Defending against increasingly sophisticated DDoS attacks

Managed DDoS protection from IBM

Executive summary
In today’s technology-driven business world, high-profile cyber attacks on governments, corporations and financial markets are becoming increasingly common. As the threat of security breaches continues to grow, the types of attacks are becoming more diverse and complex. Distributed denial-of-service (DDoS) attacks occur when hackers overload servers with requests, rendering the network unavailable to its intended audience. Traditional DDoS attacks are now giving way to more sophisticated DDoS attacks that stress applications by initiating open-ended sessions or conversations. Because of these developments, many companies are not equipped to prevent DDoS attacks and are at risk of experiencing unplanned downtime, reduced revenue and damaged reputation.

In order to defend against DDoS attacks more effectively, companies need to move beyond traditional defenses such as firewalls and intrusion-prevention systems—and find a way to deflect attacks before they ever reach the network. And in the event of an attack, they need to respond to and mitigate the situation efficiently. Downtime is simply not an option.

This white paper examines the current threat landscape related to DDoS attacks and introduces a strategic approach that uses five critical components—preparation, mitigation, around-the-clock monitoring, response and intelligence—to help you more successfully address both present and future DDoS attacks.
Industry trends and the current threat landscape

As business platforms continue to evolve, organizations rely on technology that is increasingly instrumented, interconnected and intelligent. This advanced technology introduces many opportunities; however it also comes with a new set of vulnerabilities and challenges. Companies—especially those in highly targeted industries like the financial, retail, healthcare and government sectors—must remain ever-vigilant against cyber attacks in light of today’s current threat landscape and the need to protect their reputations.

Traditional DDoS attacks overload a network with a high volume of traffic, consuming bandwidth to key servers and services. The attacks overwhelm the network and the application capacity with traffic surges up to hundreds of gigabits per second (Gbps). But recently, more sophisticated DDoS attacks have become increasingly common. These advanced attacks stress applications by initiating open-ended sessions or conversations. Additional stressors push central processing unit (CPU) cycles and memory limits; for example by sending encrypted requests, causing the target to exhaust resources in the process of decryption. Traditional defenses of firewalls and intrusion-prevention systems are no longer enough.

Pressured to address the urgent threat of DDoS attacks, businesses may find themselves diverting attention and critical resources (technical and executive alike) away from high-priority objectives to deal with this consuming and highly publicized problem. The impacts can be monumental and varied, and can be a smokescreen for subsequent breaches of sensitive data or systems. DDoS attacks can risk the consumer base which has come to depend on around-the-clock access and also weaken the brand image. Consequentially, organizations need to develop an actionable defense plan to avoid these repercussions.

A recent survey conducted by Ponemon Institute found that two-thirds of banks had been hit by at least one DDoS attack in the last 12 months, and each institution averaged an estimated 2.8 such attacks. The study further estimated an annual cost of US$3,000,000.¹

Planning the multifaceted approach to help defend against DDoS attacks

To build a defense against DDoS attacks, organizations should develop a plan that is both proactive and reactive. Ideally, a DDoS response plan should help:

- Integrate the right mix of processes, people, and technology that can defend the entire infrastructure from both volume-based and application-based DDoS attacks
- Plan for and implement the resource capacity that can scale within the specific risk tolerances determined by your organization
- Plan for normal volume surges as well as DDoS attacks by testing and setting a baseline for current network, web, and application resources (this includes private virtual environments as well as public cloud service providers)
- Leverage and optimize current architectures for traffic limiting and load balancing within the existing environment
- Use an edge device or a farm of devices—with the capacity to handle anticipated surges—to cleanse edge traffic, with “bad” traffic scrubbed or dropped
- Include alert and notification procedures, assigned priority levels, call-out lists, response and escalation actions, communication activities and other considerations
Response plans must be routinely tested along with all other disaster recovery plans. After the incident is resolved and the business has returned to normal, the closing step should be to review the overall process and make recommendations and action plans for continuous improvement.

You may want to adopt a multifaceted defense strategy—but without the available resources and technology, it can be a challenge. IBM has identified a five-component approach that includes preparation, mitigation, around-the-clock monitoring, response and intelligence. The following section will describe this approach and how IBM can help you adopt it.

**IBM can help you plan for DDoS attacks**

IBM provides a broad portfolio of security offerings to help organizations defend against DDoS attacks.

---

**Services**

IBM Global Technology Services® (GTS) offers managed DDoS protection

By combining a world-class security team from IBM and an intelligent network platform from our alliance with Akamai, we can help push the security perimeter into the cloud. With managed DDoS protection from IBM, all Internet traffic is cloaked and routed through the Akamai cloud-based Kona Site Defender. This means that any malicious traffic is kept away from your infrastructure. By absorbing the attack preemptively, you can benefit from sustained performance and availability, allowing you (and us) to focus on advanced attacks and not waste time fighting generic attacks. Meanwhile, IBM specialists provide the expertise to manage DDoS protection—so your staff can focus on other critical priorities. Our five-component approach includes preparation, mitigation, around-the-clock monitoring, response and intelligence.

---

**The five critical components of our managed DDoS protection:**

<table>
<thead>
<tr>
<th>Preparation</th>
<th>Mitigation</th>
<th>Around-the-clock monitoring</th>
<th>Response</th>
<th>Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Readiness plan</td>
<td>- Proactively stop attacks before they impact a client’s network</td>
<td>- Monitor traffic and server health</td>
<td>- A trained team for containment, eradication, recovery and identification of secondary attacks</td>
<td>- Knowledge and awareness of internet threat conditions</td>
</tr>
<tr>
<td>- Response protocols</td>
<td>- Manage DDoS technology to keep current and effective</td>
<td>- Near real-time metrics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

*Figure 1. Our multistep, proactive approach to DDoS can deliver more efficient attack detection and accurate incident escalations.*
Preparation
- IBM helps orchestrate and connect on-premise solutions with cloud solutions.
- IBM can perform a tabletop exercise designed to give you a better understanding of the impact of a worst-case scenario and help ensure your organization’s readiness to respond to attacks.

Mitigation
- The cloud-based Akamai technology provides continual protection—not simply becoming available in a crisis—and can absorb a number of threats before they ever touch the network.
- We can help you during an attack with mitigation recommendations for hybrid attacks across a variety of vendor DDoS technology.
- We have the expertise to span multiple layers of DDoS protection, web application firewall tuning and incident response recommendations from IBM specialists with years of accumulated knowledge.

Around-the-clock monitoring
- IBM helps manage and support layers of appliance and cloud solutions with an around-the-clock global security operations center.
- IBM specialists look for anomalies in network traffic that exceed a normal threshold and also monitor for situations where the DDoS attacks may be a diversion to a real attack that may have been occurring somewhere else in or around the network.
- We help monitor the overall server health and manage DDoS technology to keep it more current and effective.

Response
- We provide a 24-hour-per-day hotline to call for assistance if you believe you are experiencing an incident.
- Our highly skilled team can help contain and eradicate malicious traffic, recover the network and identify secondary attacks.

Intelligence
- IBM has broad visibility into many kinds of DDoS attack trends and can leverage knowledge and insights on behalf of our client base.
- We use near-real-time metrics to draw conclusions about your IT environment.

Layered protection
IBM provides numerous layers of protection that can supplement any DDoS solution. Here are a few highlights.

Check Point DDoS Protector
For organizations who want an additional level of security within the data center, we also can provide managed DDoS protection using Check Point DDoS Protector. With Check Point DDoS Protector, appliances block DDoS attacks within seconds with multi-layered protection and up to 12 Gbps of performance. Check Point DDoS Protector can help extend a company’s security perimeters to block destructive DDoS attacks before they can cause damage.

IBM SmartCloud
IBM SmartCloud® has software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) offerings which can be used as an alternate website or resource while the primary site is suffering a DDoS attack. The advantage of using this approach is that you have a secondary system where the load can be distributed dynamically in case the first system fails, helping to reduce the downtime of the websites.
IBM QRadar
The IBM QRadar® security information and event manager (SIEM) is designed to help detect anomalies. This product can help monitor network traffic, detect behavior associated with DDoS attacks and alert response staff at the first signs of attack. Techniques include watching for unusually high volumes of traffic to one or a few hosts, Internet control message protocol (ICMP) floods, excessive transmission control protocol (TCP) and user datagram protocol (UDP) packets, traffic originating from darknets and detecting deviations from an automatically built up baseline norm. More complex correlations can be created by consuming near-real-time threat intelligence, such as that provided by IBM X-Force. Additionally QRadar has built-in correlation rules for helping to identify potential DDoS attacks at the application layer as well. QRadar collects telemetry from hundreds of IBM and non-IBM sources. It can also distinguish between preliminary DDoS activity, which may be a diversion for an advanced attack, and the attack itself.

Conclusion
Creating a DDoS attack defense strategy is critical to surviving both current and future attacks. Traditional methods, such as firewalls, are no longer adequate. Security requires long-term strategic planning, adapting for new threats and integrating solutions into a streamlined technology environment—while at the same time keeping a constant vigil on the current situation.

Why IBM?
We have over two decades of cybersecurity assessment and response operations. Our around-the-clock hotline responds to over 500 calls every year, and each call is answered by a skilled analyst. Each member of our analyst team has years of experience, multiple industry certifications, and the hardware, software and forensic tools to perform the tasks.

For more information
To learn more about managed DDoS protection from IBM, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/services/security

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: ibm.com/financing
© Copyright IBM Corporation 2013

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
August 2013

IBM, the IBM logo, ibm.com, IBM SmartCloud, Global Technology Services, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

1 “A Study of Retail Banks and DDoS Attacks.” Ponemon Institute
2 Based on IBM internal analysis.