VERISIGN®

HANDBOOK

VERISIGN DDoS PROTECTION SERVICES CUSTOMER HANDBOOK

CONSIDERATIONS FOR SERVICE ADOPTION

Version 1.0 | July 2014

VerisignInc.com

CONTENTS

1. WHAT IS A DDOS PROTECTION SERVICE?

As more and more businesses have moved their business operations online, the Internet has become an attractive place to conduct disruptive and criminal activities. Cyber criminals are increasingly using distributed denial of service ("DDoS") attacks as the tool of choice to wreak havoc to online operations.

An attacker uses a DDoS attack to direct a large amount of traffic at a business's online resources (such as websites) with the intent of rendering those resources unreachable or unusable. "Distributed" refers to the fact that DDoS attacks use multiple – often hundreds and into the millions – of computers or servers to create and send these large amounts of traffic. Attackers can employ these machines voluntarily – often coordinating via social media and/or underground channels – or involuntarily through malware infection or other compromise. Regardless of the method employed, the result is the same: an overwhelming amount of traffic flooding your network, thereby impeding your visitors' access to your online resources, such as your website or other services.

WHAT YOU SHOULD KNOW ABOUT DDOS PROTECTION

DDoS attacks continue to emerge as a growing threat to online business continuity and security. In the last few years, DDoS attacks have significantly increased in size, frequency and complexity, creating a significant challenge for any business trying to protect its online presence and business reputation.

With the rapid changes in DDoS attacks today, traditional defensive tactics such as bandwidth over-provisioning, firewalls and intrusion prevention system (IPS) devices alone are no longer sufficient to protect your critical networks and services. For example, a volume-based DDoS attack can overwhelm your networking equipment and disrupt services at your website within a matter of minutes by simply sending an abnormally large amount of traffic to the targeted website.

Protecting your business from this evolving threat requires equally sophisticated technology to intelligently distinguish legitimate traffic from attack traffic and mitigate the DDoS threat. An effective DDoS protection solution is one that can filter attack traffic "in the cloud" before it reaches your network and overwhelms any on-site equipment.

2. HOW CAN VERISIGN HELP?

Verisign has extensive experience both in managing and maintaining the availability of critical infrastructure in spite of threats of ever-increasing scale and sophistication. Having long protected the .com and .net infrastructure from DDoS attacks, Verisign has provided DDoS monitoring and mitigation to commercial customers since 2008. The Verisign DDoS Protection Service provides the anti-DDoS expertise, global infrastructure and innovative technology to help organizations like yours guard their Internet assets and restore critical services in the event of a DDoS attack.

The Verisign DDoS Protection Service uses a software-as-a-service ("SaaS"), or "in-the-cloud" solution that provides scalable, cost-effective protection against DDoS attacks by detecting and filtering malicious traffic aimed at disrupting or disabling your Internet-based services. Verisign's cloud infrastructure is scaled to deal with some of the largest known DDoS attacks, comprising globally distributed protection sites, extensive peering and a fully resilient, interconnected network backbone.

A SaaS model allows enterprises to access technology and other resources on a distributed network that is owned and maintained by the SaaS provider and shared among users. Some of the benefits of the SaaS model include:

- You do not have to purchase, maintain or support hardware or software.
- Deployment is easy and fast.
- Cost savings are usually significant because the platform is shared among customers.
- Organizations can access the service on a global and on-demand basis.
- SaaS infrastructure is often redundant, massively scaled and has reliability and recovery built in.
- The subscription fee often includes customer support and service-level agreements.
- SaaS infrastructure may offer high security, typically featuring world-class data centers, state-of-the-art HVAC and security controls.

WHAT YOU SHOULD KNOW ABOUT THE SERVICE COMPONENTS

The Verisign DDoS Protection Service is composed of two primary components: Proactive monitoring and on-demand mitigation.

Proactive Monitoring

A service that monitors network traffic for indicators of DDoS attacks is critical to identifying and stopping attacks as quickly as possible. The Verisign DDoS Protection Service monitors your traffic 24/7 by periodically collecting information about the traffic traversing your network for analysis. This information typically includes:

- Where traffic is coming from and going to
- What type of traffic is traversing your network
- Which hosts and networks are communicating with your network

Verisign works with you to understand your organization's normal traffic patterns. When the Verisign DDoS Protection Service monitoring platform identifies traffic pattern anomalies, the service automatically alerts the Verisign Security Operations Center for investigation and response.

On-Demand Mitigation

Verisign's on-demand DDoS mitigation protects against DDoS attacks aimed at your network by redirecting traffic to a Verisign DDoS protection site in the cloud for further analysis only in the event of an attack. On-demand mitigation helps minimize the risk of collateral damage, latency or other negative impacts on your website and other services during normal operations. Redirection of traffic typically happens within minutes and, in turn, helps prevent DDoS traffic from overwhelming or otherwise harming your website, other services and/or network equipment.

As Verisign further inspects and analyzes traffic-pattern data, the Verisign DDoS Protection Service team begins filtering the traffic using diverse mitigation technologies. Experienced Verisign engineers use multiple layers of proprietary and commercial technology within our DDoS protection centers to distinguish good traffic from attack traffic. The mitigation process is designed to ensure that the impacted services at your site experiences minimum downtime or performance degradation due to the attack.

Attack traffic is progressively blocked while legitimate traffic is sent through to your organization's network, thus helping you sustain normal business operations. Traffic re-direction back to your network is available via BGP, DNS, GRE tunnels and direct connections into our network.

24x7 Reporting

Verisign provides you with access to a secure, Web-based portal, where you can view your monitored network traffic patterns, DDoS alerts and the mitigation process in near-real time with detailed reports and statistics.

Optional Always-On Hybrid DDoS protection

Through a relationship with one of our technology partners, you may also purchase on-site, CPE-based DDoS protection which can be integrated with the Verisign DDoS Protection Service. This hybrid option is suitable for customer environments that host extremely latency-sensitive applications or specifically require on-premise layer-7 DDoS protection.

3. HOW IS THE SERVICE SET UP?

Since the Verisign DDoS Protection Service is cloud-based and does not require you to invest in any additional infrastructure, Verisign can set up the service quickly, provisioning the monitoring and/or mitigation components to meet your requirements.

WHAT YOU SHOULD KNOW ABOUT THE SET UP PROCESS

The Verisign Customer Support team will work with you to carry out service setup in four steps (see figure 1):

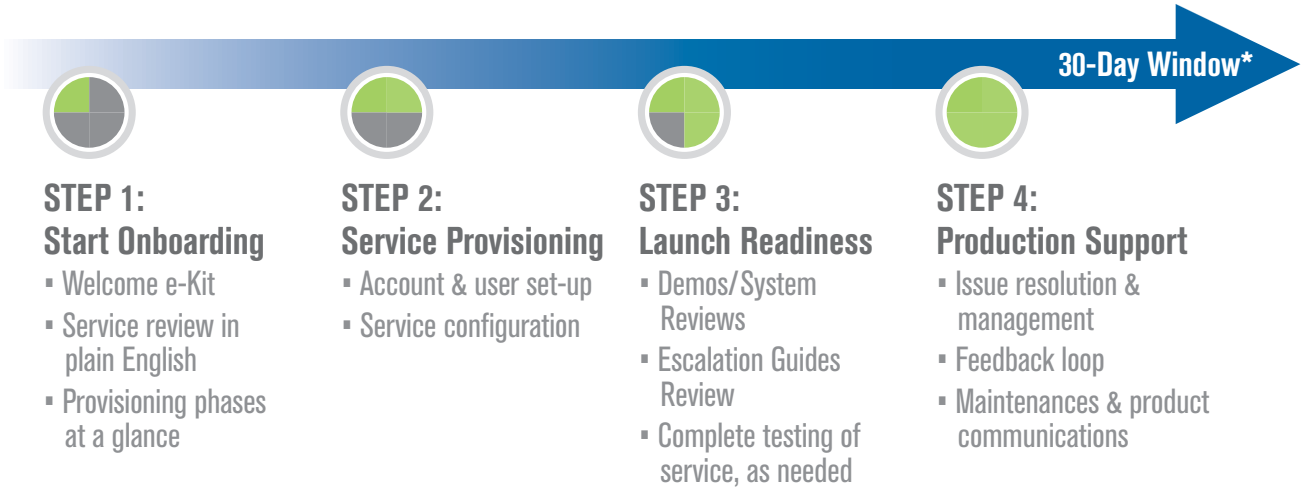

Figure 1: On boarding Milestones

Step 1: Start Onboarding

Onboarding begins with an electronic welcome kit, giving you in straightforward terms, the services that will be provisioned, how to access help 24x7 and how Verisign manages customer issues to resolution.

Step 2: Service Provisioning

As part of the provisioning process, a Customer Support engineer will set up customer accounts within its management interfaces and work with customers to ensure the DDoS Protection Service is configured properly in both the customer's and Verisign's environments, and that it is ready to begin protecting against DDoS attacks.

Step 3: Launch Readiness

Verisign recognizes the need for service testing to ensure that our service is adequately integrated with the customer's network. As part of the onboarding process, customers will have a defined and comprehensive service testing period as part of the service. In addition, Customer Support provides demonstrations of the service management console and an overview of escalation management processes to prepare your organization for the Production Support phase.

Step 4: Production Support

Upon successful integration testing, your organization will transition into the Production Support phase, where the same engineering team that helped you configure and set up the service will manage all inquiries to closure. Verisign's support team not only supports you through the issue-resolution process, but also proactively solicits your feedback and works with you to understand how we can improve the DDoS Protection Service.

4. WHAT HAPPENS DURING AN ATTACK?

When the Verisign DDoS Protection Service monitoring platform identifies traffic pattern anomalies, the service automatically generates and sends an alert (or set of alerts) to the Verisign DDoS mitigation teams for investigation and response. Verisign immediately contacts you via telephone or email as set forth in your escalation plan, and you can also view and track these alerts in near-real-time in the Web portal.

Prompt mitigation is important. When a DDoS attack is underway, some end users may experience services responding slower than normal and other end users may be temporarily disconnected until the mitigation begins.

WHAT YOU SHOULD KNOW ABOUT VERISIGN'S RESPONSE DURING AN ATTACK

Timely response is critical for quick restoration of service during a DDoS attack. Verisign follows the steps outlined below, which typically happen in minutes, so that you can return to normal operations as quickly as possible:

1. Upon alert generation, Verisign engineers begin investigation of the incident and work to eliminate false positives.
2. Where the alert, or set of alerts, is confirmed to be a possible indicator of a DDoS attack, Verisign immediately contacts you via telephone or email as set forth in the your escalation plan.
3. Verisign notifies you of the incident, provides a case number for tracking and makes a mitigation recommendation based on its expertise and the nature of the attack. Upon your consent, we will initiate redirection of your traffic to our mitigation facilities.[1]

Once your traffic reaches Verisign facilities, the response team further analyzes the attack and begins the filtering process. The filtering process continues until Verisign and you determine traffic is back to normal patterns and the impacted service is restored to normal operations. At this point, re-direction is stopped and your traffic no longer passes through Verisign mitigation facilities.

Verisign will periodically provide you with status updates about the ongoing incident via telephone or email. You can also track the mitigation in the portal in near-real time.

1 While mitigation is underway, end users may experience a slight increase in latency as traffic passes through Verisign facilities.

5. WHAT HAPPENS TO THE DATA SENT TO THE VERISIGN CLOUD?

To leverage always-on monitoring, your routers share information about your network data flows with Verisign. Verisign collects this information for the purposes of profiling traffic, detecting attacks and providing you with comprehensive reporting following a DDoS attack.

Verisign does not decrypt data during monitoring. In very rare cases, Verisign may need to decrypt the traffic during mitigation to effectively provide the DDoS Protection Service. In such cases, Verisign will decrypt and encrypt only after obtaining your consent and the appropriate keys.

WHAT YOU SHOULD KNOW ABOUT OUR DATA HANDLING

Verisign adheres to strict data-handling and -processing procedures and deploys industry-leading access controls to protect your data as it transits our network. These controls include biometric-based physical access, personnel screening and background checks, and logical separation of all services and data instances.

Within its multi-tenant cloud environment, Verisign establishes technical security controls to ensure that tenants do not pose a risk to each other in terms of data loss, collateral damage or misuse.

The Verisign cloud infrastructure complies with internationally recognized standards such as SSAE 16 and SOC 2. Ongoing risk assessments based on NIST SP 800-30 methodology are conducted to identify and minimize risk in the environment. In addition, independent third parties audit the Verisign cloud infrastructure on an annual basis. Finally, Verisign is certified under the US-EU Safe Harbor Framework.

6. WHAT SHOULD YOU KNOW ABOUT CONTRACTING FOR SAAS

For many customers, Verisign DDoS Protection Service is their first SaaS purchase. You may see some notable differences between contract terms for traditional on-premise software and those for services using a SaaS delivery model (such as the Verisign DDoS Protection Service). This is in large part because SaaS services are delivered to customers using a shared platform with limited customization of features and are offered under standardized terms. While each SaaS provider may have slightly different terms, you should expect to see the following terms and provisions in many SaaS contracts, including Verisign's contracts.

a. Warranties: SaaS Services are typically offered 'as is', 'where is', and 'as available' and without warranties of uninterrupted or error-free services. This is because SaaS providers depend on third parties, such as telecommunications providers and Internet service providers, to supply the services.

b. Acceptable Use Policy (AUP): SaaS contracts typically include an Acceptable Use Policy, or "AUP." The AUP may include guidelines for use of the SaaS service and a description of prohibited activities. Examples of prohibited activities may include, for example, infringing upon third-party intellectual property rights, engaging in illegal activities, transmitting information that is obscene and interfering with the vendor's network. The AUP may allow the SaaS provider to suspend service or terminate the contract if customers engage in a prohibited activity.

c. Data Privacy: SaaS providers typically establish policies, procedures and controls for the protection of customer data. Because SaaS is a multi-tenant platform, these practices must be standardized for all users. Therefore, it is not typical for a SaaS provider to accept data privacy terms which are inconsistent with its standard practices.

d. Suspension or Termination: Since SaaS infrastructure is multi-tenant, suspension or termination provisions are included to ensure that any one customer's use or abuse of the service does not impact the overall stability or security of the SaaS provider's infrastructure or affect its ability to service its other customers.

e. Limitation of Liability: Contracts generally cap limitations of liability for both parties (subject to some exceptions) to sustain the affordable pricing characteristic of the SaaS business model.

f. Indemnification: SaaS contracts generally require customers to indemnify the SaaS provider against any third-party claims and associated costs arising out of the customer's breach of its agreement with the SaaS provider. Some SaaS providers may indemnify the customer for intellectual property infringement, gross negligence and willful misconduct.

7. HOW TO GET HELP

INDUSTRY-LEADING SUPPORT

Verisign's Engineering Support has been recognized with the Technical Services Industry Association's (TSIA) Rated Outstanding award for its North America centers, measured against 100+ benchmark criteria across service, customer philosophy and staff development.

Built with your growing needs in mind, our support engineers are available 24 hours a day, 7 days a week.

CONTACT US

Learn more at www.verisigninc.com/ddos

Product inquiries: websales@verisign.com 1 (800) 637-8976 or (703) 763-2657

24x7x365 DDoS Protection Service support: vidnsupport@verisign.com

1 (866) 200-1979 or (703) 376-6905