Web Security (DDoS)

Phone: (877) 937-4236 Email: info@cdnetworks.com

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA

Table of Content

Status and Challenges of the Industry 3
DDoS attack incidents happen frequently, affecting enterprise business 3
Bottlenecks of traditional protection methods 3
Slow response from websites affects user experience 4

Product Introduction 4
Product Overview 4
Architecture Diagram of the Product 4
WSS Applicable Industries and Scenarios 5
E-commerce 5
Internet Finance 5
Online Education 5

Product Functions 5
Monitor and Alert 5
Attack Alarming System 5
Access Control Policies 6
Blacklist/Whitelist 6
Access Control for a Single IP 7
Access Control for a Single URL 7
Access Control for a Domain Name 7
Attack Mitigation 7
Network-Layer DDoS Mitigation 7
Mitigation Visibility 11
Web Acceleration 13
Intelligent Routing 13
Content Compression 13
Supports HTTPS Business 13
Seamless Deployment 14
Deployment without Certificates 14
SNI Certificate Deployment 14

Product Value 14
Zero Deployment and Zero Maintenance for Easy Access to Professional Mitigation Services 14
Big Data-Enabled Security for Business Continuity 14
Efficient Emergency Response 14
Intelligent Acceleration improving User Experience 15

About CDNetworks 15
CDNetworks Science & Technology Enjoys Many Firsts in This Industry 15
Quality Global Resources 16
Rich Experience of Professional Experience 16
One-Stop Sales Network 16

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

Status and Challenges of the Industry

With the rapid development of "Internet Plus", there come more and more cyber security problems, among which Distributed Denial of Service (DDoS) becomes the first choice to execute network attacks, as this type of attack is easy to launch, obvious in effect and hard to trace and defense against. Challenges for Internet industry are many:

DDoS attack incidents happen frequently, affecting enterprise business

A mature supply chain has come into shape in black market, and DDoS as a service and attack tools are sold online publicly. The skill level of launching DDoS attacks becomes very low that it is also utilized and combined with profit-driven activities like online fraud and vicious competition attacks.

According to the China Internet Security Report-2016 by CNCERT, in 2016, there were 452 DDoS incidents with over 1Gbps attack traffic per day. The volumetric DDoS incidents were increasing, and the daily incidents with over 10Gbps were 133, accounted to 29.4% of the total DDoS incidents.

DDoS attacks usually interrupt service availability which could cause customer attrition, decline in trading volume, reputation losses, to name but a few. Even worse, attackers use DDoS attacks to blackmail victim companies and it tremendously affects business operation.

Bottlenecks of traditional protection methods

Some enterprises might purchase specialized hardware to defense against DDoS attacks. This method can mitigate attacks to some extent, but bottlenecks still exist:

1. **Limited by bandwidth and equipment performance, challenge by unexpected traffic burst**
   As entry and cost for DDoS attacks level down, it is not uncommon over hundreds of Gbps scale DDoS attacks on the Internet. Scalability of traditional anti-DDoS equipment is limited by bandwidth and equipment performance, and the on-premise hardware is not able to solve bandwidth congestion while attackers power up the attack volume.
2. **Workload of deployment and maintenance**
   Inline and off-path options are usually applied for hardware equipment, though it requires adjusting or even changing network topology to fit in the solution. It usually causes extra workload of deployment, PoC test, and production line test, and might even bring in potential risks. Moreover, it takes longer for repair and maintenance if hardware dysfunctions.
3. **Limited data analysis ability prone to false positives**
   Limited by data source and data collecting ability, hardware equipment is closed in nature and data resources cannot be fully taken use of. Moreover, defense policies could not be upgraded timely and collaboration in defense has not yet come into shape, so application-layer DDoS attacks (especially CC) are difficult to be recognized by hardware equipment, affecting the defense effect.

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

Slow response from websites affects user experience

Company websites may experience more and more concurrent requests as business grows, and there might be frequent cross-ISP and cross-region access involved. ISPs in China often limit the cross-network transmission (for example, there are tens of thousands of milliseconds time delay between China Telecommunications and China Unicom in transmission), and longtime delay could happen because of such limit.

Besides, there are over 100 tier-two and tier-three ISPs in China, and the delay issue becomes more obvious among them. It could all lead to slow response from websites, affecting user experience and work productivity. In the intense competition of online business, customer attrition and reputation losses due to user experience definitely draw a lot of attentions to win or remain in business.

Product Introduction

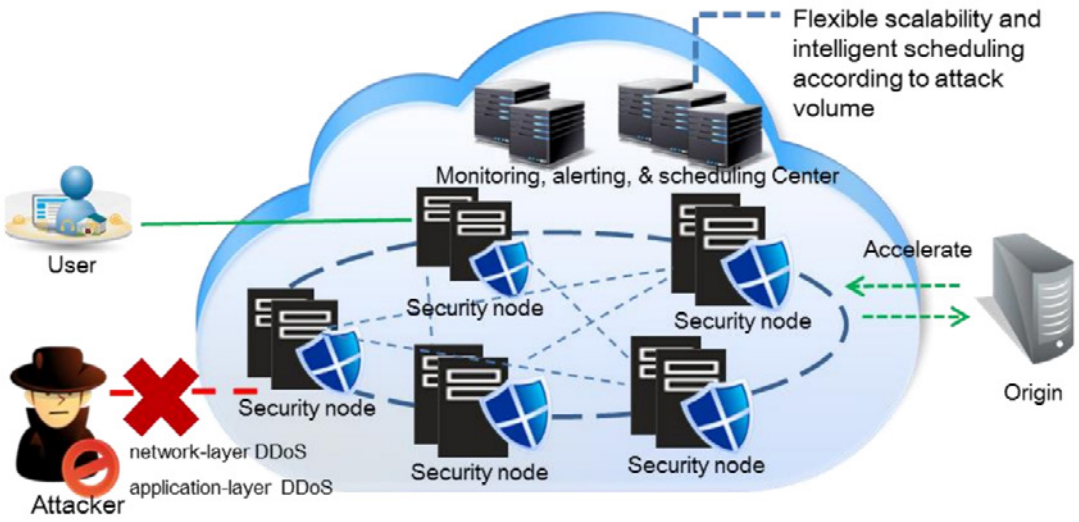
Product Overview

CDNetworks Website Security Service (WSS for short), is based on the globally distributed CDN resources, and offers proprietary mitigation algorithms combining with the big data enabled intelligence. It can detect and mitigate various types of DDoS attacks (such as SYN Flood, ACK Flood, UDP Flood, HTTP Flood, etc.) in real time, and meanwhile provides acceleration service to normal access to optimize user experience.

Architecture Diagram of the Product

Relying on CDNetworks globally distributed security PoPs, CDNetworks WSS builds up a CDN-based cloud security with dedicated attack monitor & alert center and intelligent scheduling center. Combined with big data analytics in the cloud, WSS can detect and analyze traffic in real time and block abnormal traffic based on the dynamically adjusted mitigation policies. In addition, acceleration service is provided for normal traffic optimization for a better user experience.

Please see the diagram below for the architecture of CDNetworks WSS.



CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

WSS Applicable Industries and Scenarios

CDNetworks WSS is devoted to providing integrated services seamlessly combined with DDoS protection and acceleration, aims to ensure website availability and speed up Internet access. The applicable scenarios of WSS include but not limited to the following:

E-commerce

More and more companies turn to e-commerce to facilitate trading and improve consumer shopping experience. At the same time, online shopping sites are susceptible to DDoS attacks caused by vicious competition, which usually results in business interruption. Online shopping sites are also suffered from slow web performance, due to massive concurrent requests, frequent cross-ISP access, and so on, and it could impact on business continuity and user shopping experience.

Internet Finance

Especially in the recent years, Internet finance develops with astonishing speed, online financing, online lottery, and P2P lending and loans in particular. The financial industry is always the main target of attackers for "money rush", and the peer competition is fairly intense as well. Such websites require a high level of availability and continuity.

Hence, if security problems happened, such as a website is not accessible for a short moment, it would cause tremendous losses invest panic. Besides, such websites often require real time services, problems of slow response from websites or operation failure would surely affect the credibility and user experience of the sites.

Online Education

Online education websites offer VIP tutoring and training services via audio/video and interactive whiteboard to users. Vicious peer competition usually results in utilizing DDoS attacks affecting site availability for business interruption, as it is the most effective way to slow down the website responses and affect user experience directly.

Product Functions

WSS functions as a shield guard to ensure real time services and website stability: monitor & alert, attack mitigation (network-layer DDoS and application-layer DDoS), visualization of protection, web acceleration, etc.

Monitor and Alert

It provides users with multi-dimension monitoring and alerting services, including attack alarming system, website availability monitoring, security prewarning, and QoS monitoring on security PoPs, and aims to enable users to have a clear understanding of their websites in real time.

Attack Alarming System

Comprehensive monitoring and alarming services for protected websites.

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

1. **Network-Layer DDoS Monitoring**
   CDNetworks WSS provides a group of IP addresses exclusively per customer, which enables WSS to collect the attack traffic / bandwidth at network layer in real time and analyze it by separated IP groups granularly per customer. Alerts via email or SMS will be sent out once mitigation thresholds are triggered, and attack details are included such as attack time, attack peak traffic, and etc.
2. **Application-Layer DDoS Monitoring**
   CDNetworks WSS creates a dynamic access baseline formed by the analysis on historical access logs from the security PoPs (such as access frequency of each resource, behavior signatures of each request, etc.). Once abnormal access is detected, alerts are sent out according to notification policies (such as threshold set by QPS).

Website Availability Monitoring

It includes HTTP/HTTPS and PING monitoring.

- **HTTP/HTTPS Monitoring**
  The monitoring mechanism relies on regularly stimulating visitors' access to monitored websites and analyzing on responses from globally distributed monitor nodes in real time, once anomaly is detected, alerts via email or SMS will be sent out, so the website staff can be aware of the anomaly in a timely manner.
- **PING Monitoring**
  The monitoring mechanism relies on regularly probing the monitored servers or website connectivity and obtaining websites/servers connectivity status, packet loss ratio, and RTT response time, in order to detect connection anomaly. Alerts via email or SMS will be sent out, so the website staff can be aware of the anomaly in a timely manner.

Security Pre-warning

CDNetworks WSS analyzes the cloud-based attack data via the big data analysis platform and extracts attack signatures like IP addresses, UA, Refer, etc. Then it conducts security event correlation analysis on the similar attack techniques from different websites or industries. Mitigation policies are deployed to the entire network, in advance of similar attacks happen to the potentially susceptible websites in certain industry.

QoS Monitoring on Security PoPs

CDNetworks WSS provides QoS monitoring on all the security PoPs 24/7. Refer to the PoP status, intelligent deployment and switch-over is enabled based on service quality of each node (such as load and traffic of each node) to ensure service availability and stability.

Access Control Policies

Access control policies mainly include IP/URL blacklist and whitelist, access control by IP address, access control by URL, access control by domain name, and etc.

Blacklist/Whitelist

Blacklist/whitelist includes IP blacklist/whitelist and URL blacklist/whitelist. IP blacklist/whitelist supports configuring access control by IP address. For example, if the external IP addresses of origin's office environment are added on whitelist, then these IP addresses will not be limited by protection policies.

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

URL blacklist/whitelist supports configuring access control by URL. Some attackers use illegitimate URLs to launch attacks and it causes massive requests back to origins. In this case, all the illegitimate URLs can be blacklisted and blocked.

Access Control for a Single IP

By setting the frequency threshold for requests from certain IP, requests above the frequency threshold will be blocked or further validated. Threshold of WSS can be automatically adjusted based on its self-learning results.

Access Control for a Single URL

By setting connection threshold for certain URL, connection requests above the threshold will be returned with 403, to avoid webpage connection failure from too many connections. Threshold of WSS can be automatically adjusted based on its self-learning results.

Access Control for a Domain Name

It happens that DDoS attacks are launched from a large number of attacking IP addresses and the total number of requests is huge, but a few requests per a single IP address. To counter this type of attacks, the access control for a domain name can be enabled, so that when back-to-origin requests per a domain name exceed the threshold, mitigation policy will be triggered to control the total number of requests and protect the origins.

Attack Mitigation

Network-Layer DDoS Mitigation

Attackers use many fake IP addresses to send a large number of data packets to a targeted server to consume its bandwidth resource and make the server could not respond to normal requests. This is a typical case of network-layer DDoS. Common network-layer DDoS attacks include SYN Flood, ACK Flood, ICMP Flood, UDP Flood, and reflection attacks (such as NTP reflection, DNS reflection, SSDP reflection), etc.

By intelligent mitigation mechanisms, CDNetworks WSS detects and analyzes traffic in real time, and efficiently mitigates flood traffic without affecting normal requests. The mitigation capability of the cloud platform is over 1Tbps. WSS can effectively mitigate SYN Flood, UDP Flood, ICMP Flood, NTP reflection attacks, SSDP reflection attacks, DNS reflection attacks and other network-layer DDoS attacks. Introduction to main types of attacks and their protection methods:

SYN Flood

- **Attack Introduction**

  Attackers use tools or control zombie machines to send a large number of TCP SYN messages to a targeted server, the tools or machines do not reply ACK messages after the server responding to AYN-ACK messages. In this way, it leaves many TCP half-open connections on the targeted server to consume resources, and normal requests cannot be processed by the server any more.

- **Protection Principle**

  CDNetworks WSS adopts heterogeneous architecture for mitigation and proprietary patented technologies to detect and filter abnormal and RFC-uncompliant packets in real time. WSS also conducts SYN cookie and re-sending verification to check client-side protocol behaviors, so that attacks can be mitigated without affecting connections from legitimate client-side.

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

ACK Flood

- **Attack Introduction**

Attackers use tools or control zombie machines to send a large number of ACK messages to a server to make the server occupied with the three-way handshake messages. In this way, the resources on the server will be run out and normal requests cannot be processed by the server any more.

- **Protection Principle**

The intelligent mitigation mechanism can store connection table information in real time and verify the received ACK messages legitimate or not. If not, packets will be dropped directly to realize effective mitigation in an efficient way without affecting normal requests.

ICMP Flood

- **Attack Introduction**

Attackers send massive oversized packets (for example: a packet over 65535 bytes) to overload targeted servers, and the servers are not able to provide normal services any longer or even become paralyzed.

- **Protection Principle**

The intelligent mitigation mechanism conducts packet statistics on traffic reaching the destination IP addresses in real time so that traffic exceeds the threshold will be dropped.

UDP Flood

- **Attack Introduction**

As UDP is a connectionless protocol without reliability or completeness validation in place, so the data transmission speed is fast, and this is a reason it becomes an ideal tool for attackers. The common practice of UDP Flood is that attackers send a huge number of UDP packets with fake original IP addresses to targeted server to consume the network bandwidth resources and congest links, so that the web server will no longer provide further service.

- **Protection Principle**

The intelligent mitigation mechanism drops all UDP packets for non-UDP based business. For customers with UDP business, WSS mitigates UDP Flood by rate limiting, UDP packets matching and etc.

Reflection DDoS Attacks

- **Attack Introduction**

Reflection attacks are a type pf UDP-based amplification DDoS attack. An attacker can send a packet with a forged source IP address to some public servers (like NTP or DNS servers) on the Internet. The forged IP addresses belong to the intended victims, and the utilized Internet servers respond to the victim. The amplification is realized as the replied contents from the public servers are several times larger than the requests to the servers, and all the amplified contents are reflected and sent to the victims.

- **Protection Principle**

The intelligent mitigation mechanism can directly filter packets from ports usually utilized by reflection attacks (such as NTP, DNS, SSDP, etc.) to mitigate such DDoS attacks.

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

Application-Layer DDoS Attacks

There are many mechanisms adopted by CDNetworks WSS to detect and analyze request packets in real time, such as threat intelligence database, behavior-based verification, auto-learning based log analysis, and etc. Without affecting normal requests, CDNetworks WSS effectively mitigates illegitimate requests in real time. The mitigation performance of the cloud platform reaches as high as 1 billion QPS. WSS can mitigate application-layer DDoS attacks such as HTTP Flood, Slow attack, POST Flood, etc. Introduction to the main types of attacks and their mitigation methods:

HTTP Flood Attacks

- **Attack Introduction**

HTTP Flood refers to the attacks that attackers use proxy servers to simulate real users and continuously send a large number of requests to targeted websites. For example, attackers frequently send HTTP requests to certain dynamic or non-existent URLs to consume server performance or massive back-to-origin requests, until the targeted server goes down.

- **Protection Principle**

1. Threat Intelligence Database

Relying on big data analysis platform, WSS can collect logs of attack events and extract attack signatures (like IP, URL, User-Agent, Referer, etc.) in real time. In terms of the signatures, WSS evaluates risk levels and builds threat intelligence database accordingly. High-risk IP, UA, URL and Referer are distributed to PoPs in the entire network. Once a request matches a high-risk signature, the request will be blocked directly to enhance mitigation efficiency and avoid attack impact on websites.

2. Customized Policy Configuration

If requests do not match the high-risk signatures in the threat intelligence database, then customized policies (such as IP blacklist/whitelist, access frequency control for certain IP address) can be configured to mitigate attacks.

3. Auto-learning Based Log Analysis

WSS dynamically learns the access behaviors to the websites (such as access traffic to resources, behavior features, etc.) in real time and sets up a baseline of normal access of the websites.

4. Customized Policy Configuration

If requests are not compliant with the normal access baseline, Captcha (JS validation, META validation, etc.) will be enabled to verify and determine the access legitimate or not, in order to avoid false positive affecting normal requests. Verified requests are passed as legitimate access, failed requests are blocked, and signatures are added to the threat intelligence database.

WSS provides verification mechanisms via JS, META, 302 redirecting, captcha and etc. to effectively mitigate attacks and ensure user experience of normal access.

JS Verification

It determines whether requests are from normal users or attack tools via returning HTTP code 200 with embeded JS code as the verification key to the client-side. Generally normal client-side like browsers can parse JS code and resend a request to the URL with the verification key. WSS blocks requests from attack tools which cannot respond with expected behaviors.

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

META Verification

It determines whether requests are from normal users or attack tools via adding verification parameters to Meta tags as response to the client-side. Generally normal client-side like browsers can parse the verification code and resend a request the URL with the verification key. WSS blocks requests from attack tools which cannot parse the metadata or respond with expected behaviors.

Slow Attacks

• Attack Introduction

Slow attacks intend to initiate many connections to the target web server open via sending a partial request to the server in certain duration but never ending the request, in order to keep all the connections as long as possible. In this way, the target web server uses up its concurrent connection pool and denies additional connections from normal users. HTTP slow attacks mainly include Slow Headers attacks and Slow Post attacks.

Slow Headers Attacks: attackers use GET or POST requests to connect to targeted server and then continuously send the server with HTTP header messages without ending it. Resources on the targeted server are occupied, as the server still waits for the ending symbols and keeps the connections. When attackers send a large number of such requests, server resources are run out soon and services become unavailable.

Slow POST Attacks: attackers send POST request messages to targeted server to submit data, and the content length is set to a big value. But the message sent out every time is in a small size, so the targeted server waits for the incoming data, and keeps the connections open. In this way, server resources are occupied and consumed to cause service unavailable.

• Protection Principle

To mitigate slow headers attacks, WSS checks the expiration time of request headers and the maximum number of split packets, for example, characters “\r\n” missing in a considerably long duration.

To mitigate slow Post attackers, WSS sets a threshold for the total number of small packets, for example, the content-length is set to a big value but received data each time are very small.

POST Flood

• Attack Introduction

Attackers use attack tools or control zombies to send a large number of HTTP POST messages to targeted servers to consume their resources and make them incapable of responding to normal requests.

• Protection Principle

WSS can detect and block POST Flood attacks with access control policies (such as IP blacklist/whitelist, IP access rate, etc.), Cookie verification and other methods.

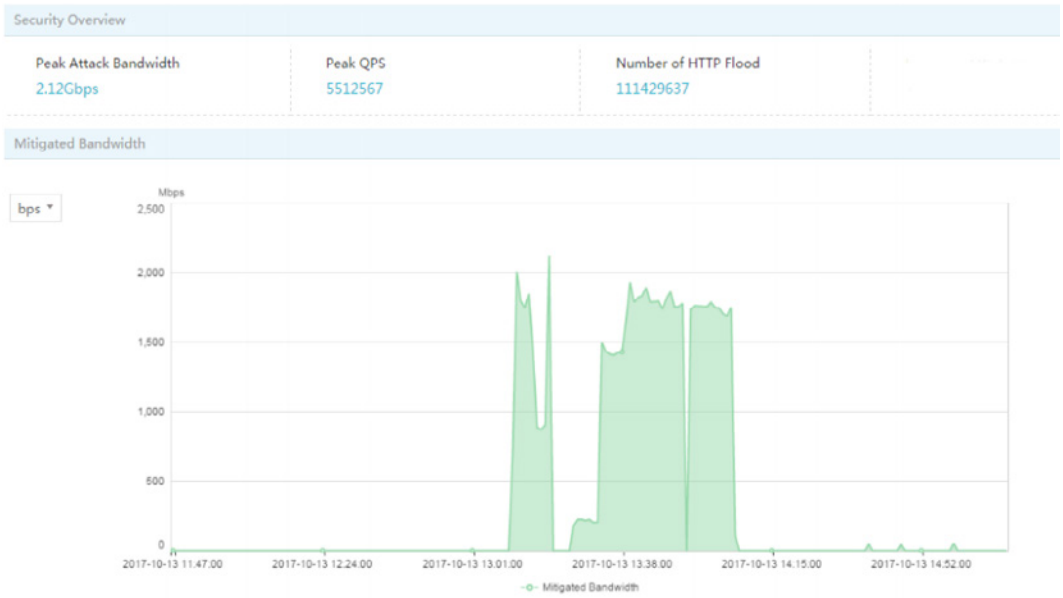
CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

Mitigation Visibility

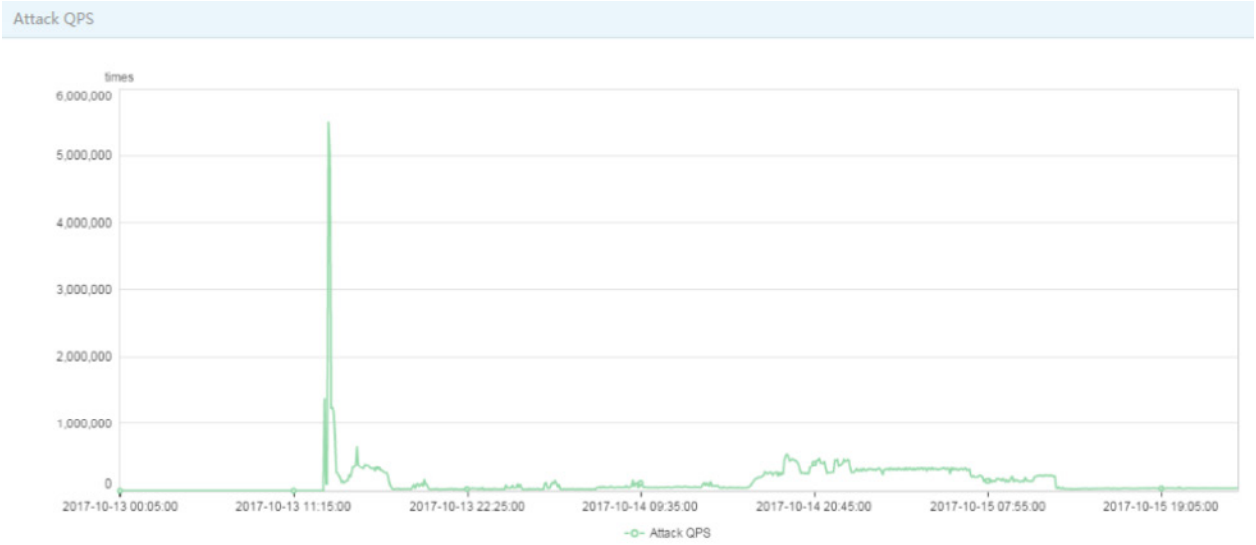
CDNetworks WSS displays the protection information of all types of DDoS attacks and users can view the protection results in real time to understand the security status of their business based on attack trends.

1. **Protection details are displayed to help customers better understand security status of their websites.**

   i. Peal Attack Bandwidth during certain period, real-time mitigated bandwidth, and normal bandwidth.



   ii. QPS of Application-Layer DDoS Attacks



CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

2. **It displays attack events by IP address, region, attak time, and attacked domain name.**

Protection Status

NO.	Attack IP	Location	Attack Time	Domain Name	Action
1	[redacted]	杭州/hangzhou/CN	2017-10-15 23:59:00	www.[redacted].com	deny
2	[redacted]	杭州/hangzhou/CN	2017-10-15 23:58:00	www.[redacted].com	deny
3	[redacted]	杭州/hangzhou/CN	2017-10-15 23:57:00	www.[redacted].com	deny
4	[redacted]	杭州/hangzhou/CN	2017-10-15 23:56:00	www.[redacted].com	deny
5	[redacted]	杭州/hangzhou/CN	2017-10-15 23:55:00	www.[redacted].com	deny
6	[redacted]	杭州/hangzhou/CN	2017-10-15 23:54:00	www.[redacted].com	deny
7	[redacted]	杭州/hangzhou/CN	2017-10-15 23:53:00	www.[redacted].com	deny
8	[redacted]	杭州/hangzhou/CN	2017-10-15 23:52:00	www.[redacted].com	deny
9	[redacted]	杭州/hangzhou/CN	2017-10-15 23:51:00	www.[redacted].com	deny
10	[redacted]	杭州/hangzhou/CN	2017-10-15 23:50:00	www.[redacted].com	deny
11	[redacted]	杭州/hangzhou/CN	2017-10-15 23:49:00	www.[redacted].com	deny
12	[redacted]	杭州/hangzhou/CN	2017-10-15 23:48:00	www.[redacted].com	deny
13	[redacted]	杭州/hangzhou/CN	2017-10-15 23:47:00	www.[redacted].com	deny
14	[redacted]	杭州/hangzhou/CN	2017-10-15 23:46:00	www.[redacted].com	deny
15	[redacted]	杭州/hangzhou/CN	2017-10-15 23:45:00	www.[redacted].com	deny

3. **Provides detailed information of intercepted IP addresses, including IP location, attack type, attack times, etc. to help customers deal with later attacks.**

Attack IP Details

Attack IP	Location	Total access	Attack type	Attack times
[redacted]	Vietnam	343,059,628	CC	343,059,628
[redacted]	China	/4,721,128	CC	/4,718,407
[redacted]	South Korea	5,673,886	CC	5,673,677
[redacted]	China	5,516,055	CC	5,287,010
[redacted]	China	1,657,284	CC	1,657,256
[redacted]	Vietnam	1,179,762	CC	1,179,762
[redacted]	China	850,673	CC	850,645
[redacted]	Hong Kong	841,344	CC	841,176
[redacted]	China	768,542	CC	768,514
[redacted]	China	626,018	CC	625,682
[redacted]	China	565,994	CC	565,980
[redacted]	China	556,953	CC	556,521
[redacted]	China	500,142	CC	500,114

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

Web Acceleration

WSS consists of ISP PoPs distributedly deployed all around China and it provides both static and dynamic web acceleration services. For static acceleration, it distributes contents onto all service nodes of the entire network with the intelligent caching technology. Cache mechanisms can be customized according to customer needs, for example, mechanisms by directory or by extension names can be realized to meet different requirements. Then the intelligent scheduling technology can dispatch visitors' requests to the nearest service nodes, which provides visitors the required contents. In this way, the pressure on the origin can be relieved and the access speed as well as user experience can be enhanced.

For dynamic contents, WSS could accelerate access speed with intelligent routing, content compression and other technologies that are developed by CDNetworks independently. The details are as below:

Intelligent Routing

There are many problems for the default transmission routes on public network, such as random failure, low connectivity, high time delay and these problems can seriously affect the speed to respond to problems. If such problems happened, service quality of user's request cannot be ensured. The optimal route selection technology developed independently by CDNetworks can effectively improve the response speed of websites.

WSS globally probes and detects the entire network, calculates each transmission route according to their weighted values intelligently, avoids faults on public network or the current congested routes, and selects the optimal, overall shortest most stable route. And also, transmission routes can be switched in real time according to actual network situations to ensure the best transmission effect, solving problems like over long transmission routes or instable network quality.

Content Compression

With the same transmission speed, less the bytes transferred, shorter time needed. Using technology of transmission content compression that developed by independently by CDNetworks, WSS can compress the data to be transferred to reduce the transferred total data amount and shorten the transfer time. The compressed data will be uncompressed at the output terminal to ensure the completeness of requested data. For example, WSS compresses a response sized in 100K to 30K through the dynamic accelerated network and un-compresses the content back to 100K at the edge nodes close to the end users.

Supports HTTPS Business

For secure data transmission, SSL encruption is appleid for more websites. CDNetworks provides seamless deployment, non-certificate deployment and SNI deployment all three deployment plans for HTTPS business to meet customers' requirements.

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

Seamless Deployment

Seamless deployment means users' certificates and private keys will be transferred and deployed in encryption without manual intervention to ensure the security of encrypted certificate file and content service. Certificate content will be reviewed and validated intelligently by scheduling center to ensure the certificate security and shorten the deployment time.

Deployment without Certificates

CDNetworks supports non-certificate deployment plan for customers (like banks and securities) that demand for high-level security of data protection but prefer not to provide private keys. In this case, customers only need to install a private key server provided by CDNetworks on the origin server to decrypt the private key. In this way, PoPs can build normal SSL connections with the client-side without customers' private keys, to ease the concerns of private key exposure, but acceleration is enabled for user experience.

SNI Certificate Deployment

With the Server Name Indication (SNI) technology of CDNetworks, multiple certificates can be deployed on one IP address. In this way, more than one HTTPS customer can share a set of IP addresses allocated for acceleration, so that fully utilized resources can improve acceleration effect and access experience.

Product Value

Zero Deployment and Zero Maintenance for Easy Access to Professional Mitigation Services

It does not require changing the existing network topology, and the professional service, combined mitigation and acceleration seamlessly, is enabled only via adding a CNAME record. Moreover, professional security experts provide 24/7 one-to-one service for quick response, in-depth understanding, and quality service.

Big Data-Enabled Security for Business Continuity

Relying on big data analysis platform and threat intelligence database, CDNetworks WSS conducts attack signature and correlation analysis in the cloud. The built-in threat assessment model can predict the attack trends and risks automatically. WSS can also deploy mitigation policies quickly to the entire network against high-risk attacks in advance, aiming to avoid customer business interruption

Efficient Emergency Response

CDNetworks WSS can provide professional one-to-one dedicated service in advance of unexpected large-scale attacks, it can respond timely to provide various contingency plans to enhance customer business continuity.

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

Intelligent Acceleration improving User Experience

Based on a globally distributed intelligent acceleration network, CDNetworks WSS enables end users to access website through the best service PoPs to improve access speed and effect. In this way, it can avoid server congestion by concurrent requests from many users and ensure service quality. At the same time, WSS can also effectively deal with cross-ISP and cross-region bottlenecks, solving the problem of instability from network fluctuation.

About CDNetworks

Founded in January of 2000, CDNetworks Science & Technology provides global solutions and services that cover content distribution and acceleration, server hosting and renting and network optimization for ISP. It's a premier comprehensive service provider of CDN and IDC. CDNetworks was publicly listed on Shenzhen Stock Exchange in October, 2009.

Headquartered in Shanghai, CDNetworks Science & Technology also has three offices in other three global cities in China: Beijing, Guangzhou and Shenzhen. CDNetworks also has set up subsidiaries in America, Hong Kong, Malaysia, Tianjin, Nanjing, Jinan and other places all 9 of them. In Xiamen and Silicon Valley of US, it has set up a R&D center in each place. There are over 2,000 employees in CDNetworks and more than 60% of them are in research and development. Our customers cover a wide of range of industries and types of portals, from Internet companies in streaming media, gaming, e-commence, search browsers and social media to governments, enterprises and various ISPs. At present, our customers are up to 3,000 and we are proud to say that our company is second to none in this industry in terms of number of customers and business range it covered.

Holding the Business License for Cross-region Value-added Telecommunications Business (IDC, ISP) issued by Ministry of Industry and Information Technology of China, CDNetworks Science & Technology is also a member to Asia-Pacific Network Information Centre (owning Autonomous System) and a member to China Internet Network Information Center (owning Autonomous System).

CDNetworks Science & Technology Enjoys Many Firsts in This Industry

- First publicly listed company in China that is specialized in CDN and IDC
- The most profitable CDN and IDC company in China
- The first company in China that has developed CDN platform independently
- The first company in China that has developed the technology of dynamic acceleration
- The first company in China that has developed the CDN content distribution platform with cloud architecture
- Largest CDN content distribution platform in China in terms of scale
- The first CDN company in China that has passed the compliance certification of PCI DSS V3.0

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com

Quality Global Resources

A complete coverage of ISPs in China, and in cooperation with big three telecommunication companies (China Mobile, China Telecommunications, and China Unicom) and two specialized network (China Education and Research Network and China Science & Technology Network). CDN content distribution and acceleration nodes of CDNetworks cover the entire globe and besides its nearly 500 domestic nodes, CDNetworks has deployed almost 60 nodes overseas, in San Jose, Los Angeles, Dallas, Chicago, New York, London, Amsterdam, Paris, Mumbai, Singapore, Sydney and other cities. Its service has expanded to developed countries and regions in 6 continents, North America, Europe, Asia, South America, Asia and Oceania. Acceleration requirements from customers around the world can be supported with our quality resources.

Rich Experience of Professional Experience

With 15 years of operation experience in acceleration and improvement of Internet user experience, CDNetworks is a premier service provider of Internet acceleration and it also has been serving Four Web Portals (sina.com, souhu.com, qq.com and 163.com) for many years. CDNetworks knows clearly the basic structure and applications of the Internet in China.

CDNetworks is committed to providing its customer with one-to-one professional service and in serving many foreign and domestic big brands with quality acceleration, it has collected many years of service experience, which in turn can help us better meets customers' needs of informationization and business development.

One-Stop Sales Network

In Beijing, Shanghai, Guangzhou, Shenzhen and other cities or regions, CDNetworks has set up subsidiaries or offices that cover regions with more than 80% of China Internet users. Business consultation and business process are available in each office of CDNetworks for 7*24, with fast response and other one-stop sales service.

CDNetworks Inc., 1500 Valley Vista Dr. Diamond Bar, CA 91765, USA Phone: (877) 937-4236 Email: info@cdnetworks.com