VERISIGN®

CRITICAL NETWORK CAPABILITIES FOR CLOUD-BASED DDoS ATTACK MITIGATION

AS A LEADER IN DOMAIN MANAGEMENT AND INTERNET SECURITY, VERISIGN'S NETWORK SUPPORTS MORE THAN 82 BILLION TRANSACTIONS ON A DAILY BASIS, ENABLING NEARLY 50 PERCENT OF THE INTERNET'S DOMAINS. BUILDING NETWORKS TO SURVIVE THE LARGEST DDOS ATTACKS ON THE INTERNET IS PART OF VERISIGN'S HERITAGE, AND VERISIGN HAS BEEN USING DDOS MITIGATION TECHNIQUES FOR MORE THAN 16 YEARS WHILE PROTECTING THE .COM AND .NET INFRASTRUCTURES. THIS GIVES VERISIGN THE ABILITY TO FLEX ITS ENTIRE 1+ TBPS INFRASTRUCTURE AS NEEDED IN REAL-TIME RESPONSE TO ATTACK SCENARIOS AGAINST ITSELF AND ITS CUSTOMERS.

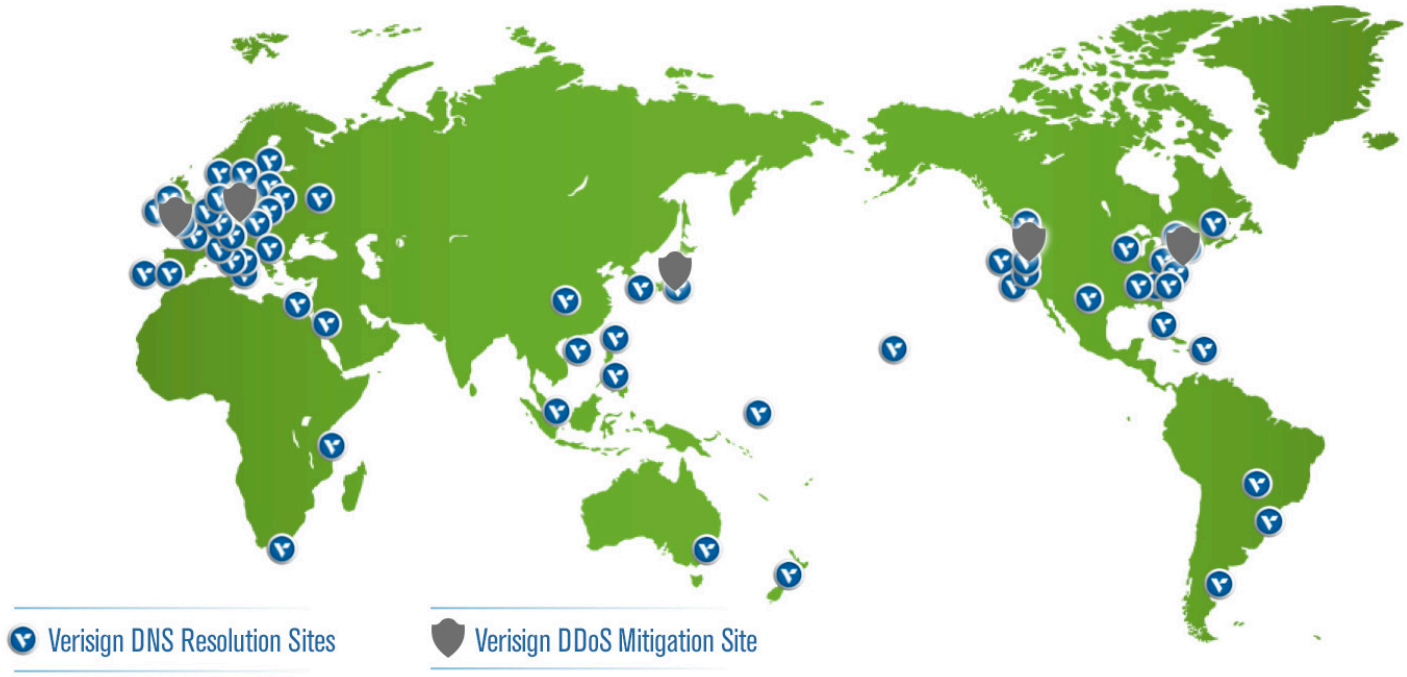
With attackers able to marshal ever-greater resources, enterprises are increasingly vulnerable if they go it alone in building DDoS defenses. Today's attackers are able to monitor a target's defensive moves and change the attack profile in real time, making DDoS defense all the more challenging. Due to this evolving DDoS threat, companies are turning to cloud based DDoS mitigation providers to keep enterprises up and running in the face of complex and high-volume assaults. Capable cloud DDoS mitigation service providers have built out massive amounts of network bandwidth and DDoS mitigation capacity, and can work seamlessly with customers that are multi-homed with one or more ISPs or cloud providers. Just as important as network capacity is the flexibility and diversity of the provider's network infrastructure in terms of design, interconnections and peering relationships. The flexibility and diversity of the service provider's own network backbone is a key factor in how quickly an attack can be mitigated to support maintaining customer resource operations.

PEERLESS PEERING

As a leader in domain management and Internet security, Verisign's network supports more than 82 billion transactions on a daily basis, enabling nearly 50 percent of the Internet's domains. When Verisign is cleansing traffic using cloud-based DDoS mitigation, attack traffic is filtered in the cloud before it ever reaches the customer network. Verisign announces customer IP assets across five global mitigation centers, and serves as a protective shield between the Internet and the customer network. Verisign's DDoS services rely on a fully redundant backbone, purpose-built on multiple diverse 10 Gbps optical infrastructures, interconnecting both regional and global mitigation centers, along with peering connectivity that leverages some of the largest and best-connected Internet exchange points (IXPs) in the world.

As the world's largest operator of Domain Name System (DNS) registry and resolution services and the operator of .com, .net, .gov, .edu and .tv, as well as two of the world's 13 Internet root servers (a.root-servers.net and j.root-servers.net), peering with Verisign is an attractive proposition for any Internet service or content provider concerned with optimizing network performance and minimizing latency.

FIGURE 1: VERISIGN'S GLOBAL NETWORK CONSTELLATION



Verisign interconnects openly and actively with networks of consequence and is positioned directly adjacent to more than 500 network operators. On average, more than 75 percent of Verisign's traffic is delivered through direct peering relationships. Since peer-learned routes offer improved performance by eliminating dependence on intermediate transit networks, Verisign's peering stature minimizes unnecessary latency and offers optimal network performance when customer services are actively under mitigation.

PEERING MEANS SPEED

A primary benefit of Verisign's network and extensive global peering relationships is speed. Verisign's IP route announcements propagate rapidly across our global mitigation centers to our worldwide constellation of 17 Internet access points and an array of global IXPs. Verisign's network is designed to provide for optimal convergence times when advertising customer IP address space; the faster the attack traffic gets to Verisign's network, the faster the malicious attack flows can be mitigated and the clean traffic sent back to a customer's network. Verisign's network reach and footprint typically enable mitigations to start in less than 180 seconds once customer IP assets have been announced from Verisign sites. This fast "announcing" or propagation of customer IP space into the global routing system is critical for rapid recovery from DDoS attacks. Verisign's backbone is also enabled by multi-protocol label switching (MPLS), to allow traffic surges to be dynamically rerouted and prioritized based on current Internet traffic conditions. This gives Verisign the ability to flex its entire 1+ Tbps infrastructure as needed in real-time response to attack scenarios.

INVESTING IN NETWORK CAPABILITY

Verisign's network continues to evolve, capitalizing on operational excellence, innovation and expertise garnered from experience and institutional knowledge gained from maintaining the availability of the .com and .net infrastructures for more than 16 years. Each infrastructure component is continually monitored, evaluated and enhanced in terms of architecture and global capacity.

"The Verisign systems and network architecture teams are driven by a core requirement to engineer the DDoS mitigation infrastructure to provide the highest performance and withstand the largest known attacks observed on the Internet."

– Ryan Donnelly, Director of Network Systems and Network Architecture, Verisign DDoS Protection Services

DDoS service providers often speak to their overall "capacity," but it is important to draw a distinction between network capacity and mitigation capacity. Our mitigation centers target the highest levels of capacity in the industry to address the scalability of volumetric attacks. However, a key differentiator of Verisign's network design is the flexibility provided by a dedicated globally interconnected MPLS-enabled optical network core. The network allows Verisign to adapt to network and system load conditions real time to optimize traffic management and performance.

"Given Verisign's role as a critical internet infrastructure provider, we have had a unique opportunity to build an infrastructure from the ground up to survive, and evolve with the internet threat landscape. With the Verisign DDoS Protection service, customers are protected by the same state-of-the-art, battle-tested technologies and processes that have kept .com and .net 100% available for 16 years."

– Frank Scalzo, Director of Network Engineering, Verisign DDoS Protection Services

Verisign's DDoS mitigation network is strategically engineered to handle both nominal traffic loads in addition to large traffic spikes which occur under DDoS attack conditions. The flexible MPLS configuration allows Verisign's DDoS Protection Services engineers to selectively engineer and route traffic flows in response to global DDoS attack dynamics so that no single component is overwhelmed. Having no single point of failure is core to Verisign's network design DNA, and extends through all logical and physical components of the network including the use of diverse fiber paths, hardware and software components, operating systems, data center providers, generator manufacturers and even fuel suppliers. DDoS attack traffic can originate from any region in the world and any given attack profile can inundate regional provider mitigation centers without the capabilities and flexibility of a globally interconnected MPLS network fabric.

Verisign's infrastructure is built in a way that maximizes redundancy and resilience, and reduces the possibility of collateral damage from one customer's attack impacting another customer. Other cloud based DDoS providers may have multiple mitigation centers, but they lack an interconnected backbone connecting mitigation centers together. This enables more effective load balancing of attack traffic across our service to deal with attack traffic closest to its source and reroute traffic efficiently to other sites in the event of site failure or maintenance.

When employing BGP mitigation, cloud-based DDoS mitigation providers typically return clean customer traffic via GRE tunnels from the mitigation site(s) to the customer data center(s). Verisign's global backbone enables customers to interconnect in locations that are most convenient for them. By leveraging our global backbone, Verisign can carry clean traffic from the far corners of the globe, back to the nearest common connection point. This simplifies the number of GRE tunnels or cross-connects customers are required to implement and manage, thus speeding up the performance of customers' websites while Verisign is supporting attack mitigation

WHEN FIGHTING DDOS ATTACKS, NETWORK SIZE MATTERS

Building networks to survive the largest DDoS attacks on the Internet is part of Verisign's heritage, and Verisign has been using DDoS mitigation techniques for more than 16 years while protecting the .com and .net infrastructures. Verisign has had the opportunity to test the platform against a diverse set of DDoS events, and unlike some cloud DDoS service providers, it has had many years to harden its platform and ensure that all components work together as they should.

LEARN MORE

For more information about Verisign DDoS Protection Services, go to VerisignInc.com/DDoS.

ABOUT VERISIGN

As the global leader in domain names, Verisign powers the invisible navigation that takes people to where they want to go on the Internet. For more than 16 years, Verisign has operated the infrastructure for a portfolio of top-level domains that today includes .com, .net, .tv, .cc, .name, .jobs, .edu and .gov, as well as two of the world's 13 Internet root servers. Verisign's product suite also includes Managed DNS Services, Distributed Denial of Service (DDoS) Protection Services and iDefense® Security Intelligence Services. To learn more about what it means to be powered by Verisign, please visit VerisignInc.com.