

## CLOUD-BASED ANTI-DDoS

Protecting your company's infrastructure, applications, Internet access, and E-business

### **BENEFITS**

- Your business stays online and available during attacks
- Robust and dynamic mitigation
- Industry-fastest response time
- No capital expenditure required
- Scalable services to meet your needs
- Comprehensive Service Level Agreements (SLAs)
- No need to change network providers or infrastructure

### **FEATURES**

- Multiple, global scrubbing centres
- Specialists in mitigating Application Layer attacks
- Defensive capacity of more than 100 GB
- Network agnostic
- Compatible with your existing infrastructure, security policies, and hosting and network providers
- No pre-requisites

"Nexusguard is well known for their high degree of expertise in stopping DDOS attacks."

Jimmy Chen  
Manager, Business Developing  
Division  
eASPN Taiwan

### **PROTECTION FROM THE THREAT OF DDOS ATTACKS**

Distributed Denial of Service (DDoS) attacks are a current and growing threat to all companies with business online. In a recent survey, Arbor Networks found that DDoS attack bandwidth increased 102 percent over the previous year. During a DDoS attack, botnets of hundreds of thousands of infected computers launch legitimate and illegitimate traffic at your company's internet infrastructure. Overwhelmed by massive amounts of traffic, your company's web site cannot respond to real customers and users. Your site goes down.

Such DDoS attacks are widespread and affect even the largest and most security-conscious organizations, including global businesses such as Google and agencies such as the South Korea Defence Ministry. Companies dependent upon online availability for their economic survival must establish a scalable, economically viable anti-DDoS defense for their business.

Malicious hackers have many motivations for using DDoS attacks against your business, including politics, blackmail, profit, and competition. The consequences for your business can be devastating, including:

- Loss of service
- Loss of revenue
- Loss of reputation
- Loss of business
- Loss of customers
- Loss of company

DDoS attacks target many types of business and organization, including:

- Financial Institutions
- Successful Enterprises
- E-Commerce
- Government Agencies
- ISPs and their Customers
- Online Gaming

Despite the dramatic increase in DDoS attacks, many companies make anti-DDoS defense a low priority. Unfortunately, protection from a network carrier or firewall is easily overwhelmed.

### **NEXUSGUARD PROTECTION**

Nexusguard protects online businesses from DDoS attacks:

- Quickly, effectively, and with minimal business impact
- Using proprietary cloud-based strategies
- With greater protection capacity and granular analysis than server-based and premise-based solutions

## Cloud-Based DDoS Protection

Nexusguard's three-part protection strategy includes Network, Infrastructure, and People.

### ***NEXUSGUARD NETWORK***

- Uses more than 6 Asian network carriers, plus global, American, and European carriers
- Carrier diversity allows better routing optimisation
- No single point of failure
- Delivers superior network performance to Asian end-customers

### ***NEXUSGUARD INFRASTRUCTURE***

- Scrubbing centres globally distributed to handle global attacks: Taipei, Hong Kong, San Jose USA, London, Manila
- Mitigation of all DDoS attacks
- Over 100 GB of network capacity to handle attacks

### ***NEXUSGUARD PEOPLE***

- Specialize and focus on DDoS mitigation
- World-class multinational experts providing consultation and support in English, Mandarin, Bahasa Indonesia, Malay, Tamil, and Tagalog
- Develop scripts, policies, and filters to deliver real-time response to Zero-Day Application Layer attacks
- Thorough knowledge of Asian networks, routing, market conditions, and trends
- Experienced, flexible, ready to employ their combined know-how, skills, commitment, and expertise
- Respond to all modes of attacks

### ***MODES OF PROTECTION***

Nexusguard offers multiple modes of protection from DDoS attacks, including the following:

- Always On: Nexusguard constantly monitors for malicious traffic to customers and stops all attempted DDoS attacks immediately.
- On Demand: Customer responds to attacks with Domain Name Server (DNS) / Border Gateway Protocol (BGP) redirection into the Nexusguard cloud, providing immediate and effective mitigation.

### ***PROTECTION DURING ATTACKS***

Nexusguard filters out all malicious traffic and forwards all legitimate traffic for ordinary processing. Active development and employment of scripts and filters stops all attacks, to ensure site availability. Your company's site stays up and running.

### ***BUSINESS VALUE SOLUTIONS***

So often, potential customers of anti-DDoS services are hampered by restrictive offerings that don't add business value. By contrast, Nexusguard has developed solutions for IDC Operators and regional ISPs that provide real protection for the data centre or network, and a progressive revenue stream.

Nexusguard has developed a suite of services that address the needs of online businesses. We understand the levels of support and protection that Asian-based online businesses require. From our expertise in DDoS mitigation to our deep understanding of the applications deployed on online sites, we have strong experience in maintaining site availability, while reducing the interaction needed from the customer's network team.

### ***GET PROTECTION NOW!***

Gartner says, "Any business or government agency that depends on its Internet presence and is operating without DDoS protection is placing its operations at unacceptable risk." Contact Nexusguard now to gain the protection from DDoS that your company needs.



Suite 1602, 16/F, Nina Tower 2  
8 Yeung Uk Rd, Tsuen Wan  
New Territories, Hong Kong  
contact@nexusguard.com

© 2011 Nexusguard Limited. All rights reserved.