CXNet Anti-DDoS Protection Shield
Secure your online operation from DDoS attack

FACTS:

DDOS ARE INCREASINGLY USED BY CYBERCRIMINALS AS THEIR PREFERRED WEAPON TO BREACH CYBERSECURITY; MORE THAN DOUBLE OF COMPANIES IN 2017, COMPARED TO 2016, HAVE EXPERIENCED A DDOS ATTACK.

ACCORDING TO DELOITTE, IN 2017, 60% OF DATA CENTER OPERATORS, 41% ENTERPRISE AND GOVERNMENT INSTITUTIONS REPORTED THAT DDOS ATTACKS HAVE BURST THEIR INTERNET BANDWIDTH.

IT IS ESTIMATED THAT OVER 10 MILLIONS DDOS ATTACKS SHALL TAKE PLACE IN 2017, AT APPROXIMATELY OVER 27,000 ATTACKS PER DAY.

One of the most difficult yet common threats to protect against is the distributed denial of service attack, also known as a DDoS attack. According to a report by Kapersky Lab and B2B International, a single DDoS attack can potential cost an enterprise its reputation, customers and over USD $1.6 million, or USD $5,000 - $19,999 per hour.

To protect your servers and network from DDoS attacks, CXNET has worked together with top tier providers to provide an infra anti-DDoS solution that secures users with multi-layers against DDoS attacks.
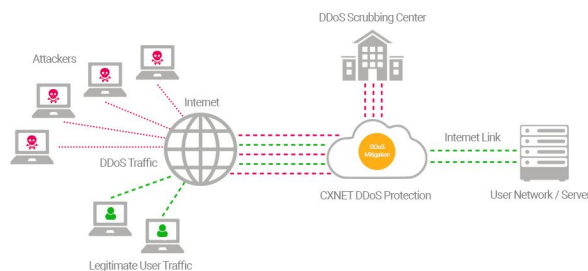
KEY BENEFITS:

Business as usual during DDoS attack
With ours augmented filtering, by limiting query quota and the support of early detection + intelligent mitigation solutions, we shall able to stop DDoS attacks before they reach your equipments.

Protection against volumetric attacks
By working together with top tier infrastructure provider, we are able to defense your business from even the largest of DDoS attacks—over hundreds of gigabits per second—with advance DDoS attack mitigation bandwidth.

Clean pipe network
Our DDoS defense system shall clean all traffic, eliminating malware, spam and viruses before go into your equipment.

Advanced monitoring system
Examine closely and thoroughly on network traffic in real-time to identify anomalies, quarantines attack packets and blocks malicious traffic.

Gain attack mitigation insights
Our customer portal provides you a transparent visibility on attack mitigation and reporting before, during, and after an attack.

Get expert service
Consultancy, configuration and support for complex DDoS mitigation.
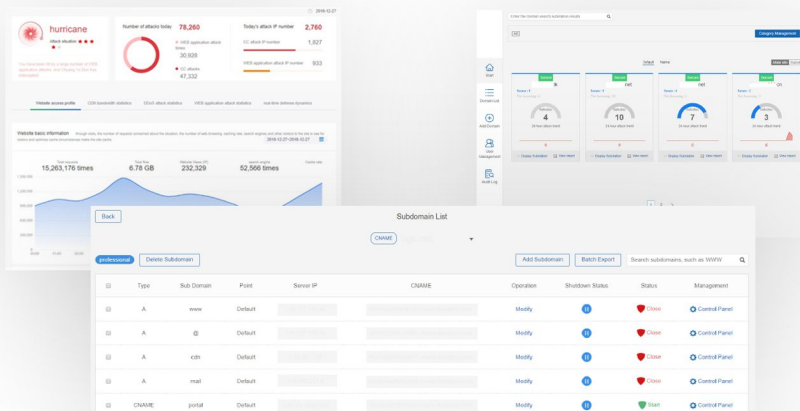
cxnet

CXNet Web Application Firewall

Protection against Web-based Application Attacks

In addition to protect against volumetric/L3+L4 DDoS attacks, CXNet Anti-DDoS has also included Web Application Firewall (WAF) that shall protect your applications, APIs and mobile app backend against common web exploits that could affect the availability of your application, data leakage, compromise security or consume excessive resources.

CXNet WAF protects web applications from attacks by filtering and monitoring HTTP traffic between your web application and the Internet. CXNet WAF allows you to define your own protection policies, including but not limited to IP addresses, HTTP headers, HTTP body, or URI strings, which shall protect against common attacks patterns, such as SQL injection or cross-site scripting (XSS).
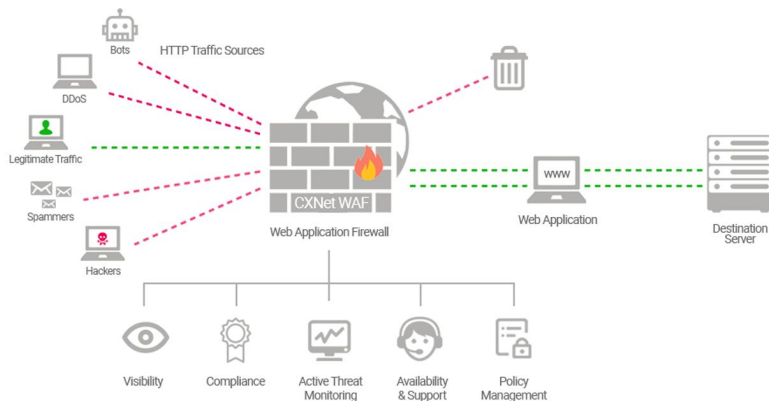
CXNet WAF Control Center provides a single point of control for all your WAF deployments. It facilitates management, helps ensure up-to-date policies, and provides the tools necessary to deliver ongoing security for your applications wherever they reside.

CXNet WAF protects against OWASP Top 10 Application Security Risks:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

CXNET DATA Solutions Pte. Ltd.

CXNET Data Solutions is a leading service provider in Cloud Hosting, IP Transit, and Internet Security, and with infrastructure covers across North America, Europe and Asia region.

🌐 www.cxnet.com.sg
✉ info@cxnet.sg

cxnet