



# **VERISIGN® INTERNET DEFENSE NETWORK**

**FAQs**



## FAQs

### **WHAT IS A DOS OR DDOS ATTACK?**

A Denial of Service attack or Distributed Denial of Service attack occurs when a single host (DoS), or multiple hosts (DDoS), send legitimate traffic to a target with malicious intent for the purpose of disrupting an application or service either temporarily or permanently.

Targets can include, but are not limited to, Web servers, DNS servers, application servers, routers, firewalls and Internet bandwidth.

### **WHAT IS IN-THE-CLOUD?**

The term cloud is used as a symbol or metaphor for the Internet, based on the way the Internet is depicted in network diagrams. In-the-Cloud typically refers to a service that is provided/performed for a customer before entry into their Internet service connection(s)/infrastructure.

Essentially, an In-the-Cloud DDoS protection service redirects traffic destined for an organisation through an Internet data centre, where undesirable items such as DDoS packets are dropped. The cleansed traffic is then delivered to the organisation.

### **IS THE VERISIGN INTERNET DEFENSE NETWORK A COMPLEMENTARY SERVICE OR WOULD IT REPLACE OUR FIREWALL, INTRUSION PREVENTION SYSTEM (IPS)/ INTRUSION DETECTION SYSTEM (IDS) AND/OR OTHER SECURITY PRODUCTS WITHIN OUR NETWORK INFRASTRUCTURE?**

The VeriSign Internet Defense Network is a complementary service and is not intended to replace existing security infrastructure.

### **I HAVE MULTIPLE INTERNET CARRIER CIRCUITS FROM DIFFERENT INTERNET SERVICE PROVIDERS (ISPs). CAN THE VERISIGN INTERNET DEFENSE NETWORK WORK WITH MY SOLUTION?**

Yes, the VeriSign Internet Defense Network can monitor and mitigate DDoS attacks on any ISP, and can provide the same level of service for customers who are multi-homed

through more than one ISP. This means that a customer only has to deal with one team and one threat remediation process in order to knock down the attack, rather than relying on multiple bandwidth providers to reach similar conclusions on the same timelines. Since our solution is network agnostic, you have the flexibility to change your infrastructure to suit your changing business needs.

### **HOW LONG DOES IT TAKE TO DEPLOY THE VERISIGN INTERNET DEFENSE NETWORK?**

It typically takes less than fourteen (14) calendar days to set up the monitoring solution and start receiving customer flow traffic.

### **HOW LONG BEFORE I AM CONTACTED ABOUT A DDOS ATTACK TO MY NETWORK OR APPLICATION? WHAT KIND OF SERVICE LEVEL AGREEMENT (SLA) IS PROVIDED WITH THE VERISIGN INTERNET DEFENSE NETWORK?**

Typically, customers are notified of a potential attack within five minutes of a monitoring alert being generated.

The currently provided SLA states that VeriSign will contact the customer, in accordance with its escalation plan, within 15 minutes of receipt of a monitoring alert. Upon contact, VeriSign will work with the customer to determine if mitigation is required or if the alert was caused by legitimate customer activity. If mitigation is needed, VeriSign will recommend the best course of action.

In the event that redirecting the customer's traffic is the recommended course of action, the customer's traffic will be redirected to VeriSign's Internet Defense Network sites before reaching the customer's network. VeriSign will apply layered filters to the traffic redirected to the VeriSign Internet Defense Network sites, which progressively block traffic aimed at disrupting or disabling the customer's Internet-based services. Legitimate traffic is then redirected from the VeriSign Internet Defense Network sites back to the Customer's network. When the DDoS attack has abated, VeriSign will coordinate with the Customer in order to return the Customer to normal operations.





## FAQs

### **IS THERE ANY MANUAL INTERVENTION CARRIED OUT ON MY INFRASTRUCTURE DURING A DDoS ATTACK?**

VeriSign establishes event mitigation procedures with you to fit your service model. Optimal solutions vary and depend upon network size and types of services used, among other considerations.

If Internet traffic is redirected using our BGP off-ramping, no manual intervention is needed on the customer network. If traffic is redirected via DNS, you will need to point your “A” records to a VeriSign IP address and set the time-to-live, TTL, to the minimum time for redistribution.

After mitigation, traffic is proxied back to you.

### **WHAT IS THE PROCESS FLOW DURING AN ATTACK SITUATION?**

When an alert is generated, the VeriSign support team contacts the customer, provides them with a ticket number and begins investigation. Once the alert is determined to be a DDoS event, a recommendation is made to mitigate. Our SLA is to contact the customer with a recommendation on a mitigation strategy within 15 minutes after receipt of an alert. With customer permission, in order to mitigate the DDoS attack VeriSign will swing traffic to a mitigation facility or facilities. The VeriSign Internet Defense Network support team begins further analysis of the source of the attack and begins to reach upstream providers to resolve the attack closer to the source, as needed.

### **DO YOU CONTACT THE CUSTOMER AFTER THE DOS/DDOS ATTACK HAS ENDED?**

Yes. One of our VeriSign Security Operations personnel will contact the company representative identified in the escalation plan to discuss moving traffic back to its original path.

### **CAN I SET UP MY ROUTER TO THWART A DDoS ATTACK?**

Routers cannot block spoofed IP sources or trace back manually to thousands of IP addresses, which makes Access Control Lists (ACLs) useless against DDoS attacks.

### **CAN I SET UP MY FIREWALL TO THWART A DDoS ATTACK?**

Firewalls are not designed to mitigate DDoS attacks. Using a firewall for mitigation could cause the CPU to spike and deplete memory resources. Also, firewalls do not have anomaly detection capabilities.

### **CAN I SET UP MY INLINE IPS OR MY IDS TO THWART A DDoS ATTACK?**

Yes, but IPSs and IDSs require extensive manual tuning that takes time and can leave you vulnerable.

An IDS traditionally sits behind the firewall with an uplink to a router or switch that sits in front of the firewall. An IDS issues an alert when it detects an anomaly. At that point, the attack traffic is already consuming your Internet bandwidth with the potential for saturating the link, which can cause the CPU to spike and deplete memory resources.

An IPS has the capability to work as an anomaly detector; however, it requires several weeks for an IPS to understand “normal” traffic patterns, and frequent manual tuning to specify which traffic is allowed and which should be alerted or blocked.

### **I HAVE OVER-PROVISIONED X AMOUNT OF BANDWIDTH TO TRY TO PREVENT DDoS ATTACKS. WHAT CAN THE VERISIGN INTERNET DEFENSE NETWORK DO FOR ME?**

Over-provisioning is not a cost-effective solution. For example, if you know that your normal amount of traffic could reach 15 Mbps, but you provision 30 Mbps in case a DDoS attack should occur, then you have over-provisioned by 100 per cent and doubled your monthly recurring charges. And attackers can easily increase the volume of their attacks. Since some DDoS attacks now reach more than 40 Gbps, over-provisioning an Internet circuit could become very costly.





## FAQs

### WHAT ABOUT “BLACKHOLING” THE IP ADDRESS(ES)?

Blackholing an IP address or a range of IP addresses can result in legitimate packets being discarded along with malicious attack traffic, which means that the attacker wins. If an ISP performs the blackhole, they must first identify the source of the traffic, which can cost valuable time and may still end up blocking legitimate traffic.

### WHERE ARE THE VERISIGN INTERNET DEFENSE NETWORK MITIGATION DATA CENTRES LOCATED?

- Ashburn, Virginia
- San Francisco, California
- Amsterdam, Netherlands
- Tokyo, Japan

### ARE THE VERISIGN INTERNET DEFENSE NETWORK DATA CENTRES IDENTICAL IN TYPES OF MITIGATION EQUIPMENT AND CAPACITY?

All the VeriSign Internet Defense Network data centres are identical in capacity: dual 10 Gigabit Ethernet. Because we are NOT dependent upon any hardware vendor or service provider, our data centres do NOT have identical equipment.

### WHAT DOES THE VERISIGN INTERNET DEFENSE NETWORK SOLUTION DO WITH DATA RETENTION? HOW LONG IS DATA KEPT IN STORAGE?

Our current data retention policy is:

- Mitigation Events = 1 year
- DoS alerts (low) = 30 days
- DoS alerts (medium) = 60 days
- DoS alerts (high) = 90 days
- Traffic Reports = 60 days

This is subject to change and does not constitute a guarantee. Please consult your VeriSign representative for details.

### HOW DO CUSTOMERS OBTAIN TRAFFIC REPORTS?

Traffic reports can be generated via the portal and then exported to an XML or PDF file.

### WHAT KIND OF DEVICE OR DEVICES DOES A POTENTIAL CUSTOMER NEED AT THEIR FACILITY?

The VeriSign Internet Defense Network supports the following equipment:

#### CISCO ROUTERS

Peakflow SP 4.5 supports the following Cisco routers:

Cisco traditional IOS-based routers that run IOS 12.0 or later (Netflow v5 and v9)

Cisco Catalyst 4500 family w/Sup IV or later and NFFC (Netflow v5)

Cisco Catalyst 5500 family w/suitable Sup and NFFC (Netflow v7)

Cisco Catalyst 6500 family w/Sup 2 or later, hybrid or native (Netflow v5 and v7)

Cisco CRS-1 (Netflow v9)

**Important: Cisco Catalyst routers do not support TCP flags.**

#### JUNIPER CFLOWD V9 TRAFFIC

Juniper cflowd v9 is only supported for IP traffic. Cflowd data from MPLS-derived traffic might not work with current JunOS software and Peakflow SP does not officially support it.

#### JUNIPER ROUTERS

Peakflow SP 4.5 supports the following Juniper routers:

Juniper T-series (cflowd v5 or v9 with services PIC)

Juniper M-series with Internet Processor II (cflowd v5 or v9 with services PIC)

Juniper J-series (cflowd v5)

Juniper TX-series (cflowd v9)

Juniper MX960 (cflowd v5)

#### FOUNDRY ROUTERS

Peakflow SP supports Foundry routers with sFlow v2, v4 and v5. Foundry does not support ACL generation

#### FORCE10 ROUTERS

Peakflow SP supports Force10 routers with sflow

Devices or other vendors that can provide flow data or IPFIX will be handled on a case-by-case basis.





## FAQs

### **DO I NEED TO PURCHASE A CIRCUIT TO THE VERISIGN INTERNET DEFENSE NETWORK DATA CENTRE SO THAT MY TRAFFIC CAN BE REDIRECTED?**

You have the option of purchasing a circuit to one of the VeriSign Internet Defense Network data centres, or we can redirect/on-ramp your traffic with a GRE tunnel (most preferred) or a VPN tunnel.

### **ARE THERE ANY REQUIREMENTS REGARDING IP ADDRESS SPACE?**

In order for VeriSign to off-ramp your traffic via BGP, you must have a minimum of /24 or 254 continuous IP address spaces. The /24 can be obtained from your Internet Service Provider or from ARIN, APNIC, RIPE, AFRINIC or LACNIC.

- [www.arin.net](http://www.arin.net) – North America
- [www.apnic.net](http://www.apnic.net) – Asia Pacific
- [www.ripe.net](http://www.ripe.net) – Europe
- [www.afrinic.net](http://www.afrinic.net) – Africa
- [www.lacnic.net](http://www.lacnic.net) – Latin America and the Caribbean

### **IS IT POSSIBLE FOR THE VERISIGN INTERNET DEFENSE NETWORK SOLUTION TO PROTECT JUST A SINGLE WEB SERVER?**

Yes, in the case of a single Web server we can divert traffic with a DNS change. However, you will need to make some changes to your system. We will provide VeriSign IP addresses for you so that you can change the “A” record in your (or your ISP’s) managed DNS server to the newly assigned VeriSign IP address.

### **WHEN THE CUSTOMER’S TRAFFIC IS OFF-RAMPED TO VERISIGN, IS THERE ANY LATENCY THAT NEEDS TO BE FACTORED INTO THE EQUATION?**

Latency is determined by the distance between the customer’s protected facility and the VeriSign Internet Defense Network data centre. VeriSign has extensive public and private peering at most of the global Internet exchange points; this allows VeriSign optimal routing paths throughout the Internet. VeriSign also distributes data centres geographically to minimise latency. Centres are located in the Washington DC Metro area, Silicon Valley/San Francisco Bay area, Amsterdam and Tokyo. Customers in these markets should expect no measurable latency increase (<5 ms). Beyond these metro markets, customers in the US could experience an additional latency of 15-30 ms per 1,000 miles of distance from the data centre. Past experience indicates that from one US coast to the other, latency averages around 30 - 35 ms.

### **IT CAN TAKE OVER 30 MINUTES FOR BORDER GATEWAY PROTOCOL (BGP) TO ANNOUNCE A CUSTOMER NETWORK BLOCK. BEFORE VERISIGN HAS THE ABILITY TO START FILTERING TRAFFIC, WHAT MEASURES ARE USED TO DECREASE THE CONVERGENCE TIME?**

VeriSign has studied the issue of BGP convergence time in depth. VeriSign uses a BGP route monitoring industry leader that has hundreds of BGP probes all over the globe with thousands of BGP feeds. VeriSign uses this tool to track the time it takes for BGP updates to propagate across the Internet. While convergence time is not completely controllable or predictable, we typically see all the BGP feeds converge on the new protected path in two (2) minutes or less. VeriSign advises customers to expect convergence time to be about five (5) minutes, but we have seen the time be much less. VeriSign has been using BGP announcement techniques to failover critical .com and .net infrastructure services for years.





## FAQs

### **HOW DOES VERISIGN EXPLOIT ITS RELATIONS WITH OTHER ISPs DURING AN ATTACK THAT THE CUSTOMER CANNOT MITIGATE ALONE?**

VeriSign has extensive public and private peering at most of the global Internet exchange points, giving VeriSign the ability to reach close to 60% of the Internet via peering. As a critical infrastructure provider, VeriSign participates with most large networks in the same operational security forums that Tier 1, 2 and 3 carriers use to interact with each other. When a customer has an issue, VeriSign can exploit those relationships to interact directly with the carriers, via the same forums and other facilities used by those networks to work with one another.

### **HOW DOES VERISIGN BEST WORK WITH ENCRYPTED DATA (SSL) TO UNDERSTAND THE NATURE OF AN ATTACK?**

If only the payload is encrypted and customers do not want to exchange keys, we can only filter the headers or anything outside the payload. If the customer is willing to provide exchange keys, we can decrypt -> filter -> and re-encrypt the packet and send it to the customer via a secure return path.

### **CAN THE VERISIGN INTERNET DEFENSE NETWORK WORK WITH THE CUSTOMER'S MONITORING, MITIGATION OR CORRELATION EQUIPMENT DEPLOYED IN THE NETWORK INFRASTRUCTURE?**

VeriSign will evaluate such deployed equipment on a case-by-case basis and determine whether it can be integrated with the VeriSign Internet Defense Network.

### **DOES THE VERISIGN INTERNET DEFENSE NETWORK SUPPORT IPv6?**

We are testing IPv6 with the VeriSign Internet Defense Network, but do not have an availability date as yet.

### **LEARN MORE**

For more information about the VeriSign® Internet Defense Network, please contact a VeriSign representative at [InternetDefenseNetwork@VeriSign.com](mailto:InternetDefenseNetwork@VeriSign.com) or visit us at [www.Verisign.co.uk](http://www.Verisign.co.uk).

### **ABOUT VERISIGN**

VeriSign is the trusted provider of Internet infrastructure services for the networked 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.co.uk](http://www.Verisign.co.uk) for more information.

