VERISIGN™

WHITE PAPER

VERISIGN® DDOS PROTECTION SERVICES

IN-THE-CLOUD SOLUTION FOR SCALABLE, RELIABLE, AND FLEXIBLE DDOS MONITORING AND MITIGATION

VerisignInc.com

CONTENTS

AS DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS GROW IN SIZE, COMPLEXITY, AND FREQUENCY, SECURITY ORGANIZATIONS ARE DISCOVERING THAT IN-HOUSE AND PREMISE-BASED SOLUTIONS FOR MONITORING AND MITIGATING DDOS ATTACKS ARE NO LONGER ADEQUATE.

In general, these solutions inherently lack the scalability; 24/7 expertise; and device, network, and geographic diversity that today's DDoS protection strategies require. When delivered by a competent provider, in-the-cloud services are much better equipped to monitor and mitigate current and future DDoS threats.

As the registry operator for some of the Internet's largest top-level domains, Verisign manages more than 60 billion transactions per day and has maintained 100 percent availability of its .com and .net infrastructure for more than 12 years. Verisign also manages two of the world's 13 Internet domain name system (DNS) root servers, a.root-servers.net and j.root-servers.net, which are considered national IT assets by the U.S. federal government.

In the course of managing these vital assets, Verisign has developed a highly effective strategy and state-of-the-art technology for DDoS monitoring and mitigation. This report describes the strategy and technology that Verisign uses to protect not only the critical Internet infrastructure under its management but also the critical assets of its customers. Specifically, this report focuses on Verisign® DDoS Protection Services, a cloud-based solution for DDoS detection, mitigation, and actor attribution. Using this managed service, organizations not only alleviate the cost and complexity of in-house and premise-based third-party solutions, but they also gain tactical advantages that only a trusted, in-the-cloud service can provide.

DDOS GAINING GROUND ON ALL FRONTS

DDoS attacks have become increasingly massive, sophisticated, targeted, and stealthy in recent years and are now part of the mainstream hacker's arsenal. Since 2005, the size of attacks has mushroomed 1,000 percent.[1] Whereas DDoS attacks were once relatively uncommon outside of a few industries, they have now become the bane of organizations and governments of all types and sizes. In a 2011 Verisign-commissioned survey of 225 U.S. IT executives and decision makers,[2] nearly two-thirds (63 percent) of mid- to large-sized organizations reported having experienced at least one DDoS attack in the past year, and 11 percent had experienced six or more. The respondents also revealed that more than one-third of their organizations' downtime in the past year was due to a DDoS attack.

Nearly any individual or group can launch a crippling DDoS attack simply by renting inexpensive botnets or acting collectively to bombard network resources. In many cases, attackers with minimal technical skills can orchestrate attacks, and even relatively small and unsophisticated attacks can have high-profile impacts.

Attack vectors include not only networks and specific devices but also protocols, services, and Internet infrastructure. While botnet-driven brute-force flooding is still the most popular type of DDoS attack, application-layer attacks are the fastest-growing DDoS attack vector.[3] A global survey revealed that 77 percent of respondents had experienced application-layer attacks in 2010.[4] Application-level attacks often operate within an application's (or an application server's) normal

[1] Arbor Networks, Sixth Annual Worldwide Infrastructure Security Report, February 2011, http://www.arbornetworks.com/arbor-networks%E2%80%99-sixth-annual-worldwide-infrastructure-security-report.html.

[2] Merrill Research, Distributed Denial of Service: Finally Getting the Attention IT Deserves, 2011, http://verisigninc.com/en_US/forms/ddosattentionreport.xhtml.

[3] Labovitz, C., Arbor Networks, The Internet Goes to War, December 2010, http://www.dataprotectioncenter.com/antivirus/the-internet-goes-to-war/.

[4] Ibid.

thresholds of activity, making them difficult to detect with threshold-based detection tools. Disturbingly, application-layer attacks increasingly target data center infrastructure.

THE PROBLEM WITH OUTMODED APPROACHES

While many organizations are beginning to address the DDoS threat, they often rely on approaches that lack the capacity and agility to mitigate attacks rapidly—and preferably before they reach those organizations' networks. In addition, they are unable to selectively mitigate risk to allow legitimate transactions to proceed with minimal delay.

As explained fully in the Verisign white paper, *Best Practices for a Rapidly Changing Landscape*, the following measures, when implemented within most organizations, are insufficient to mitigate today's attacks:

- Over-provisioning of bandwidth
- Firewalls
- Intrusion detection system (IDS) devices
- Intrusion prevention system (IPS) devices
- Routers
- Black hole routing
- Reliance on Internet service provider (ISP) mitigation

In actuality, these devices can render networks more susceptible on even the most scalable platforms and can be overwhelmed with moderately sized DDoS attacks. Nearly 49 percent of respondents to a recent IDC survey reported a firewall or IPS outage due to a DDoS attack.[5]

In-House and Premise-Based vs. In-the-Cloud Technologies

Even when organizations have the expertise and proper resources to implement in-house or premise-based technology, the unique nature of DDoS attacks frequently renders these solutions less feasible and less effective than solutions provided by qualified providers of in-the-cloud DDoS protection.

In house – Typically, in-house solutions are effective only for low-level or network-level attacks, and organizations must continually update their technology. In addition, the organization incurs considerable costs related to hardware and over-provisioning.

Third party – Third-party on-premise solutions, for which organizations must deploy hardware in multiple locations, require significant upfront expenditures for hardware and installation, and ongoing maintenance. Depending on the solution design, hardware may be difficult to scale to next-generation attacks.

ISP based – Solutions provided by Tier 1 ISPs are often less than ideal because they are network dependent, may require hardware provisioning, and may be limited in the types of attacks they can mitigate.

Besides the significant benefits of reduced cost and complexity, in-the-cloud DDoS mitigation services provide tactical advantages that other types of solutions cannot. These advantages figure prominently in an effective DDoS monitoring and mitigation strategy.

Upstream location – With in-the-cloud services, packets destined for the organization travel through an Internet monitoring and mitigation center first. This center redirects and mitigates DDoS attack traffic before it reaches the organization's network, protecting availability and performance and obviating the need to over-provision bandwidth as a DDoS mitigation tactic.

Core Internet connectivity – Because in-the-cloud services have core Internet connectivity, they have an inherently higher capacity for traffic and can handle larger attacks than any single organization can handle. In addition, they can use core-routing techniques (e.g., border gateway protocol [BGP]) to more efficiently divert malicious traffic.

Massive bandwidth – Managed services providers can afford to over-provision bandwidth and invest heavily in scalable infrastructure, allowing them to absorb larger attacks than most individual organizations. In addition, the best providers have multiple network operations centers, distributed globally, to ensure redundancy and high availability.

Greater visibility – A standalone organization can rarely match the field of view that managed service

[5] Arbor Networks, Sixth Annual Worldwide Infrastructure Security Report, February 2011, http://www.arbornetworks.com/arbor-networks%E2%80%99-sixth-annual-worldwide-infrastructure-security-report.html.

providers gain by working with multiple carriers, clients, networks, and peers worldwide. This wider view of Internet traffic helps providers accurately distinguish between normal and malicious traffic and more quickly recognize sources of malicious activity.

VERISIGN DDOS PROTECTION SERVICES

Verisign DDoS Protection Services is a scalable, reliable, and flexible cloud-based DDoS detection, mitigation, and actor attribution solution that rapidly and selectively mitigates risk to maintain high throughput rates for legitimate traffic.

Designed to continually adapt to the steadily evolving DDoS threat landscape, Verisign's DDoS Protection Service reflects Verisign's proven strategy for successfully detecting and mitigating DDoS attacks in .com and .net domains for more than 12 years. Its in-the-cloud deployment enables highly scalable always-on monitoring with on-demand mitigation. With this approach, inbound traffic is filtered only in the event of an attack, thereby eliminating filtering-related latency when no attacks are underway. In addition, because cloud-based deployment does not require equipment to be deployed on customer premises, customers save time and money through operational efficiencies, support costs, and economies of scale.

The core set of Verisign DDoS Protection Services consists of monitoring, threat detection, mitigation, and reporting, and is available either as a shared service or a dedicated service. In addition, Verisign is uniquely capable of delivering network performance and security services that complement the DDoS service, including Verisign® Managed DNS and Verisign® iDefense® Security Intelligence Services. The DDoS Protection Services team and its customers can leverage the technology and expertise within these organizations to better understand and mitigate DNS-led DDoS attacks, gain global visibility into DDoS threats, and receive actionable DDoS threat and vulnerability analysis.

Implementation Strategy

In the course of managing critical Internet infrastructure, Verisign has developed a proven strategy for ensuring the transactional availability of its Internet resolution sites in the face of increasingly massive and sophisticated DDoS attacks. Verisign DDoS Protection Services leverages this strategy for its monitoring and mitigation facilities.

The following service features reflect this strategy:

Solution and device diversity – To minimize exposure associated with the vulnerabilities of a single hardware solution or network connection, Verisign DDoS Protection Services uses multiple vendor-diverse, commercial off-the-shelf (COTS) tools for DDoS mitigation, and Verisign's proprietary technology platform (called Athena). This approach allows Verisign to manage a much wider range of attacks than some service providers, successfully mitigate attacks that use new or combined techniques, flexibly scale mitigation functionality based on new attack vectors, and resist zero-day attacks.

Carrier diversity and neutrality – Today's DDoS attacks often direct significant amounts of traffic toward a specific target. For optimum availability and to increase immunity to carrier-specific attacks, each Verisign DDoS mitigation center maintains multiple upstream providers, and numerous peering and backbone connections. The Verisign DDoS Protection Services solution is carrier-agnostic, encompassing all the ISPs within an organization and allowing an organization to change its infrastructure as needed to suit evolving business needs.

Geographic diversity – Verisign maintains fully redundant, geographically separate monitoring facilities to help ensure the continuity of DDoS protection services in the event that operations at a single site fail. In addition, Verisign leverages its strategic relationships with the largest providers of Internet services and data center hosting to globally distribute mitigation centers at some of the world's highest-volume Internet peering points. By scrubbing traffic at major Internet peering points, Verisign can take advantage of bandwidth density and traffic routing options at these points to better manage overall attack loads and flexibly mitigate events either closer to the attack or closer to the target as the situation demands.

Proven scale – Verisign sites are over-provisioned and globally distributed to ensure protection against the largest DDoS attacks. Verisign's globally deployed IP backbone provides access to more than 350 gigabits per second (Gbps) of bandwidth across Verisign scrubbing centers.

24/7 DDoS expertise – Intelligence gathering, threat analysis, monitoring, and mitigation require a seasoned team with a diverse skill set. The Verisign DDoS monitoring and mitigation team is available around the clock to monitor and mitigate events. It has extensive experience in evaluating threat intelligence, configuring and updating systems to recognize existing and evolving threats, organizing and managing traffic reports, distinguishing suspicious traffic from legitimate traffic, dealing with botnets, and managing and defending against DDoS attacks.

Monitoring

Monitoring customer traffic is critical to identifying and mitigating attacks in their infancy. Verisign DDoS Protection Services continually collects Internet traffic flow data (i.e., NetFlow, jflow, Sflow, Cflowd, and read-only simple network management protocol [SNMP] data) from the customer's Internet-connected routers. The service samples only the packet headers of the flow data, not the data in the packet. Header data, which includes source IP, destination IP, source port, destination port, time-to-live (TTL), and transmission control protocol (TCP) flags, is exported to the Verisign DDoS Protection Services correlation engine.

Verisign's correlation engine uses the data in the packet header samples for threat detection, alerts, and reporting. It analyzes and classifies packets by correlating the header data with SNMP and BGP data. This approach allows Verisign DDoS Protection Services to build an intelligent, dynamic baseline traffic profile without deploying any hardware to the customer site. The packets are then categorized and passed through a heuristics engine to separate normal traffic from anomalous patterns.

Deviations from expected baselines generate customer-specific alerts that enable Verisign's monitoring and mitigation team to immediately begin to evaluate and prioritize potential attacks, and coordinate internal and customer escalation plans.

Verisign DDoS Protection Services monitors up to the transport layer. It can also accept monitoring output from the Arbor Threat Management System platform to provide application-layer visibility into attacks.

Threat Detection

Identifying potential threats in their early stages is critical to mitigating them before they can affect an organization. Effective threat detection requires extensive insight into threat intelligence, state-of-the-art mechanisms for identifying threats, and methodical alert and escalation processes.

Global Visibility

Few service providers can match Verisign's global visibility into DDoS threats. It draws on its relationships with network carriers, ISPs, and other network service providers to supplement its threat intelligence. The Verisign iDefense Security Intelligence Services team, which interacts with an experienced multinational network of security experts, provides additional insight into DDoS attack methodologies and operations, including current information on DDoS attack methods, botnets, command-and-control (C&C) hosts, and actors and groups involved in the DDoS threat.

Threat Identification

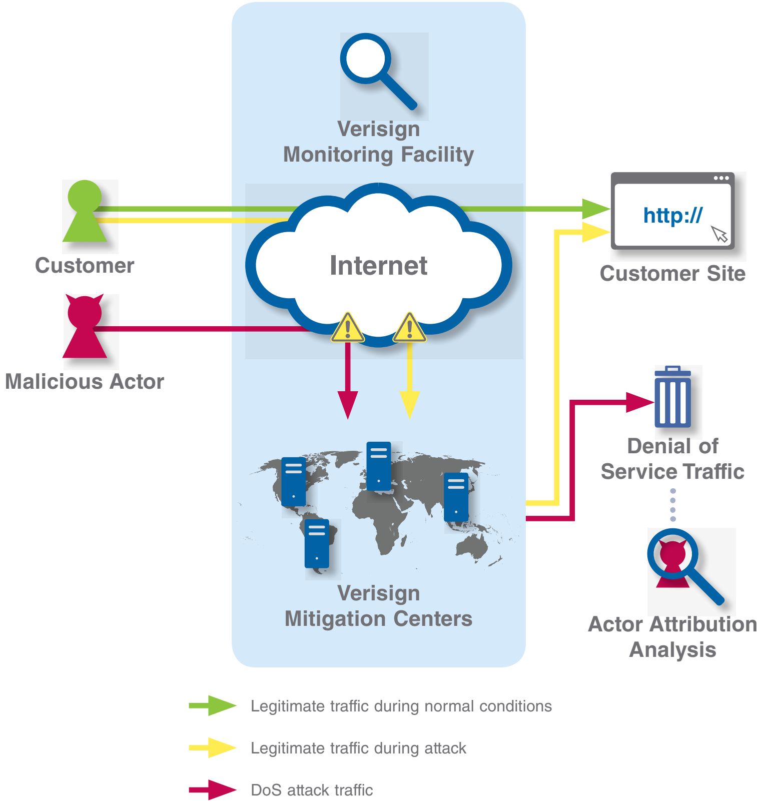
Depending on its source, updated threat information is manually or automatically fed into the Verisign DDoS Protection Services event correlation engine. To identify threats and potential attacks as it monitors a customer's network, the correlation engine relies on two mechanisms:

Signature analysis – Signature analysis, or misuse detection, looks for predefined deviations that indicate a DDoS attack. Verisign uses a combination of industry best practices, proprietary intelligence, and third-party intelligence to identify these signatures. Because attacks are always evolving, Verisign's ongoing research and development incorporates lessons learned from attack mitigation to help identify new threat signatures.

Dynamic profiling – Because all customers are different and attack profiles are changing constantly, it is vital that Verisign understand each customer's "normal" traffic patterns. To do so, Verisign works with the customer to establish—and periodically update—a dynamic profile of its Internet traffic. This profile incorporates both temporal and topological components to produce sophisticated models of network behavior. Then, Verisign applies custom, real-time algorithms to distinguish legitimate traffic from DDoS attacks. Deviations from the established customer profile that exceed pre-defined thresholds automatically activate an alert for Verisign's 24/7 security teams, enabling Verisign to respond quickly to new and one-of-a-kind attack profiles.

Threat Alert and Escalation Process

Figure 1: Verisign DDoS Protection Service Process



Verisign maintains a 24/7 monitoring and mitigation team for Verisign DDoS Protection Services. This team monitors customer environments and traffic data around the clock. When the monitoring platform detects a threat, it sends an alert to the team for real-time review and immediate triage (see Figure 1). To identify false positives and avoid unnecessary mitigation, the team starts by comparing the monitoring data to the previously established operating thresholds of the customer network and correlating any additional alerts regarding the customer website or domain.

If the alert warrants customer intervention, the monitoring team notifies the customer via a predefined escalation path and begins a discussion regarding the next steps. A typical alert call will direct customers to log in to the service portal (discussed in the Reporting section below) so both the customer and the monitoring and mitigation team can view the same information in real time. The Verisign team presents recommendations for mitigation, which can range from basic access control lists (ACLs) and filtering to a full redirection of traffic to a Verisign mitigation site.

During the mitigation process, the Verisign team continues to monitor traffic thresholds and bandwidth levels and analyzes this data to determine whether a more detailed mitigation is required. The team can also engage the Verisign iDefense Security Intelligence Services team to assist in additional forensics analysis and real-time situational awareness, such as monitoring of C&C chatter to identify targets or changes in attack methodology.

Attack Mitigation

The implementation strategy discussed above—device, network, and geographic diversity; proven scalability; and DDoS expertise—is essential for effective attack mitigation in today's rapidly mutating threat landscape.

By combining best-of-breed, off-the-shelf tools with its proprietary monitoring and mitigation platform (called Athena), the Verisign service can agilely handle a wide range of attacks, including high-volume stateless flood attacks (e.g., SYN, UDP, and ACK), high-volume stateful flood attacks (e.g., HTTP and HTTPS), and low-volume stateful flood attacks (e.g., HTTP and HTTPS).

Verisign provisions massive amounts of bandwidth in its mitigation facilities and positions these facilities at major Internet peering points, allowing Verisign to optimize traffic routes and better manage traffic diversion and return paths.

Mitigation consists of three components: off-ramping, filtering, and on-ramping. Because timeliness is critical to protecting customer services, Verisign works extensively with the customer during the initial service setup and testing phases to ensure a seamless implementation of all three components and to establish event mitigation procedures that fit the customer's service model.

Traffic Off-Ramping

Off-ramping occurs when a potential attack warrants traffic redirection to a Verisign mitigation center (e.g., if the customer's website performance has degraded significantly). In this scenario, Verisign DDoS Protection Services diverts Internet traffic that is destined for the customer to one or more Verisign mitigation sites, where traffic is filtered before reaching the customer.

Verisign offers two main methods for off-ramping traffic to a mitigation site:

DNS-based redirection – In this method, the customer points its domain's A record to a Verisign Internet Protocol (IP) address. After scrubbing, the clean traffic is returned to the customer's Web servers as standard Web traffic via the Internet.

BGP rerouting – In this method, Verisign uses BGP routing to swing traffic to Verisign. This method supports a variety of connections, including a generic routing encapsulation (GRE) tunnel, direct cross-connect (for customers in the same co-location facility as Verisign), metro-Ethernet (for customers in the same metropolitan area), a multi-protocol label switching (MPLS) tunnel, or an existing peering connection with Verisign. This method also allows Verisign to globally load balance incoming traffic across two or more Verisign mitigation facilities.

Athena is a large-scale distributed system that identifies, prevents, and adapts to network-related threats. It consists of a collection of fan-out components acting as a load balancer and a multitude of machines running customized proxy software. These machines read and validate incoming requests and are responsible for absorbing massive DDoS attacks. Athena is capable of acting as a transparent proxy, inspecting the validity of HTTP headers, performing regular expression (regex) pattern matching for arbitrary strings, validating active sessions, performing challenge-response processes, and applying other mitigation techniques.

Filtering

As discussed in the Monitoring section, Verisign filtering devices analyze TCP ports, source IPs, source autonomous system numbers (ASNs), destination ports, destination IPs, time to live (TTL), TCP flags, type of service (ToS) to differentiated services code point (DSCP) mapping, packet size, and other packet header data. Because blocking all traffic to a customer accomplishes the same goals as a DDoS attack, Verisign filtering devices use a layered filtering and analysis process that helps legitimate traffic reach its intended destination with minimal delay. This layered verification process enhances rule sets over time so the filtering technology progressively blocks a greater volume of malicious traffic. It also enables Verisign to more rapidly and accurately identify and block complex and changing attacks.

Although some attacks can be mitigated by implementing filters at the Internet layer alone, Verisign applies filters at multiple layers of the TCP/IP stack (see Figure 2) to address complex attacks that require analysis and filtering up through the application layer.

Verisign DDoS Protection Services uses the following traffic analysis processes to filter malicious traffic from legitimate traffic:

Dynamic profiling – This is the first filter that diverted traffic encounters. The system generates this filter based on detailed analysis of the traffic flow. Verisign can also implement a user-configured static filter. Traffic that the filter identifies as malicious is either dropped or subjected to an increased level of verification.

Active validation – When traffic triggers an alert or event, this filter algorithmically challenges the suspicious traffic to determine whether it is legitimate, or whether it is spoofed or a bot.

Anomaly recognition – This filter further inspects traffic thatthe dynamic/static filters or the anti-spoofing filter did not stop. It compares the profiled traffic to the baseline behavior over time, looking for any deviation that would identify the source of the malicious packets.

Application-level and protocol-based analysis – If traffic is within normal baseline parameters, the filtering technology further examines the traffic to identify any application-specific attacks and anomalous protocol transactions. Verisign can also perform regex-type filtering for non-standard protocol types.

IP reputation lists – The service leverages a Verisign iDefense IP list of malicious URLs and domains to selectively filter IP packets from known bad actors. Verisign iDefense updates the IP list daily. The service can also accept customer-specific data, modifications, or requests.

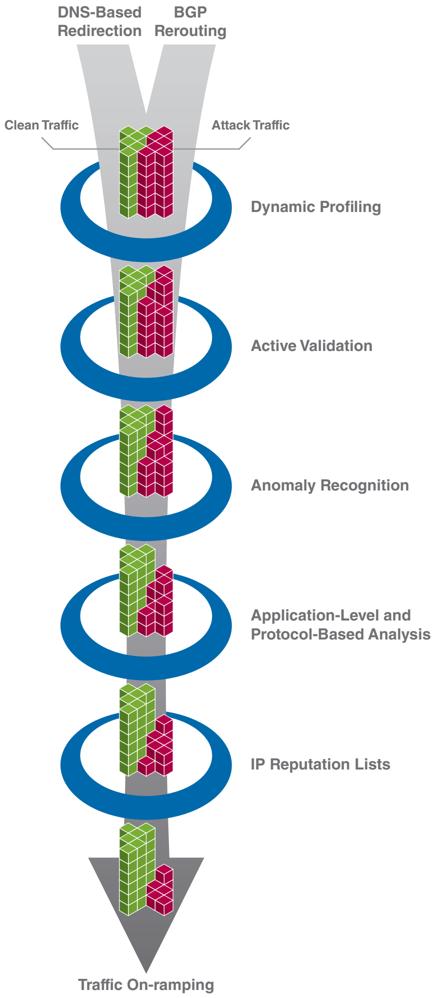
Traffic On-Ramping

Once traffic has been “cleaned,” Verisign redirects it from the Verisign DDoS mitigation center to the customer’s network. Verisign network architects work with the customer to establish the best method for redirecting clean traffic back into its network. Potential redirection methods include generic routing encapsulation (GRE) tunneling, establishing a virtual private network (VPN), or directly connecting to a site.

If off-ramped traffic is redirected via DNS, a customer must point its “A” records to a Verisign IP address and set the TTL to the minimum time for redistribution. After mitigation, traffic is proxied back to the customer.

If Internet traffic is redirected using BGP off-ramping, the customer can either perform the BGP off-ramping itself or direct Verisign to activate the service on its behalf.

Figure 2: Verisign’s DDoS Protection Services Traffic-Filtering Process



SSL and HTTPS Attack Mitigation

Verisign has been mitigating DDoS attacks on HTTPS sessions for some time. In general, Verisign can mitigate HTTPS-based attacks via methods that do not require the packets to be decrypted. However, through a proprietary process, Verisign DDoS Protection Services also enables the encryption and escrow of customer keys in the event that the mitigation process requires decryption, filtering, and re-encryption.

Reporting

Because understanding customer traffic is the first step to making informed decisions, Verisign DDoS Protection Services provides detailed reports on customer traffic statistics. A significant advantage of Verisign DDoS Protection Services is the transparency of service data, which is available via Verisign's secure, Web-based customer portal. By giving customers 24/7 visibility into network traffic, patterns, alerts, and the mitigation process, the portal helps expedite event response and mitigation.

The Verisign DDoS Protection Services portal is a centralized utility that provides customers with the same 24/7 real-time reports that are available to Verisign's DDoS monitoring and mitigation team. It is available in both customer and reseller configurations.

Using the portal, customers can:

- Receive attack alerts
- View bandwidth and traffic graphs in real time
- Track the start time and duration of an attack
- View detailed reports
- Manage escalation plans

The portal's master dashboard includes two main tools:

Active Alert summary – Shows alert(s) status (New, Investigating, Mitigating, or Closed), severity (High, Medium, or Low), total incoming bits per second (bps), and total incoming packets per second (pps). This summary is produced both during an attack and after it has ended. Customers can also use this tool to view the details of specific alerts.

Traffic Graph – Displays a summary of incoming traffic (in bps and pps) at all sites and can be broken down by site, network, application, or protocol.

The Verisign DDoS Protection Services monitoring solution securely stores all time-series header data for traffic reports in its round-robin databases. At the customer's request, Verisign has the ad hoc capability to capture full packet data for forensic analysis during BGP or DNS mitigation. A list of active IPs sending data during the attack is also available. Verisign uses this information to perform post-attack analysis and to enable the iDefense Security Intelligence Services team to determine trends, botnet activity, and attribution services..

CONCLUSION

As the DDoS attack profile continues to change and expand, organizations will need a monitoring and mitigation solution that is highly flexible, reliable, and scalable. An in-the-cloud DDoS protection solution that incorporates proven scalability; 24/7 expertise; and device, carrier, and geographic diversity can usually monitor and mitigate DDoS threats more effectively than in-house or commercial premise-based solutions.

Using Verisign DDoS Protection Services, organizations not only minimize expenditures and complexity but also gain the peace of mind that comes from working with a leader in network intelligence and availability.

FOR MORE INFORMATION

For more information about Verisign DDoS Protection Services, please contact a Verisign representative at 1-866-200-1979 or 1-703-376-6905, or email ddos@verisign.com.

ABOUT VERISIGN

Verisign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

VerisignInc.com