided to the customer. The visibilities are provided on the attacks that happen on the application layer where attacks are targeting sites on Layer 7 protocols. In such type of attacks AppTrana also sends alerts to customer when site is under DDOS attack. These alerts are just information in nature, and it is not expected from customers end to take any further action.

Managed Protection:

As a fully managed solution, notification on DDOS is also sent to internal teams when a site is under DDOS attack. The internal team is equipped with sophisticated monitoring tools to analyze the request pattern when the site is under attack. When such alerts are received, internal team checks the request patterns and take further corrective action to thwart DDOS attacks. If needed, tailor made sophisticated custom rules are written which will help thwarting these attacks.

Customer is sent notification once DDOS is thwarted. DDOS is marked thwarted if none of the DDOS protection mechanism is triggered in last 10 minutes.

DDOS protection is complex and you need a solution like AppTrana that provides comprehensive managed protection. Check out the solution now.

ABOUT INDUSFACE

Indusface is a SaaS company which secures critical Web applications of 2000+ global customers using it's award winning platform that integrates Web application scanner, Web application firewall, CDN and threat information engine. The company has been mentioned in the Gartner Magic Quadrant and Forrester Tech Now report and is CERT-In empanelled as a trusted scanning vendor and is funded by Tata Capital Growth Fund.

Bengaluru | Vadodara | Mumbai | New Delhi | San Francisco

Contact: marketing@indusface.com