WHITE PAPER

BUILDING BETTER DDOS MITIGATION:

A guide to choosing technologies, architecture and strategy

By Michael Smith, Field CTO, Neustar Security Services

neustar®
Security Services

TABLE OF CONTENTS

Overview

ABOUT THIS WHITE PAPER

This white paper discusses the six leading technologies that mitigate DDoS attacks:

- Overprovisioning
- DDoS Mitigation Appliances
- ISP Scrubbing Centre
- Third-Party Cloud Scrubber
- Cloud-Based Web Application Firewall
- Remotely Triggered Black Hole

DDoS (distributed denial of service) attacks have been a serious and persistent threat to the availability of networks, websites, and other internet-facing services for more than 25 years. And they are growing in intensity.

The steady and ongoing annual increase in the frequency, duration, and size of DDoS attacks is the product of multiple factors: rising broadband speeds available to home and mobile users; the ability for attackers to leverage amplification attacks to increase the effective available bandwidth; increasing numbers of vulnerable servers and web applications that can be combined into a botnet; and the proliferation of internet-connected devices.

With years of experience facing this evolving threat, security professionals have developed a range of architectures, solutions, and techniques to effectively mitigate DDoS attacks of every size and duration. Today there are six widely accepted technologies available to protect online assets.

Organizations that successfully defend against DDoS attacks typically use a combination of these technologies in an overarching architecture in addition to a strategy that includes gating criteria and runbooks in the Security Operations Center to reduce detection and response times. This strategy should match appropriate mitigations to the targeted assets on one hand, and attacker tactics, techniques, and procedures on the other.

This white paper provides the information you need to assess your current architecture against the types of mitigations available and choose the right solutions to protect your network, services, and applications.

It covers their characteristics, strengths, and weaknesses; and concludes with suggestions on selecting solutions and creating a strategy that will meet your needs and help you stay online – even during a complex, large, and rapidly-changing DDoS attack.

With one or more technologies identified and in place along with a plan to guide their use, your teams can respond confidently and effectively to the next DDoS attack you face.

Why DDoS Protection Matters

DDoS attacks have been part of the landscape for so long they can sometimes be overlooked as a threat. And because they are cyclical, an organization and its peers may not face an attack for years, making them easier to dismiss.

But DDoS attacks present serious risks, especially as organizations shift revenue generation and customer relationships to their online presence.

If you haven't tested your mitigation capability recently – or been the victim of an attack – you probably don't know how well you can detect and respond to one, which could put your organization at risk.

Some things about DDoS attacks haven't changed. They still threaten to overwhelm your network, freeze your website, and block access to critical online assets for hours or longer. They still occur with depressing frequency – we estimate around 30,000 times every day. And they still overwhelm security teams and disrupt operations at enterprises large and small around the world.

But in important ways, DDoS attacks are changing as attackers try new strategies and techniques. Malicious actors have assembled larger botnets to launch larger sustained attacks and adopted quick-moving "carpet bombing" attacks against multiple targets in serial to evade detection. They constantly explore new attack vectors that can exploit different vulnerabilities, and they seek to do more damage than simply bringing down a victim's website.

3x more attacks

The pace of attacks is rising steadily. Neustar Security Services saw a three-fold increase in the number of attacks in 2021. Other security sources also reported all-time highs. The 2021 surge is part of an ongoing trend; in 2020 we saw attacks increase by 151% over 2019. There is no indication the pace is slowing down.

13x more large attacks

One security source reports the number of attacks larger than 250 Gbps ballooned 1300% in 2021,[1] and November saw the largest attack so far: 3.47 Tbps.[2] The vast increase in the number of IoT devices has enabled attackers to assemble ever-larger botnets to launch larger and larger attacks.

Many more stealthy attacks

Detection is an issue. 42% of the DDoS attacks Neustar Security Services saw in 2021 were part of a carpet bomb attack – numerous, short-duration attacks targeting hundreds or even thousands of individual addresses or subnets at a single organization. The individual attacks can be so quick that they are overlooked.

More DDoS ransom attacks

Attacks can cost you real money. 22% of DDoS victims reported in a Q4 2021 survey that their attacker demanded a ransom.[3] Attackers typically specify a significant payment in cryptocurrency to prevent or stop a massive attack.

More application layer and multi-vector attacks

You're more likely to face attacks that change throughout the attack. One security source reports application layer attacks surged 164% in Q1 2022 compared to the previous year. When the attacker utilizes multiple vectors, they can monitor and modify the attack to exploit vulnerabilities in defenses. These complex multi-vector attacks are also more common now; one attack in 2021 utilized 31 different vectors.[4]

In 2020 we saw attacks increase by

151%

over 2019

Number of attacks larger than 250 Gbps ballooned

1300%

in 2021

Application layer attacks surged

164%

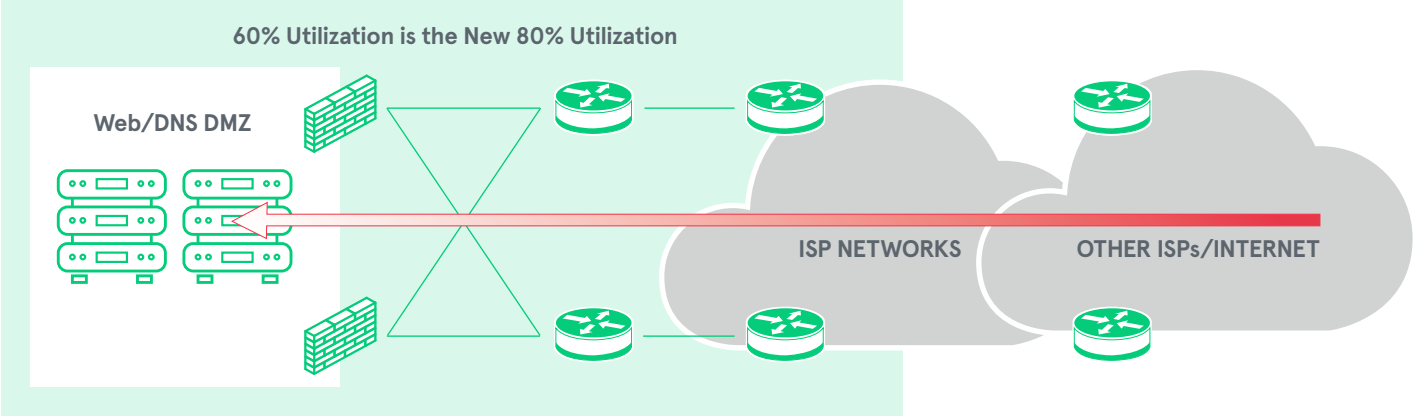
in Q1

[1] 2022 Application Protection Report DDoS Attack Trends
[2] Here's How We Stopped the Biggest Ever DDoS Attack
[3] DDoS Attack Trends for Q4 2021
[4] DDoS Attacks Are Becoming More Prolific and More Powerful, Warn Cybersecurity Researchers

DDoS Mitigation Technologies

1. Overprovisioning

How it works: Your enterprise overprovisions critical network resources (web and email hosting, servers, network connections) at just 40 – 60% of normal usage requirements, instead of typical provisioning of around 80% utilization.



Pluses

- Provides internal capability to handle small DDoS attacks
- Can leverage autoscaling capabilities of cloud resources for larger attacks
- Requires no specialized expertise for implementation
- Provides passive mitigation without operator involvement
- Some technology such as routers, firewalls, and IDS have organic DDoS mitigation controls
- Could increase performance for users if scaling includes additional points-of-presence (PoPs) and load-balancing across them

Minuses

- Capacity is very limited, and cannot be increased quickly (without autoscaling)
- Attacks that exceed capacity will still succeed
- Requires CapEx to buy, install, and configure, resulting in overspending on infrastructure if you don't receive an attack
- Can result in additional, unexpected expenses that rapidly exceed your services budget if an attack results in cloud autoscaling
- Need to constantly monitor usage against capacity and make adjustments

Best for:

Organizations that self-host their applications

Small and non-critical websites or networks

Large organizations with the ability to autoscale their hosting and network

Organizations with rapidly growing network and application usage

Organizations that have never been targeted by a DDoS attack but want resiliency

Discussion

Overprovisioning is often the choice of smaller security-conscious organizations and the initial mitigation step for larger enterprises, because it is relatively simple to implement.

It can make use of the organic DDoS capabilities built into existing equipment such as routers, firewalls, and intrusion detection systems (IDS). An effective implementation, however, involves upsizing a long list of network components including backend databases, web and email servers, application servers, firewalls, network switches, routers and so on.

Autoscaling to cloud resources can also provide additional capacity virtually instantaneously. Those additional resources will come at a price, however, that may not be cost-effective, particularly if larger attack drives autoscaling to significantly higher usage levels.

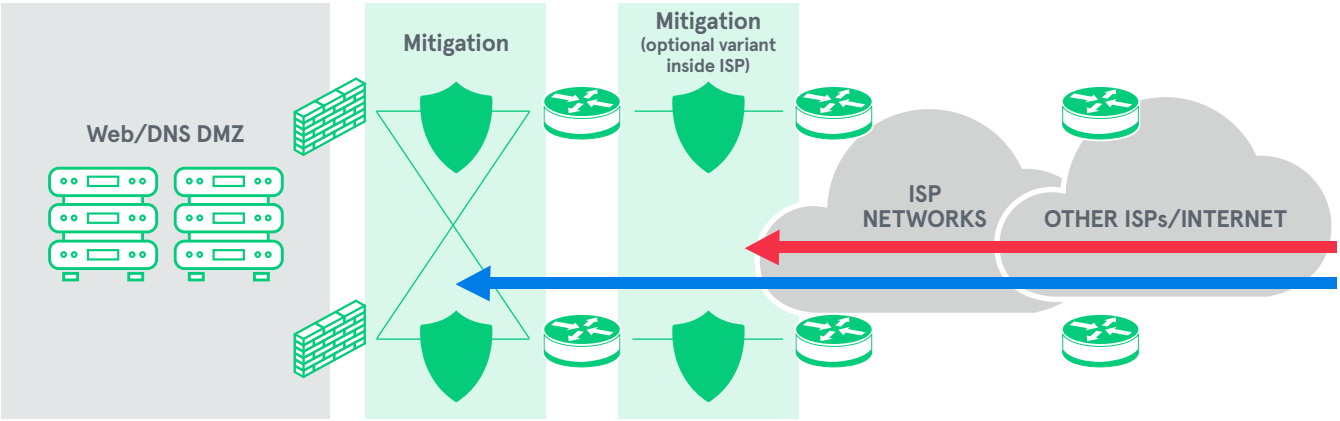
How Neustar Security Services can help

Neustar Security Services provides compatible solutions for an overprovisioned data center by monitoring network connections and diverting traffic in the event of a large attack to UltraDDoS Protect, our cloud-based DDoS solution.

In addition, Neustar Security Services can ensure access with UltraDNS, an authoritative DNS service that uses overprovisioning, multi-tenancy, and a huge number of points-of-presence (PoPs) to absorb large DDoS attacks against an organization's authoritative nameservers. Since every public-facing service depends on DNS to direct traffic to the appropriate server, the impact of a DNS outage affects everything. For this reason, DNS is heavily targeted by DDoS attacks.

2. DDoS Mitigation Appliances

How it works: Your company deploys appliances specifically designed to mitigate DDoS attacks – essentially stateless scrubbing devices that can detect and drop DDoS traffic – in the datacenter, or in more advanced instances upstream of the datacenter inside the ISP.



Pluses

- Drops DDoS traffic in your datacenter environment or upstream in the ISP
- Can scrub traffic for either network blocks or individual IP addresses
- Sufficient capacity to handle small DDoS attacks, which are extremely common
- Additional appliances can expand capacity to handle moderate attacks
- Traffic can be diverted to mitigation quickly
- Provides traffic monitoring and detection capabilities that can be used in conjunction with other, higher capacity technologies
- Some appliance manufacturers offer a cloud scrubbing service to mitigate excess capacity at additional cost

Minuses

- Aren't cloud native so deploying in cloud environments is challenging
- Capacity is limited by the amount of bandwidth into the hosting data centers
- Each datacenter or ISP requires appliances
- Enterprises without dedicated and trained mitigation staff will have a higher rate of false positives and collateral mitigation damage
- Requires additional and cyclical CapEx to acquire, update, and replace appliances, with unpredictable benefits
- Requires IT engineering involvement and, ideally, some DDoS security experience

Best for:

Organizations with capable internal security teams and an interest in on-premise mitigation capabilities

Larger organizations that function as an internal cloud provider for multiple business units

Organizations operating in regulated industries that do not allow cloud service

Organizations that are frequently attacked

Discussion

DDoS mitigation appliances detect potential attacks by counting – packets, bytes, tcp sessions, http requests – and dropping traffic with telltale patterns. They should be located upstream of firewalls and routers in the datacenter, or upstream of the datacenter in the ISP.

Some enterprises have responded to repeated attacks by deploying multiple mitigation appliances in what amounts to an internal DDoS scrubbing center. These organizations typically have a dedicated, capable IT security team and a very large infrastructure, capable of handling as much as 100 Gbps of traffic.

Even these large implementations, however, face the limiting factor for mitigation appliances: the bandwidth available between the network and the ISP(s). If an attack exceeds that bandwidth, the network circuits will become saturated before the traffic reaches the mitigation appliances, which will result in an outage.

How Neustar Security Services can help

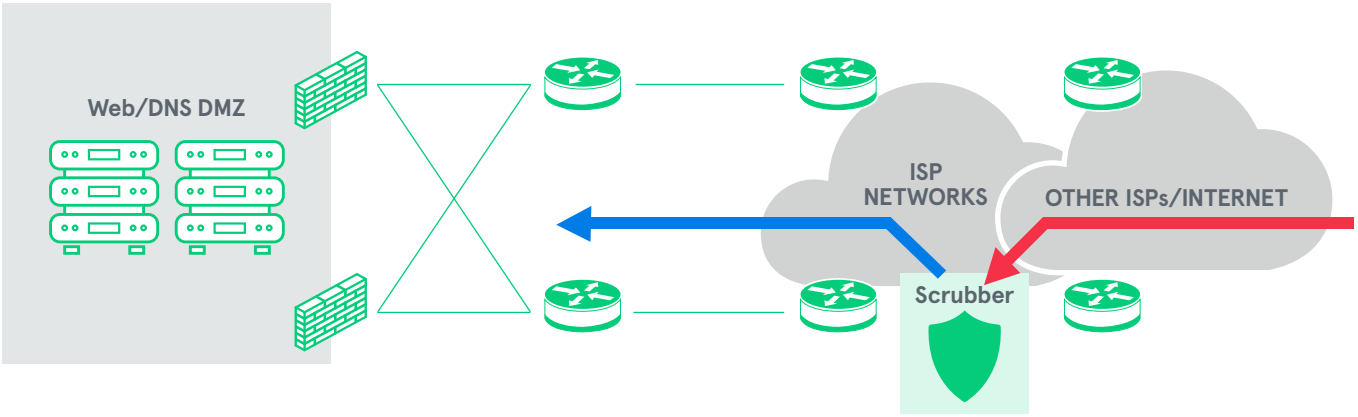
UltraDDoS Protect from Neustar Security Services is very compatible with on-premise appliances by providing back-up protection if attack volume exceeds the capacity of your on-premise array of mitigation appliances. Protection can be provided in two ways:

- On demand, with your Network Operations Center (NOC) or Security Operations Center (SOC) diverting traffic to our mitigation platform, or
- As a managed service in which we monitor data from your appliances and network devices and divert traffic to our platform based on preset thresholds.

In both cases, clean traffic is returned to your network, and all traffic is undiverted when the attack is over. We have direct integrations available with Arbor and Correro on-premises equipment for a fully hybrid option and we support an OpenHybrid API for signaling and integration with other on-premises vendors.

3. ISP Scrubbing Center

How it works: Your enterprise contracts with your ISP(s) to route traffic for specific IP addresses through scrubber appliances deployed within their network, clean it, and send it to your data center. These are typically the same mitigation appliances discussed previously, deployed in greater numbers and with more bandwidth.



Pluses

- Larger capacity than all but the largest on-premise solutions, typically 20-120 Gbps
- Can scrub traffic for either network blocks or individual IP addresses
- Mitigation can be activated very quickly because traffic is diverted through internal ISP routing and doesn't rely on BGP (border gateway protocol) propagation for diversion
- Some ISPs can provide monitoring services to detect a DDoS attack and divert to their scrubber
- Some ISPs contract with mitigation appliance vendors to offload excess attack capacity at an additional cost

Minuses

- Requires enterprises to contract with all their multiple ISPs which adds complexity and cost
- Capacity is limited by the unused capacity of an ISP's peering bandwidth
- ISPs typically route attacks exceeding their capacity to a remotely triggered black hole in order to protect their other customers if the attack exceeds their available peering bandwidth
- Most ISPs don't have dedicated and trained mitigation staff so they have a higher rate of false positives and slower response times
- During large campaigns, ISP bandwidth and scrubbing capacity can get saturated by multiple simultaneous mitigations

Best for:

Supplementing or replacing on-premise solutions for small- to medium-sized websites

Organizations that only use one or two ISPs for bandwidth

Organizations that self-host their applications in their datacenter

Discussion

ISP scrubbing centers provide a relatively low-effort option to mitigate attacks that exceed the capacity of on-premise solutions. The ISP service provider(s) are already business partners providing bandwidth, so protection can be added to existing contracts.

There are limitations, however. ISPs have an upper limit on their scrubbing capacity based on their peering bandwidth. An attack that exceeds that limit will overwhelm their peering, and the ISP will have no choice but to divert traffic to a remotely-triggered black hole (RTBH), which cuts off access to your site as effectively as a successful DDoS attack.

In addition, because DDoS mitigation is a sideline for ISPs, most offer limited services. For example, some ISPs will not monitor your traffic to detect a possible attack; your team must take on that responsibility. And while ISPs will have staff trained in how to handle an attack, their experience is generally limited.

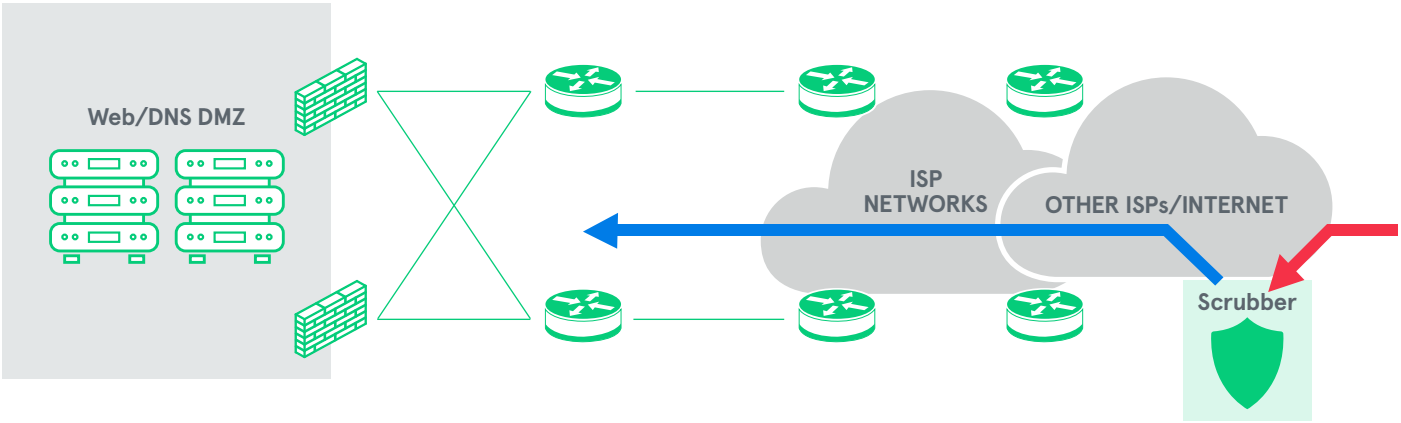
Finally, if your enterprise uses more than one ISP and an attack successfully passes through one of them, your website will be cut off even if the others are successfully scrubbing it. Consequently, you must contract with and rely on all your ISPs for DDoS mitigation services.

How Neustar Security Services can help

Ultra DDoS Protect from Neustar Security Services is very compatible with ISP DDoS mitigation services for large volume, longer duration, and rapidly changing DDoS attacks that exceed ISP capacity.

4. Third-Party Cloud Scrubber

How it works: Your enterprise contracts with a dedicated DDoS mitigation specialist, operating a massively scaled scrubbing center built with mitigation appliances. You route traffic to the scrubbing center using diversion of BGP (border gateway protocol) or by changing the DNS A or AAAA record for the host you would like to protect. The traffic is then returned via a generic route encapsulation (GRE) tunnel, direct interconnection, virtual circuit or using back-end DNS.



Pluses

- Much higher capacity that an ISP scrubber, generally from 3-15 Tbps or more
- Capacity is continually upgraded to keep pace with growing attack volumes
- Uses multiple points-of-presence (PoPs) fronted by anycast for load-balancing and to combine capacity
- May offer an always-on service to reduce problems with BGP propagation, convergence, and route suppression
- Maintains a Security Operations Center to oversee operations, with staff responding to DDoS attacks on a daily basis
- Can support DNS diversion for individual hosts

Minuses

- Diversion of traffic to the scrubber and back to your datacenter can introduce latency
- BGP diversion requires your enterprise to own and manage routing for a network block or ASN
- Diversion for on-demand service options requires time for BGP to propagate
- DNS diversion relies on DNS being available and attackers following DNS to mitigation
- Always-on scrubbing comes at a cost

Best for:

Organizations that receive frequent or large attacks

Organizations that have a large amount of production traffic and large mission-critical websites

Organizations with multiple datacenters

Organizations with circuits from multiple ISPs

Discussion

Because they continually and successfully mitigate the largest and most intense DDoS attacks, third-party cloud scrubbers are generally considered to offer the most fail-safe protection from a broad range of attacks. Some ISPs even use them to offload attacks that exceed their capacities.

Most large scrubbers have multiple points-of-presence around the world, deployed close to internet exchanges to minimize the potential effects of latency. They typically buy bandwidth from multiple ISPs for the same reason, and to ensure redundancy.

In most instances, traffic is routed to the front of the scrubber using BGP, although some third-party scrubbers own IP addresses to allow customers to divert individual host names to their platform using DNS – a useful option for on-demand mitigation involving a relatively small number of hosts.

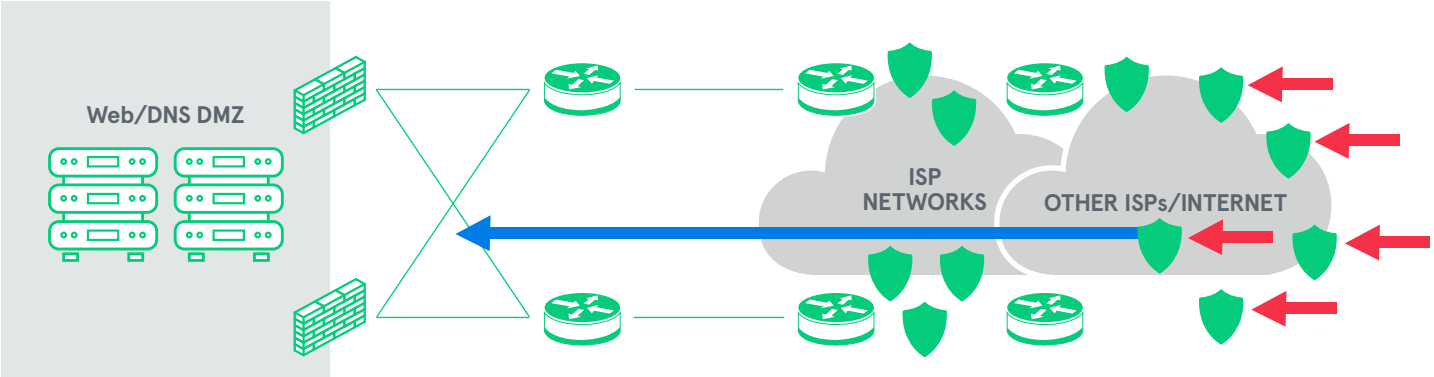
Scrubbers typically route clean traffic back to your network using GRE tunnel, fiber direct connect or SDN (software defined networking) for an additional measure of security.

How Neustar Security Services can help

Neustar Security Services offers a leading global third-party scrubbing solution with UltraDDoS Protect, available to provide both always on and on-demand protection through one of the world's largest dedicated DDoS mitigation platforms.

5. Cloud Web Application Firewall

How it works: Your enterprise contracts with a provider of a cloud-based Web Application Firewall (WAF) service to protect HTTP and HTTPS traffic while also providing protection from web application attacks that can lead to impacts such as data breaches and defacement.



Pluses

- Can provide protection against content scrapers
- Usually has significant capacity that meets or exceeds all other solutions
- Complementary to network-based mitigation such as appliances, ISP scrubbing centers, and 3rd-party scrubbing centers
- Always-on solution that provides passive and active DDoS protection
- Protects against SQL injection, cross-site scripting, and other threats targeting the application layer that are more frequent than DDoS attacks
- Many can cache and deliver objects as part of a CDN (content delivery network)
- Uses TLS (transport layer security) certificates and inspection of traffic inside of TLS for improved accuracy
- Uses rate controls that can detect and block an application-layer DDoS in seconds
- Drops non-HTTP/HTTPS traffic instantly which can be a very effective passive DDoS defense
- Can perform some web traffic management functions such as load-balancing across datacenters, instant http redirects, and http request rewrites
- Uses multiple points-of-presence in order to improve performance for users
- Most cloud WAFs publish an "allow" list of IP addresses so customers can block direct internet access to their servers and force traffic through the WAF

Minuses

- Limited to protecting web traffic (HTTP/HTTPS) and not other protocols such as UDP (user datagram protocol), SMTP (simple mail transfer protocol), or VPN (virtual private network)
- Can be bypassed by attacking the application server directly instead of following DNS to the WAF
- Requires TLS certificates and traffic inspection to defend TLS and HTTPS traffic
- Smaller cloud WAF providers may have to deplatform a customer that is hit by a large attack to protect their other customers

Best for:

Large websites that use TLS

Websites that have sensitive data such as financial, healthcare, government, or other kinds of Personally Identifiable Information that also need protection from data breaches

Web applications that have vulnerabilities that need a virtual patch

Discussion

With every major enterprise leveraging cloud resources – and more and more DDoS attacks targeting the application layer – a cloud-based web application firewall provides a crucial additional layer of protection against a wide range of threats.

A cloud-based WAF functions as a highly distributed reverse web proxy with global points of presence. Web (HTTP/HTTPS) traffic is routed to the WAF via DNS. The WAF then performs rate controls by counting requests and and cuts off source IPs that send an excess of requests. It also drops non-web traffic. The clean traffic is forwarded back to the authoritative application servers.

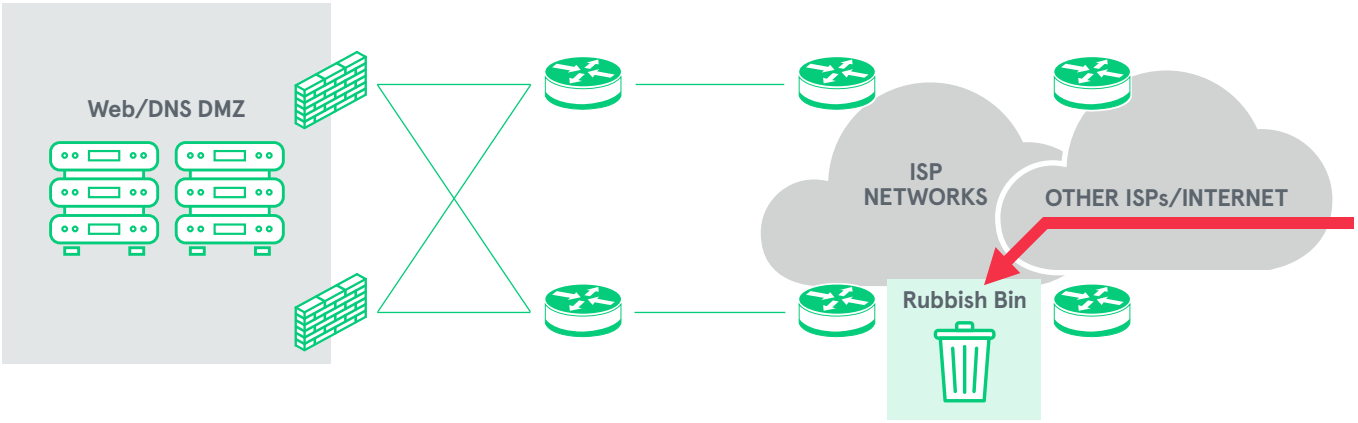
As noted above, a WAF can be bypassed by a direct attack on the hosting platform. Most providers, however, offer a means for their customers to ACL traffic into their hosting platforms.

How Neustar Security Services can help

Neustar Security Services offers a leading cloud-based web application firewall in UltraWAF, a vendor and location agnostic solution with flexible positive and negative security. UltraWAF is in turn protected by UltraDDoS Protect that mitigates additional DDoS volumes.

6. Remotely Triggered Black Hole

How it works: This "solution" simply dumps all traffic, good and bad, across the internet, using BGP to send it to a non-routable address space. It is a commonly used DDoS mitigation technique that is applied when it is not cost-effective to defend against an attack or the attack is so large that it impacts other organizations besides the target.



Pluses

- Capacity is not an issue
- Requires no advance preparation or planning
- Can be combined with BGP communities to only blackhole distant traffic while close traffic is delivered

Minuses

- Requires your enterprise to own and manage routing for a network block or ASN
- Drops legitimate traffic as well as malicious traffic
- Renders your website and other services inaccessible, as if the DDoS attack succeeded

Best for:

Limited, non-critical websites

Used as a last resort when the attack is large in volume or duration

Used by ISPs when the attack is too large for their infrastructure

Discussion

The fact that remotely triggered black holes are a commonly used technique to deal with DDoS attack suggests that many organizations are simply not prepared to mitigate attacks, because it doesn't actually mitigate the attack. It just dumps all traffic – good and bad – in the equivalent of giving up.

A remotely triggered black hole relies on the RFC 1918 address space, set up by every ISP to send traffic to the null interface on routers. When access to a network block is diverted to an RFC 1918 network, every router around the world immediately starts dropping the traffic, cutting off the DDoS attack along with all legitimate traffic.

As a result, this technology of last resort is best reserved for use with non-critical websites or for network segments where the costs associated with more nuanced mitigation measures are not justified by either the revenue it generates or the importance of accessibility.

How Neustar Security Services can help

The capacity of our cloud-based mitigation solutions prevents the need for this technology.

Which Technology Should You Choose?

DDoS Mitigation Technology Summary

Technology	Hosted	Capacity	Comments
Overprovisioning	On-Premise / inside a Cloud Service Provider	Only for small attacks	Best practice for most organizations
DDoS Mitigation Appliances	On-Premise	Small-medium (depending on # of appliances and circuit bandwidth)	Useful for mitigating small/medium attacks without outside resources – if enterprise has IT expertise
ISP Scrubbing Center	ISP	20-120 Gbps	Good mitigation for small-medium attacks
Third-Party Cloud Scrubber	Cloud-Based	3-15 Tbps or more	Excellent mitigation with greater capacity and staff expertise. One of the top all-around solutions.
Cloud WAF	Cloud-Based	>10 Tbps (web traffic only)	Excellent protection for application layer attacks of all kinds; can only protect websites
Remotely Triggered Black Hole	N/A	Unlimited	Mitigation of last resort

There really is no single choice for every organization, fit, and purpose. If you can only pick just one answer, a cloud-based third-party scrubbing service is a true all-around solution that makes it a good place to start. In addition, there are, however, agreed on best practices:

- Establish a clear policy and architecture as well as processes, criteria, and standards for the use of the technology(ies) for each potential target, and for attacks of different volumes, duration, and types.
- Consider a layered defense using two or more technologies that complement each other: overprovisioning of DNS and other critical services plus a third-party scrubbing service plus a cloud WAF for key websites, for example, or an ISP or third-party scrubbing service for self-hosted applications with a cloud WAF for applications hosted on a cloud service provider.
- Test your mitigation controls a minimum of every 6 months to verify that the service dependencies and assumptions are still valid. Neustar Security Services encourages its customers to do a range of tests from a basic diversion test to a full live DDoS traffic test in order to establish trust in themselves and the services that we provide.

The more useful question is "which technologies are best for my enterprise?" Each technology can protect some things well; each has its limitations.

Consider capacity, for example. Third-party cloud-based scrubbing services have the largest capacity out of most of the options and make for one of the best all-round solutions but are not cost-effective for a single small-use website. Overprovisioning has a very limited capacity but can mitigate small attacks with minimal effort and no operator intervention. A cloud web application firewall has relatively unlimited capacity and offers additional application layer protection, but can only protect services that use HTTP/HTTPS. ISP scrubbing centers can only protect traffic that traverses their network.

To identify the technologies that can best protect your enterprise, your security team should weigh these interrelated factors.

- **The extent and value of the assets you need to protect**

  Small, less important websites or network segments may merit a different security approach than large, mission-critical websites, or sites that generate significant revenues. Also consider where assets are hosted – cloud vs. data center – and whether they are part of a single network block.

  Focusing on these issues will help you determine the scope and capacity of the solutions that are appropriate for your assets, possibly including separate approaches for different segments of your online assets.

- **Understand current attack trends**

  Finally, review current information about and trends in DDoS attacks targeting your industry to gauge the size, intensity, and types of attacks you could reasonably expect – while recognizing that the unexpected is always possible. DDoS attacks are a dynamic threat, with attack trends that change over time, sometimes quite suddenly.

- **Protection levels from current and anticipated DDoS mitigation assets**

  Include DDoS capabilities organic to your network hardware and security infrastructure such as routers, firewalls, and IDS as well as dedicated mitigation appliances. Find out if your ISPs and cloud providers include any level of DDoS protection as part of your service agreement, and if any optional add-on services are available.

- **The consequences and costs of a successful attack – and your willingness to absorb them**

  Evaluate how long you can afford to have your assets unavailable, and what it would mean to your enterprise, your business partners, and your customers. Most organizations determine the cost impact of a DDoS using the average dollar value of a transaction, the average number of transactions per minute or hour, the average duration of a DDoS attack, and the number of attacks they receive in a calendar year. Keep in mind that attacks have a much higher impact at certain times of the year, such as the holiday shopping season or tax filing deadlines.

  Your risk assessment will help you decide the degree of certainty and reliability your protection must provide. In turn, you can establish how much your enterprise is willing to invest to secure it, whether that involves purchasing additional capacity or mitigation appliances, or contracting with an ISP or third-party scrubber.

- **The effects of DDoS attacks on the efficacy of other technical controls**

  In considering risk, keep in mind that DDoS attacks are increasingly being used in combination with other attacks, exhausting SOC staff or even flooding application and boundary controls so that defenders turn them off and leave the application exposed to other impacts such as a data breach. Network, boundary, and application controls are very asymmetrical to network traffic in that they use a lot of resources to inspect incoming traffic and determine if it is malicious. Because of this, they are easily overwhelmed by DDoS attack traffic and will either fail closed (you take an outage) or fail open (the website is up but without any protection). A good defense against DDoS attacks increases the effectiveness of these controls and their ability to continue to perform functions such as deep packet inspection and application input validation.

- **Technology cost and secondary benefits**

  Because of the cyclic nature of DDoS attacks, some organizations do not receive one for more than a year. Mitigation technologies such as routers, firewalls, a cloud WAF, or a DNS service that provide additional benefits beyond DDoS mitigation can help with budget and procurement decisions.

Thoughtful consideration of these factors will enable you to select the mitigation technologies that match your security goals and resources. If they include independent third-party providers, the next step is to evaluate providers for their mitigation capacities, offerings (such as always-on or on demand, ability to monitor your traffic, etc.), experience, and service intangibles such as responsiveness to inquiries.

After you have chosen and implemented your technologies, make sure your enterprise establishes specific attack criteria for triggering your mitigation technologies. You should also create clear procedures, such as when and how to change BGP or DNS settings to divert traffic or procedures for sharing TLS keys, if necessary, and share them with your IT staff and partners.

When a DDoS attack hits, every minute counts. Well-defined, rehearsed, and tested procedures will speed your response time and limit the impact of any attack.

Strengthen the Implementation of Your Mitigation Strategy

Regardless of your DDoS mitigation plans and architecture, Neustar Security Solutions can make it more effective. As a leading global specialist in security solutions, we offer superior cloud-based mitigation technologies that deliver the highest level of protection for your websites and network assets.

Neustar Security Services provides three of the six solutions discussed in this white paper overprovisioning for authoritative DNS with UltraDNS; a third-party scrubbing service through UltraDDoS Protect; and cloud WAF with UltraWAF. These services are very compatible with the three remaining technologies to create a multi-layer defense.

- UltraDDoS Protect provides cloud-based mitigation with more than 15+ Tbps of capacity, one of the most extensive and highly scalable scrubbing networks in the world. It is driven by an advanced orchestration platform to support mitigation of complex, multi-vector, and multi-phase attacks.

  Service options include both always-on protection, with all traffic routed through our global platform at all times; and on-demand protection, with traffic diverted to our platform when an attack is detected. On-demand service offers the additional option of managing and monitoring of your appliances to detect attacks and implement mitigation.

- UltraWAF is a cloud-based web application firewall that mitigates web traffic DDoS attacks while also providing effective protection against a broad range of other threats targeting the application layer, including the OWASP top 10.

  It can incorporate customized positive and negative security rules and apply them consistently across a complex hybrid network, and offers unparalleled visibility into application traffic.

- UltraDNS is a cloud-based authoritative DNS solution spread across 30 high-capacity points-of-presence that provides peak performance, scale, and resilience despite peak loads and DDoS attacks.

Neustar Security Services maintains a global network of points of presence, supporting real-time load-balancing to prevent a single attack or outage from affecting service and minimizing latency. Our cloud-based DDoS mitigation solutions are complemented by a high-capacity recursive DNS service and an advanced bot management solution to counter the threat of malicious bot traffic.

All our solutions are vendor- and carrier-neutral, and actively overseen by a 24/7 security operations center (SOC) staffed by experienced security professionals with significant real-world expertise in dealing with DDoS attacks and other serious cyberthreats.

For more than a decade, Neustar Security Services has supported major enterprises around the world, mitigating some of the largest, most intense, and most complex DDoS attacks ever launched.

Put our experience to work – and strengthen your protections against DDoS attacks of every type and size, as well as other serious threats to your online enterprise.

About Neustar Security Services

The world's top brands depend on Neustar Security Services to safeguard their digital infrastructure and online presence. Neustar Security Services offers a suite of cloud-delivered services that are always secure, reliable, and available and enable global businesses to thrive online. The company's Ultra Secure suite of solutions protects organizations' networks and applications against risks and downtime, ensuring that businesses and their customers enjoy exceptional, and uninterrupted, interactions all day, every day. Delivering the industry's best performance and always-on service, Neustar Security Services' mission-critical security portfolio provides best-in-class DNS, application and network security including DDoS, WAF and Bot management services to its global 5000 customers and beyond.

Find more information at:

neustarsecurityservices.com

Call USA: +1 (844) 929 - 0808
Call EMEA: +44 808 175 1189

WP-SEC-295760-08.03.2022