



DATA SHEET

VERISIGN® INTERNET DEFENSE NETWORK OVERVIEW

The increasing frequency and severity of Distributed Denial of Service (DDoS) attacks is rapidly changing the face of network security. Driven by financially, politically, or technologically-motivated criminals, these attacks routinely exceed the largest events of only a few years ago. Stopping them at organizational network borders has become an expensive and often ineffective solution. As a result, DDoS mitigation has become one of the top security issues for any organization conducting business online.

The VeriSign® Internet Defense Network provides organizations with a reliable and scalable DDoS protection strategy. As a trusted partner, VeriSign helps companies stay online without having to invest in the massive infrastructure to do so.

DDOS ATTACKS: A GROWING THREAT

DDoS attacks intentionally deprive legitimate users of Internet resources, typically by overloading a network with a flood of data packets from multiple sources. Attackers usually create the Denial of Service condition by either consuming server bandwidth or by impairing the server itself.

Today, malevolent actors are enlisting the help of compromised computers to form “botnets” capable of launching major attacks against unsuspecting victims. Estimates suggest that anywhere between 4 and 6 million computers are actively used in botnets at any time. These botnets harness the processing power and bandwidth of thousands of compromised computers to bring down the largest and most sophisticated networks. Some reports estimate that more than 10,000 attacks occur each day with many ISPs reporting attacks in excess of 10Gbps.

OVERVIEW

The VeriSign Internet Defense Network helps protect organizations from catastrophic DDoS attacks by detecting and filtering malicious traffic aimed at disrupting or disabling Internet-based services. Unlike traditional security solutions, the VeriSign Internet Defense Network filters harmful traffic upstream of the organizational network or, In-the-Cloud.

The VeriSign Internet Defense Network combines the security from VeriSign’s world-class traffic analysis and detection platforms with the flexibility of utilizing the mitigation components only when required. When an event is detected, VeriSign will work with the customer to redirect Internet traffic destined for the protected service to a VeriSign Internet Defense Network site. The redirection happens “In-the-Cloud” to swing attack traffic to the Internet Defense Network site before it can overwhelm or otherwise harm the customer network. As VeriSign monitors and analyzes traffic pattern data, the 24x7 security team begins “scrubbing” redirected traffic through the use of world-class mitigation technologies. Malicious traffic is progressively blocked while filtered traffic is sent to the customer’s network, thus helping them sustain normal business operations.

KEY BENEFITS

Massive Capacity and Scalability
Sites are over-provisioned and globally distributed to protect against the largest DDoS attacks.

Global Peering Relationships
Our relationships with carriers, ISPs and other network service providers around the world provide an additional level of threat intelligence.

24x7 Management, Monitoring and Support
VeriSign security analysts are available 24x7 to identify and mitigate events.

Lower Costs
Since no on-premise equipment is required, customers save time and money through operational efficiencies, reduced support costs, and economies of scale.

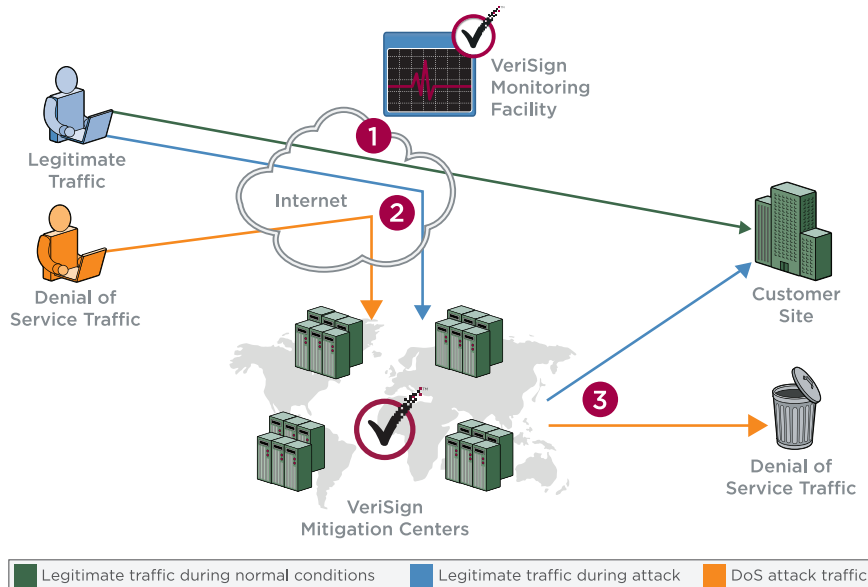
Trained and Dedicated Professionals
Certified security professionals undergo extensive training and rigorous background checks.

Responsiveness
Customer-specific escalation procedures are designed to detect, identify, and mitigate issues.

Progressive Filtering
VeriSign network teams work with the customer to adjust filtering levels. As attack vectors are more clearly identified, VeriSign filtering becomes more comprehensive.



How the VeriSign Internet Defense Network Works



KEY FEATURES

- Always-On Monitoring
 - On-Demand Mitigation
 - Easy set-up and configuration
 - Choice of DNS or BGP traffic off-ramping
 - Tunneling, VPN, or Direct Connect* traffic on-ramping options
 - Detailed event reporting and analysis
 - Secure customer portal
 - Requires no Customer Premise Equipment**
- * Available in certain areas
** If VPN is not required

SERVICE COMPONENTS

Monitoring

Monitoring customer traffic is critical to identifying and mitigating attacks in their infancy. VeriSign collects traffic flow data from the customer's Internet-connected routers. Samples of the customer's Internet traffic are incorporated into VeriSign's correlation engine for threat detection, alerts, and reporting. The frequency of packet sampling can be tailored based on customer size, type, and router performance.

Packets are classified and analyzed by correlating a number of fields contained in the headers of the sampled packets. The packets are then broken down into categories and correlated using advanced heuristics to profile normal versus anomalous traffic patterns.

Customer Traffic is monitored by VeriSign's 24x7 Security Operations Center. Customer-specific alerts enable trained security experts to immediately identify nascent potential attacks. Additionally, customers can monitor their own traffic and alerts via a secure online portal.

Threat Detection

Identifying potential events in their early stages is critical to mitigating them before they can impact organizations. As such, VeriSign continually looks for new methods to identify and classify malicious activity. Threat detection is comprised of two primary components: Signature Analysis and Dynamic Profiling



- **Signature Analysis** - Signature analysis, or misuse detection, looks for predefined deviations that are signs of a DDoS attack. VeriSign uses a combination of industry best practices and proprietary intelligence to identify these signatures. Since attacks are always evolving, lessons learned from mitigating them feed into ongoing research and development to help identify new threat signatures.
- **Dynamic Profiling** - Because all customers are different and attack profiles are constantly changing, it is vital that VeriSign understand each customer's "normal" traffic patterns. To do so, VeriSign works with the customer to establish a dynamic profile of its Internet traffic. Deviations from the established customer profile that exceed pre-defined thresholds automatically activate an alert for VeriSign 24x7 security teams, enabling VeriSign to respond to new and one-of-a-kind attack profiles.

Mitigation

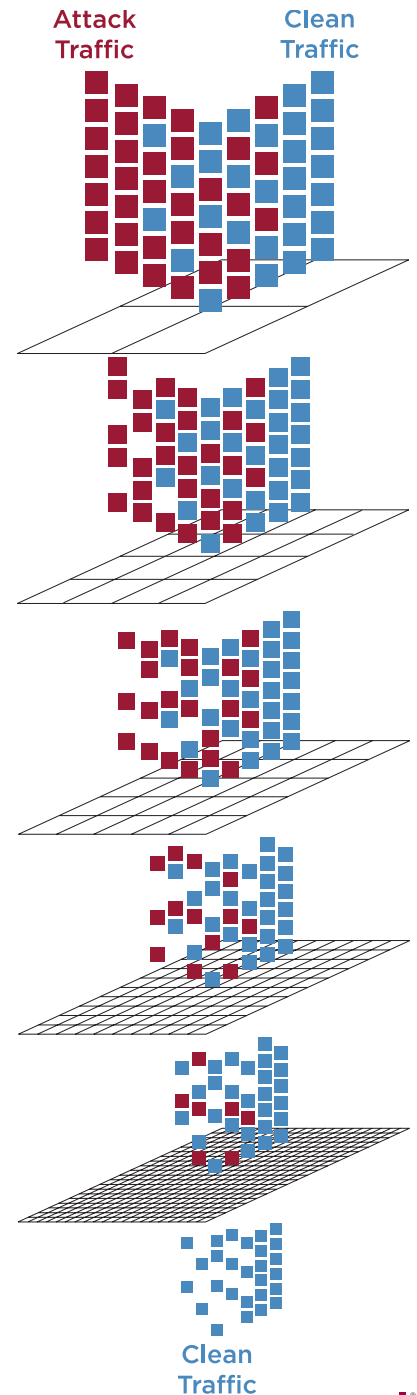
VeriSign establishes event mitigation procedures with the customer to fit their service model. Mitigation is comprised of three components: Off-ramping, Filtering, and On-ramping. Because timeliness is critical to protecting customer services, VeriSign works extensively with the customer during the initial set-up and testing phases to ensure a seamless implementation of all three components.

- **Off-ramping Traffic** - VeriSign security experts redirect Internet traffic destined for the customer service "In-the-Cloud" to VeriSign Internet Defense Network sites, so the traffic reaches VeriSign first. Off-ramping occurs when a potential attack warrants traffic redirection.
VeriSign offers several methods for off-ramping traffic, including BGP announcements or changes to customer DNS records. Optimal solutions vary by customer and depend upon the size of the customer network, the types of services they utilize, and a host of other considerations.
- **Filtering** - VeriSign employs a layered approach to traffic filtering that progressively enhances rule sets over time. Since blocking all traffic to a customer accomplishes the same goals as a DDoS attack, VeriSign helps legitimate traffic reach its intended destination. Over time, state-of-the-art filtering technology increases the level of filtering to progressively block more malicious traffic.

Filters are applied at various layers of the OSI stack. Although some attacks can be mitigated by implementing filters at the network layer, complex attacks now require analysis and filtering up through the application layer. VeriSign is able to complement commercially available products with custom, in-house development to create a world-class DDoS mitigation solution.

- **On-ramping Traffic** - Once traffic is "cleaned," VeriSign redirects it from the VeriSign Internet Defense Network site 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, such as GRE tunneling, establishing a VPN, or directly connecting to a site.

A LAYERED APPROACH TO FILTERING





Reporting

Because understanding a customer's traffic is the first step in protecting critical services, VeriSign provides detailed reports on customer traffic statistics to enable informed decisions. Examples include traffic summary reports, application reports, protocol reports and event reports.

SUMMARY

As malicious actors relentlessly pursue new means to sharpen their craft and avoid detection, the threats to organizational networks grow exponentially. Botnets composed of hundreds of thousands of compromised devices provide the foundation for tools that can inflict devastating attacks that not only impact revenue but damage company reputations and reduce customer confidence. Simply stated, threats are evolving at an extraordinary rate – and so too must security solutions.

The VeriSign Internet Defense Network is a product of this security evolution. By mitigating threats closer to the core of the Internet, VeriSign is able to effectively and efficiently mitigate some of the world's largest attacks. At the same time, VeriSign is able to quickly react to defend against the rapidly changing environment. As a proven leader in protecting critical Internet infrastructure, VeriSign now provides that experience and technology to help organizations guard their own Internet assets.

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. Visit us at www.Verisign.com for more information.

LEARN MORE

For more information about the VeriSign® Internet Defense Network, please contact a VeriSign representative at InternetDefenseNetwork@Verisign.com, or visit us at www.Verisign.com/vidn.

