DDoS Shield

Service Description

May, 2026

Note: Due to the inherent evolutionary nature of technology, Verizon reserves the right to change, modify, update or enhance this DDoS Shield - Service Description from time to time without notice.

verizon business

Table of Contents

verizon business

1. DDoS Shield at-a-glance

DDoS Shield is a cloud-based, carrier agnostic Distributed-Denial-of-Service detection and protection solution. DDoS Shield provides a solution to large-scale volumetric denial-of-service type threats across your entire enterprise. The service provides constant monitoring and analytics of all configured inbound traffic and can proactively mitigate the effect of attacks as they happen. This mitigation minimizes the impact on traffic and resources, allowing normal business operations to continue.

DDoS Shield provides a fully managed service to detect volumetric DDoS threats and mitigate the impact of the attack for protected IP address space (IPv4 and IPv6) on a global basis. It pairs a high scale global platform with a bespoke web-based user portal providing near real-time customer traffic information before and during a DDoS event.

DDoS Shield subscriptions may be obtained as either an enterprise-wide entitlement that may be used with any eligible internet service provider connections (including Verizon) or as a charged feature to Verizon Internet Dedicated Services.

2. Introduction to DDoS Shield

While the concept of a Distributed Denial-of-Service (DDoS) attack is nothing new, attack trends over the past three to five years have changed significantly. The involvement of nation-state threat actors, groups intending on-line social or political statements and the rise of 'ransom' DDoS attacks have driven up the frequency and peak volumes of attacks. At the same time, the popularity of cloud computing and attack services for-hire have lowered the barriers to entry and made the instigation of damaging attacks accessible to anyone with ill-intent. Organizations both large and small must be prepared to defend against protracted and determined attacks that use a combination of attack vectors as well as short, high-volume attacks often used to distract attention from the attackers' true intent.

DDoS Shield is a managed, cloud-based, service designed to:

- Monitor inbound traffic to provide early warning of DDoS activity against any protected Internet assets **(Detection)**
- Intercept and drop malicious DDoS traffic inbound to a customer's Internet-connected network to mitigate the impact of the attack **(Redirection)**
- Return cleaned (good) traffic, allowing customer services to continue as normal

When DDoS Shield redirection is initiated, it will re-announce subscribed IP addresses from Verizon's cloud-based mitigation facilities as the best route, thus diverting all inbound traffic away from the targeted location. At the mitigation centers, Verizon applies filters and other countermeasures to the redirected traffic prior to returning legitimate traffic via dedicated clean traffic return tunnels. In most cases, DDoS Shield

verizon business

is utilized to redirect and filter traffic only during an active DDoS event, ensuring that normal network paths to your servers are maintained and there is no impact to normal traffic. When an attack occurs, DDoS Shield can detect and alert on the incident to allow either manual redirection driven by our portal or by contacting Verizon Operations to approve a response or, with prior customer approval within our portal, a redirection can be initiated either automatically or by Verizon directly to deal with the attack without your initial intervention.

There is no limit to the use of DDoS Shield when under attack, the frequency of attack redirections, the length of time Verizon will protect against an attack, or the size of attacks mitigated.

DDoS Shield is always available, meaning that Customer's traffic filtering policies and configurations are accessible in all of our global mitigation centers at all times ready to act on receipt of the first redirected packet. The manual or automated response to a detected attack incident can be directly defined per IP subnet via the portal, allowing greater flexibility.

DDoS Shield customers may also subscribe at any time to an optional Always Routed service. This add-on feature allows selected subnets to be continuously redirected through DDoS Shield scrub centers even when no DDoS attack is present. The Always Routed feature provides around the clock protection, ideal as a solution for short length, high frequency attacks and eliminates route setup/propagation delays. The Always Routed service also enables constant filtering against a customer-defined baseline policy that can be defined in the portal and reporting of inbound forwarded/dropped traffic. Customers can always add, change, or remove the IP subnets being redirected to DDoS Shield directly from the portal allowing extreme adaptability to threats as they evolve.

Whether used as always available and on demand, or with our Always Routed feature, the DDoS Shield operates uni-directionally. DDoS Shield will only alter the route path and filter inbound traffic to the protected IP addresses and we will typically use the smallest traffic redirection possible to handle the attack. All traffic outbound from the protected sites will follow its normal routing path to the Internet as usual with no impact.

When traffic is redirected to DDoS Shield, sudden high volume inbound traffic spikes will be mitigated by a combination of Verizon default anti-DDoS policies developed over many years of experience securing one of the world's largest IP networks, and by using customer pre-defined policies configured via the self-service portal. These filtered mitigation countermeasures will be applied to traffic without requiring further customer intervention and can be safely tested periodically.

At times, additional countermeasures may be required using further tools and methods at our disposal. These mitigation countermeasures are provided as a managed service by Verizon's Security Operations Center (SOC). These custom configurations persist

only for the duration of the ongoing attack incident. Note: Ongoing mitigations may still require some customer participation to ensure the continued optimal removal of malicious traffic as an attack progresses.

3. How it works

DDoS Shield will operate in concert with the customer's own environment. It is not a replacement for edge security systems such as firewalls and intrusion prevention systems (IPS), and web application firewalls (WAFs) capable of filtering and blocking bad traffic up to maximum circuit bandwidth. Those systems are best placed to handle lower volume application level security. When the customer's circuits/edge equipment is at risk of being overwhelmed by volumetric attacks, DDoS Shield can take over mitigation responsibilities. When traffic returns to normal levels, DDoS Shield will be removed from the routing path unless the redirection is marked as part of an 'Always Routed' service subscription.

Verizon's DDoS node model is unusual as each node is constantly available for inbound traffic to subscriber IP subnets. This enables traffic to be redirected into the service with no lead time for configurations to be loaded, in fact traffic can be redirected directly by use of eBGP without resorting to the customer portal to achieve filtering from the first packet received.

Each of the DDoS Shield mitigation nodes is super connected to Verizon's global IP backbone using our PPR (Partner Peering Route) systems that we use to deploy large scale connectivity between Verizon and our largest peers ensuring we have the capacity to mitigate attack.

When traffic is redirected, DDoS Shield forces traffic to be routed to the closest mitigation node to the source of the traffic, this provides least impact on legitimate traffic yet also allows large attacks generated by globally dispersed botnets to be mitigated across all of the DDoS Shield locations.

verizon business

Figure 1: DDoS Shield node global locations

Note: DDoS Shield is not approved for sale/provisioning to protect IP assets in China, Russia or countries in the Middle East and North Africa. Seek assistance from your Sales Account manager if you require protection in these locations.

To use DDoS Shield, a customer location must either have a public Internet circuit, and publicly re-routable IP address space via Border Gateway Protocol ("BGP"), of at least a Classless Inter-Domain Routing ("CIDR") /24 for IPv4, /48 for IPv6. Alternatively, for eligible Verizon IP services, Verizon can support redirection of subnets between IPv4:/25 and /32 (single host), IPv6:/49 and /128 (single host).

From a top-level view, triggering a response to an attack can be managed very quickly, either via a one-way BGP traffic announcement, using our portal to control our managed route servers directly or via a phone call to the Verizon SOC or by pre-authorizing one of the 2 proactive response modes that are included to customers.

Some pre-configuration is required, but once the necessary routing announcement changes have been made and detection feeds have been created for non-Verizon IP services, the ability to redirect traffic into DDoS Shield becomes quick and seamless. The pre-configuration involves ensuring the required route announcement policy is in place to permit Verizon to become the preferred route for the customer's traffic should the customer's own circuit/route become unavailable.

During a high traffic volume event, the routing policy in place on the customer's own routers and on Verizon DDoS Shield routers will ensure that the customer's network remains available. The customer's route announcement will be any-cast to global peers from all locations simultaneously by default. This helps to assure nominal additional

latency for the good traffic, high availability and redundancy and a highly (global) distributed platform to stop DDoS attacks before they impact customer or network-critical peering points within any one region or country. DDoS Shield offers a self-service dashboard to manage configurations and custom traffic policies that are applied to redirected traffic.

When a redirection is required either as a customer reported incident or after a detected attack notification, it is started by either:

- Sending a BGP routing signal;
- Reporting the suspected attack via the Portal.
- Calling the Verizon SOC to request activation & investigation.
- Preauthorizing Verizon to respond to attack incidents detected directly.

The Portal is the fastest and most secure method to manually start a redirection and report a suspected attack. Customers can pre-authorize Verizon to act upon attack alerts to redirect traffic through the Portal, this is recommended in most cases. The Portal allows configuration of a default response to attack incidents that can be configured for individual IP address groups.

Verizon retains the right to remove any non-impacted route announcement and turn off any unnecessary redirection from the service platform unless declared as part of an Always-Routed allowance when there is no evidence of attack traffic or justification given for the continued usage. The SOC team will always notify Customer's Authorized Contact prior to ceasing any redirection. Mitigation may not be used on a continual basis or as a precautionary measure unless declared as an 'Always Routed' Subnet or with the SOCs approval. Verizon may stop mitigations 72 hours after Verizon has determined that a DDoS attack either has ceased or did not occur.

4. Service cost elements and requirements

Service requirement specifics:

- To enable use of DDoS Shield, Customer must either:
    - Subscribe to an eligible Verizon IP service where subnet routing will be used to mitigate smaller subnets (below CIDR IPv4:/24 down to /32 or below IPv6:/48 down to /128) or,
    - Subscribe to any IP service (3rd party or Verizon) that is able to BGP route at least a CIDR /24 for IPv4, CIDR /48 for IPv6 or larger subnet.
- Verizon IP only subnet routing (IPv4:CIDR /25 to /32, IPv6:CIDR /47 to /128) will be announced on the Verizon autonomous system number ("ASN").

- For normal customer routing initiated /24 (IPv6:/48) and Supernet configurations using BGP redirection, DDoS Shield service will assure that the original origin ASN is preserved on its subnet.
- Each circuit protected typically requires a clean traffic return. This may be via Generic Routing Encapsulation (GRE) tunnel built on the customer premise equipment (CPE). Customers can have as few as one or as many GRE returns as necessary – one per circuit, per carrier is recommended. Verizon IP customers may also elect to utilize Multi-Label Packet Switching Layer 3 Virtual Private Networking (MPLS L3 VPN) as a methodology to receive post mitigation IPv4 traffic over their existing Verizon Internet connection in eligible locations without requiring changes to CPE router configurations.
- Verizon recognizes that customers may have disaster recovery or High-Availability locations (two circuits that load share available bandwidth at a specific location). Each Circuit will need a clean traffic return and monitoring configuration to support load sharing and traffic return failover automation. Customers opting for MPLS based traffic return may not combine GRE on the same protected subnet.

DDoS Shield subscriptions may be obtained as either a stand-alone enterprise-wide entitlement **(DDoS Shield)** that may be used with any eligible internet service provider connections (including Verizon) or as a feature to Verizon Internet Dedicated Services **(DDoS Shield for Internet Dedicated Services)**.

- **DDoS Shield** package tiers start as low as 50Mbps normal inbound throughput on the platform; this tier may be consumed using multiple traffic returns (it can protect multiple circuits). As this is asymmetrical traffic mitigation, we need only consider normal inbound traffic volumes. DDoS Shield will help provide customers the peace of mind required to operate their businesses on the open Internet regardless of Internet Service provider used. Customers will receive a fixed monthly invoice based on their own predetermined needs and optional features selected. DDoS Shield package tier utilization is based on 95th percentile clean traffic observed inbound (Mbps) across all protected IP ranges. Verizon does not charge for changes made to the IP circuit configurations. This pricing model is ideal for customers with; many IP services that need to be protected that may not be Verizon IP services; with large IP port capacity typically used for outbound traffic but with lower inbound traffic volumes; that require a single service to cover multiple locations.
- **DDoS Shield for Internet Dedicated Services** can be added as a feature to existing or New Verizon Internet services. The DDoS protection is tied specifically to the Verizon IP service and may not be reconfigured/re-used to protect other IP services. This solution is priced on the IP port speed for the protected Internet service and will be billed as part of the Internet service. This solution is ideal where ingest volumes or other technical details are not known; where contracting and invoicing should match that of the IP service (for example local budgets are used); where Customer requires the DDoS service to match the IP service it protects at all times.

Always Routed Allowance can be optionally purchased in addition to the basic 'on demand' DDoS Shield service listed above, subscribers may purchase as much as is required to allow the constant redirection of some or all of their IP traffic. For example, DDoS Shield package of 1Gbps (1 Gbps p95 inbound clean traffic expected used across multiple protected IP subnets may have up to 1 Gbps of Always Routed Allowance attached). However, if only one protected subnet is required to be 'Always Routed' and it normally flows less than 50Mbps of inbound traffic, only 50Mbps of Always Routed Allowance may be all that is required. Subscription to Always Routed requires a **DDoS Shield** subscription, however customers with both DDoS Shield and DDoS Shield for Internet Dedicated may consume Always Routed Allowance on the IP ranges protected by either service.

Additional/less Always Routed capacity may be added at any time during the DDoS Shield service subscription. The actual IP address subnets that are redirected as Always Routed may be changed as needed to respond to threats seen by simply redirecting the subnet to be protected and using the Portal to inform the SOC that the reason for redirection is Always Routed. This is directly under Customer's control.

5. DDoS service components

DDoS Shield provides near real time analytics of both un-redirected (if detection is configured) and traffic redirected into DDoS Shield which includes detailed views of traffic such as top sources (by IP, country), protocol and top destinations (targets). It also provides detailed review of traffic dropped/passed listed by the countermeasure used.

5.1 Internet circuit or return path

DDoS Shield for Internet Dedicated Services provides attack detection and mitigation for the Verizon Internet Dedicated Service that it was contracted to, using the IP addresses that are routable for that specific circuit for traffic redirection and detection purposes. Traffic redirected may be returned to any configured clean traffic return in the customer's portal account.

DDoS Shield supports traffic routed from any ISP, carrier, provider or data center on the public internet, provided the service subscriber can perform BGP routing changes and can accept clean traffic return. Multi-homed configurations (more than one ISP/IP circuit used to announce the same IP subnets), are fully supported. Customer may change the IP services protected during the service subscription at no extra cost.

5.2 Clean traffic return

The service requires a way to return redirected traffic without using BGP routing that would cause a feedback loop. This can be achieved with either:

- Customer Premises Equipment (CPE) capable of supporting GRE tunneling. This model requires a one-time configuration but supports advanced failover configurations including clean traffic load sharing across multiple IP services.
- an eligible Verizon IP subscription allowing the use of a Verizon configured L3 MPLS tagged VPN, which has the advantage that it requires no CPE configuration and has zero impact on maximum packet sizes.

Verizon's architecture allows all scrub centers globally to participate in the mitigation of the attack without requiring multiple GRE configurations per customer CPE.

Each Clean Traffic Return is constantly monitored for availability to the DDoS Shield service. This requires a one-time configuration to allow test packets to be sent through the tunnel and returned over the Internet, ensuring DDoS Shield is always available when required. Customers may select how sensitive this monitoring is when used to trigger automatic failover.

6. Capacity and service options

6.1 DDoS Shield for Internet Dedicated Services

DDoS Shield for Internet Dedicated Services is a billable feature of Internet Dedicated Services linked to the IP port speed subscribed/consumed, as such any changes to the Internet service will affect the DDoS feature directly. This means that regardless of ingest volumes, the DDoS feature will protect that IP circuits IP port speed. It is assumed that Verizon will be protecting the IP ranges routed to this IP service and (normally) would be returning clean traffic to this location. By default, the service will be configured using The IP services IP ranges, MPLS clean traffic return and with Verizon configured detection and proactive response to attacks enabled. Customers may use the portal to change these defaults at any time after the initial provision.

6.2 DDoS Shield for any ISPs

For ISP agnostic DDoS Shield packages to properly select the correct service tier, a customer will need to answer the following questions:

- How many traffic return locations are needed?
- For each return location, what is the maximum expected good traffic (while in normal use and not under attack) inbound to the circuit?

Each clean traffic return (above the single return included in the DDoS Shield package) will require an Additional Return subscription. For example, if there are two carrier circuits going into the same location (dual homed) or 2 single circuits into 2 separate locations, this will require two traffic returns (1 included in the package + 1 additional).

One common exception is when there are 2 circuits in a disaster recovery/cold spare scenario where both circuit routers will utilize the same routing configuration to the Internet. This would require a single DDoS Shield traffic return configuration.
If GRE is used for clean traffic return (for returning post-mitigation traffic) it is required to provide a publicly routable IP address for the GRE tunnel endpoint. This IP address cannot be a portion of the IP range(s) to be protected by the service, as a routing loop would occur.

Note: it is possible for Verizon IP services to request a separate /30 IP allocation for use for GRE end-points. This provides end endpoints that are not associated with the customer for additional security.

Traffic Returns using MPLS L3 VPN over Verizon's IP network do not require an IP address as normal router configurations are retained.
DDoS Shield subscription tiers are detailed below. All tiers come with 1 single circuit return included, additional clean traffic returns may be ordered to allow the DDoS Shield package to be shared across multiple locations.

- Maximum of 50 Mbps clean inbound traffic
- Maximum of 100 Mbps clean inbound traffic
- Maximum of 500 Mbps clean inbound traffic
- Maximum of 1000 Mbps (1Gbps) clean inbound traffic
- Maximum of 2000 Mbps (2Gbps) clean inbound traffic
- Maximum of 5000 Mbps (5Gbps) clean inbound traffic
- Maximum of 10000 Mbps (10Gbps) clean inbound traffic

The Mbps is the 95th percentile inbound traffic routed to protected IP & IP services combined, measured using detection data (specifically SNMP). Verizon will measure and monitor the volume of total traffic in the DDoS Shield service tier purchased. Usage in excess of such service tier ("Overutilization") will be provided at Verizon's sole discretion. No service capping or rate limiting of customer traffic will occur during Overutilization but Customer will be contacted to review package options in the event of Overutilization.

Non-Verizon IP services that are protected for mitigation as part of the package, that are not configured with detection (specifically SNMP) will be considered to be using 10% of their maximum port speed for the purposes of overage calculation.

6.3 Mixed services

Customers may subscribe to DDoS Shield for Internet Dedicated Services and DDoS Shield at the same time but may not have the same Verizon Internet Dedicated Service configured in both. Customers may access both services from the same DDoS Shield portal account. This is particularly useful when an ISP agnostic service is required for multi-tenant type applications (such as critical applications in a datacenter) as well as protection needed for office locations that may only have Verizon Internet services. Traffic observed/ingested for DDoS Shield for Internet Dedicated Services will not be included in calculations for DDoS Shield utilization.

6.4 Always routed allowance

In addition, any DDoS Shield package may be enhanced with a subscription for the Always Routed feature, which permits protected subnet(s) to be constantly routed through Verizon's DDoS Shield scrubbing centers, where filtered mitigation will be applied constantly. Filtered mitigation will apply Verizon's default Anti-DDoS policies plus any white list, black list and custom filters that may have been created by the customer in the portal.

Verizon will observe Customer's configuration settings for incident response on Always Routed subnet. For example, if an Always Routed subnet is configured as 'Customer permission needed' has an attack incident, Verizon would wait for customer approval before adding further countermeasures. If the subnet is configured for 'Proactive or Algorithmic response' Verizon will add configurations as countermeasures as required based on the incident data without additional permission from Customer.

The Always Routed service subscription may be modified at any time during the DDoS Shield service term. Always Routed tiers are 50Mbps, 100Mbps, 500Mbps, 1000Mbps, 2000Mbps and 5000Mbps. Larger capacities may be available on application. Utilization is measured as the 95th Percentile traffic returned to Customer for all Always Routed redirections while no Attack incident is observed. As soon as an Attack incident is observed on an Always Routed subnet, Verizon will no longer count that traffic towards Always Routed utilization.

6.5 Service support

Every customer will have access to Verizon's Security Operations Center (SOC) team from the moment the service activation begins through any essential ticketing escalation, and of course during the mitigation of any DDoS attack. The Verizon SOC will support the customer's NOC. All administrative changes will be performed via standard ticketing that is available on the Portal, a platform that allows all Verizon Security service subscriptions to be accessed, viewed and administered centrally. While support during security incidents is 24x7x365, support for testing and service

modification (other than self-service features) is limited to standard business hours at US Eastern Time.

7. Mitigation technology

Verizon's DDoS Shield mitigation capacity is built with a combination of Verizon technology supplemented by industry leading technology to combat massive and sophisticated DDoS attacks. The use of internal developed and best of breed commercial technologies gives strength against zero-day type vulnerabilities and attacks. The service leverages a combination of devices that are either purposely built or specifically configured to handle large-scale attacks through anomaly recognition, protocol analysis, and dynamic filtering capabilities. Multiple devices are paired together within each mitigation node, and these nodes are geographically dispersed within a distributed architecture.

Ultimately, Verizon's DDoS Shield relies on a combination of scalable engineering, quality hardware, and highly experienced operational staff to manage the complexity of co-mingled good and bad traffic at extreme loads compared to any normal networking environment.

Benefits of incorporation of these elements into the design of DDoS Shield include:

- Local and global redundancy between our hubs;
- Highly optimized traffic routing within the backbone, intercepting redirected traffic closest to its source using Global Any-cast;
- High-capacity architecture with multi-Terabit support capacities;
- High scalability for assured future growth capabilities.
- Large scale connectivity through both the Verizon Digital Media Service network and directly to Verizon's global Internet backbone allows huge scale, yet also Verizon IP specific features to make use of the service easier and more transparent without a trade-off between the two features.
- The support of two distinct mitigation layers:
    - Filter policies which cater for most attacks and allow near real time configuration from the portal to minimize false positives in mitigation. Filtered mitigation is tunable, testable and will have a known impact on traffic routing through DDoS Shield. All traffic routed though DDoS Shield receives these filters whether for Attack incident or Always Routed Allowance traffic.
    - Elegant, the use of fully managed in-house and vendor technologies to refine and tune out attacks based on evidence of specific attack vectors. Elegant countermeasures require more monitoring and review, they are only applied during an attack incident and will be removed once the attack ends.

7.1 Customer Premises Equipment (CPE)

The Internet access router or other device within the customer's CPE must support GRE tunneling or have a Verizon IP service subscription supporting the MPLS tagged return method, which negates the need for any CPE router configuration.
Where GRE is required, Verizon has engineered their solution to avoid the need for multiple GRE configurations on each protected router yet traffic from all DDoS Shield nodes can still be returned, thus full mitigation capacity is provided.

These are the only methods used by Verizon to return filtered traffic back to the protected network. GRE has been selected for multi IP circuit/ISP configurations as it is a commonly supported protocol on a variety of routers and devices and can support features like load sharing over multiple circuits.

To provide analytics, attack detection and any form of proactive response to attacks, Verizon must be able to process SNMP and IPFIX NetFlow data on normal route path traffic before it is redirected into DDoS Shield. In most cases for Verizon IP services, we can collect this directly from the Verizon network. For third party ISP services, a one-time CPE configuration will be required to allow the export of sampled IP metadata into DDoS Shield. This is optional, but is a requirement for detection and Verizon's proactive response to attacks. The data collection is IPFIX netflow and read-only SNMP.

7.2 Resource exhaustion attacks

Verizon DDoS Shield is a Cloud based TCP/IP (ISO layer 3 and layer 4) mitigation service. Resource exhaustion attacks (ISO layer 5) are not fully supported. There is no monitoring of any resource use on a customer premise equipment, such as a web server, but if the customer's NOC can identify a specific volumetric attack threat (via a regex header) showing which packet type is impacting their premise-based server, Verizon will attempt to mitigate the resource exhaustion attack.

7.3 Mitigation in a multi-homed environment

DDoS Shield for Internet Dedicated Services can only be configured to mitigate attacks against the Verizon IP service it is attached to. DDoS Shield can be used in single or multiple location scenarios and can be configured to protect multiple Internet connections at each location, regardless of the IP providers used. There are no restrictions on the number of traffic return tunnels that can be subscribed to in the service platform for each package. Each clean traffic return is monitored individually with reports appearing within the DDoS Shield Portal to give a single view on all protected subnets, regardless of the IP carrier used.

The relationship between the IP subnets being redirected and the clean traffic returns is controlled within the portal allowing direct control over self-service or automated:

- Switching between primary and failover traffic returns
- Geographic failover between sites
- Load sharing return traffic between multiple GRE return tunnels

8. DDoS Shield user interface

DDoS Shield service subscriptions include access to a web-based portal that provides a variety of functions key to the service with high levels of near real time automation. The portal is secure and requires two-factor authentication to access.

8.1 DDoS Shield service portal

DDoS Shield service subscriptions include access to a web-based portal that provides a variety of functions key to the service with high levels of near real time automation. The portal is secure and requires two-factor authentication to access. Once authenticated, customers will be able to navigate to a dedicated DDoS Shield section.

The DDoS Shield service portal supports traffic analytics and service configuration, including many real time features such as reporting an attack and service reporting. It is also a primary interface with the DDoS SOC team. The portal allows both DDoS Shield for IDS and DDoS Shield services to be configured/managed in a combined policy.

The portal may be used to start, stop, or amend traffic redirections and to configure the self-service filter policies that will be enforced on all redirected traffic in near real time. The portal provides a constant review of service health including BGP peers, tunnel status and details of any on-going incidents/traffic redirections.

Before traffic redirection, the portal may be used to show analytics of inbound traffic and can provide alerts on suspected DDoS attacks as they emerge. The portal can be used to configure the response to attack incidents (i.e. wait for Customer to trigger/request redirection or to pre-approve Verizon to act upon any incident directly). During any redirection, the portal will display near real time inbound, mitigated and returned (forwarded) traffic totals and top talkers/top inbound attacking IP addresses.

The homepage view displays all relevant information for a customer in one screen, providing call outs for action and acts as a launch pad into more detailed, searchable views of traffic analytics and a timeline of activity as well as more detailed configuration screens.

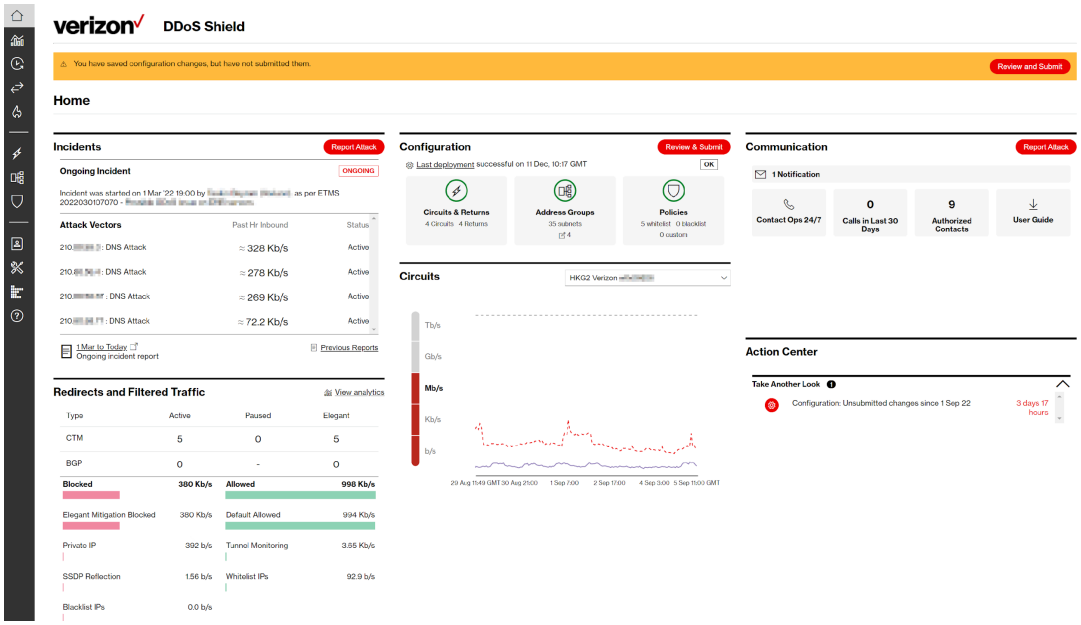

Figure 2: DDoS Shield Service Portal

9. Implementation

Implementation methodology for DDoS Shield (which may support multiple circuits including non-Verizon IP solutions) and DDoS Shield for Internet Dedicated Services will vary.

9.1 DDoS Shield for Internet Dedicated Services

After adding DDoS Shield for Internet Dedicated Services to a Verizon Internet service, Verizon will use data known for the IP service to validate that it is eligible for a default initial configuration to provide a working solution tailored to the IP service without additional information collection where possible. This initial configuration can be changed at any time by Customer once the service has been provisioned to enable more advanced features. The initial configuration will include:

- Configuration to protect the IP addresses associated with the protected IP service
- Use of Verizon network data for detection of attacks/analytics
- Use of MPLS clean traffic return as a method
- Enrolment for Proactive Response to DDoS attacks with Operations review
- Global redirection policy

Where the IP service configuration requires clarification (for example we detect that the same IPs are routable to 2 IP services), Verizon will be in contact to clarify your requirements.

When Internet Dedicated Service orders require a circuit installation, DDoS Shield for Internet Dedicated service configurations will commence only when the IP service is provisioned.

9.2 DDoS Shield

After subscribing to DDoS Shield, Verizon's installation group will engage to gather required configuration information. Verizon will help correct any identified errors in the information collected via an email exchange.

To complete installation, it is necessary to provide the following information:

- A location name for each clean traffic return tunnel; e.g. Carrier 1 NYC, Carrier 2 Chicago. This is intended to be a meaningful name or label to identify the location.
- The IP address of the tunnel endpoint on the applicable CPE (GRE based returns only. **Note**: This cannot be within a protected CIDR. If a protected IP address is used then a routing loop would occur.
- A CIDR, subnet or list of subnets to be announced from each location. For ISP agnostic services, this will be a minimum /24, or Class C subnet, its BGP neighbor address, Autonomous System Number (ASN), and if desired its MD5 keys); this is the CIDR to be protected.
- While the CIDR block does not have to be Provider Independent (PI), if the circuit ISP's IP space is used, the subscriber will be required to offer a Letter of Authorization (LOA) from their ISP permitting the BGP redirection into the DDoS Shield environment.
- If there are multiple GRE returns present and the same /24 is announced from more than one tunnel, a weighting on the announcement will be requested. If none is given, each return will be weighted equally. This may be altered after implementation by opening a change ticket. Mixing MPLS and GRE return methods for the same subnets is not supported.

If required, Verizon will reach out to obtain clarification and to request modification of the configuration submission prior to completing the service implementation.

Once implementation is complete, Verizon will perform validation testing to verify DDoS Shield service configuration is operational and ready to receive/return redirected traffic (pending any configurations required on Customer premise/network) and a welcome letter will be sent indicating that DDoS Shield is ready for use and is billable. **Note**: DDoS Shield is not linked to any specific IP service so may be used to protect any eligible service. Changes made to support different Circuits/ISPs are not chargeable.

Customers are strongly advised to conduct testing with the objective of confirming that traffic can be routed into the DDoS Shield service and returned at any time once the service has been implemented. Verizon recommends that this testing is done periodically.

9.3 Support

As providers of one of the world's largest publicly routable networks, a long-established security services provider and one of the earliest global providers of network based anti-DDoS solutions, Verizon has a wealth of experience to match the network capacity of the service. A DDoS Shield subscription provides 24x7 access to the Verizon's Operations teams who have unrivalled experience and visibility into DDoS threats.

Customers may reach these teams of highly-skilled professionals either electronically by submitting a trouble ticket through the Security Service Portal or via 24x7 support numbers provided at service initiation.

9.4 Service Level Agreements (SLAs)

Verizon offers comprehensive remedies-based Service Level Agreements (SLA) that demonstrate our commitment to providing and maintaining the highest levels of service. These range from delivery SLAs to service availability at 99.999%. Please see your Verizon Account Team for details.

9.5 Billing

DDoS Shield utilizes a flat, monthly recurring billing structure that is based on subscribed service tier package and optional services selected for the package. DDoS Shield is billed on a monthly basis in arrears.

There are no surcharges for DDoS attack traffic volume mitigated by the service or on the number of redirections required to mitigate attacks. However, Verizon will measure and monitor the volume of total traffic in the DDoS Shield service tier and utilization of the Always Routed service, if purchased. Traffic mitigated during an attack does not count towards any Always Routed allowance. Usage in excess of such service tier ("Overutilization") will be provided at Verizon's sole discretion. Verizon may, however, request adjustment to the correct tier.

10. Testing the service

It is good practice to perform operational readiness tests by coordinating with the Verizon SOC. The temporary redirection allows confidence that, in the event of an attack, traffic will be routed to and delivered back from the DDoS Shield scrubbing centers and that any predefined whitelist, blacklist or custom defined filter policies work as expected. Verizon should be notified of the reason for the redirection (test) using the portal or by calling the SOC. While testing is encouraged, launching a DDoS attack over the Internet of any form to test DDoS Shield is strictly prohibited. This will violate Verizon's Acceptable Use Policy (AUP) or the AUP for any other Internet providers affected. In many geographies, launching a DDoS attack on the public Internet may be illegal regardless of the purpose.

Operational readiness test

We encourage you to be ready to use DDoS Shield	You may not perform load testing	Verizon
• Perform operational readiness tests • Activate DDoS Shield (announced or unannounced via portal 'click to Mitigate') at least twice per year	• Load testing companies use the same resources and tools as active attackers to launch what is essentially a DDoS attack which is prohibited in most legal jurisdictions.	• We perform extensive load testing and hardware review in controlled lab environments to simulate real-word attacks.

Verizon performs full regression and load testing of all network-based hardware and software used in the operation of DDoS Shield.

11. Responsibilities before and during an attack

You control	Verizon controls	During the attack

• If Customer elects to use BGP to drive redirection (optional):
  o Your BGP peering status.
  o Your BGP announcement
• For 3rd party ISP connections: Your CPE configuration and IP's to support GRE return, tunnel monitoring, and detection data export
• Your custom filter policy definitions
• Your permissions for Verizon' response to detected attack incidents (proactive response permissions)
• Your authorized points of contact (POCs)
	• Full lifecycle management of DDoS Shield infrastructure
	• 24x7 support for authorized POCs
	• Monitoring of your return tunnel endpoints
	• Collection of IP data to provide detection and analytics
	• Where Proactive response is authorized, review and application of redirections and countermeasures required.
		You must either:
		• Recognize that you are under attack and initiate redirection by contacting Verizon, using portal or using BGP to redirect traffic
		• Pre-authorize Verizon to act upon detection alerts to mitigate attacks as they occur.
		• During the attack window, you must respond to requests for information from the SOC.