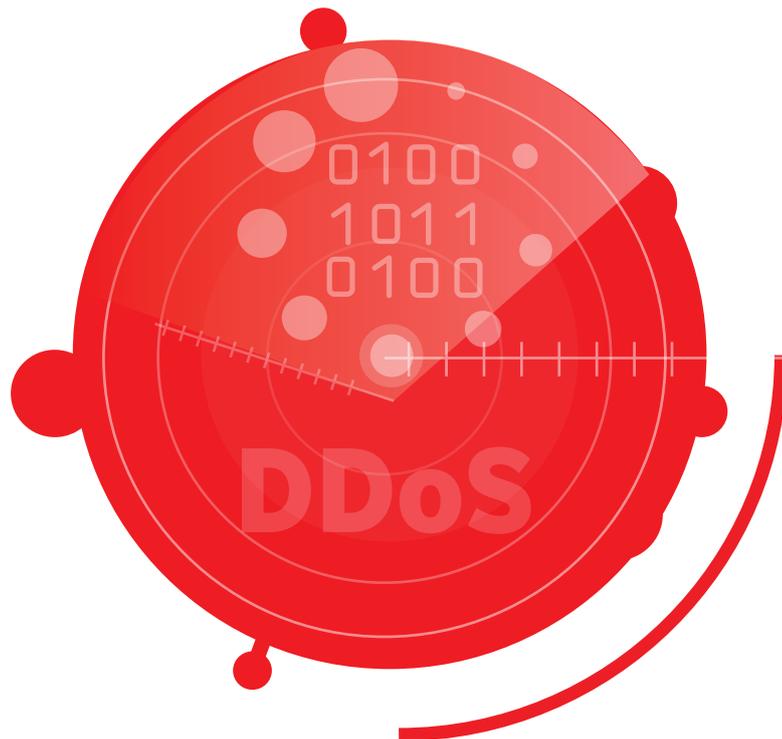


Being Ready to Face DDoS Challenge



Vodafone
Power to you



Introduction

With competitive pressures intensifying and the pace of innovation accelerating, recognising key trends, understanding their implications and, where appropriate, responding decisively is essential to remain successful. Vodafone has created five insight papers which discuss many significant business and technology trends shaping Enterprises today and into the future. We discuss their implications and make recommendations as to the steps businesses need to take.

- **The new customer relationship in the digital age**
- **The rise of the borderless enterprise**
- **Understanding the impact of the connected revolution**
- **The changing role of the IT department in a cloud-based world**
- **The importance of mobility for tomorrow's enterprise**

This paper describes our thinking relating to understanding the impact of and the threats from the connected revolution. If you are interested in topics such as the growth of the Internet of things, machine-to-machine (M2M), the opportunity it represents for businesses, the requirements for success and ensuring security, then you will find this of interest.

Executive Summary

From targeting gaming and financial websites, DDoS has become a tool to attack the image of brands. Re-evaluating security infrastructure taking this into account is imperative.

Cyber threats are increasingly getting sophisticated with attackers trying to exploit holes for every new software or program. At the same time, an age old threat continues despite advances in technology and building sophisticated defence mechanisms – DDoS.

DDoS (Distributed Denial of Service) refers to the denial of access to a web property due to a flood attack aimed to drown it with traffic and take it offline. Till a decade ago, it referred to a basic attack aimed at making a web site unavailable to legitimate users. This type of high bandwidth attack typically originated from a large number of geographically distributed bots. Today, though, its implications go beyond mere saturation of crashing of a site.

DDoS attacks can be caused by software bugs aimed at crashing or freezing a service or network resource, or bandwidth limits through a flood attack of ranges exceeding 100Gbps. Not only the sheer size of the attacks but even the tools, targets and techniques have changed with time.

Finance, gaming and e-commerce were the targets in the initial days of DDoS attacks. But today, any site is vulnerable and can be the target of anyone with a grievance, perceived or real, by customers who wish to harm the brand image by making their website inaccessible.

This whitepaper explores the trend in the market, the technology used in DDoS and how ready businesses are prepared to tackle this threat at the point of entry.

- Online servicing key to brand image
- Denial of service attack on image
- IP solutions insufficient
- Designing layered protection
- Nipping denial of service in the bud



19.4% is the projected CAGR from 2012-2016 for prevention of DDoS services

Rising DDoS Attacks- Market Trends

Research ^[1] firm International Data Corporation (IDC) corroborates the evolving trend in DDoS from hacktivism to financial gain to disguising more targeted attacks exploiting the weaknesses and vulnerabilities of some of the world's largest and most powerful organizations.

In 2012, there was a sharp increase in the frequency, bandwidth volume, and applications orientation of these attacks. "As these attacks surged in prevalence and sophistication, organizations were often caught unaware. Embedded capabilities were quickly overwhelmed and outages were readily apparent on the Web. This is driving the need for proactive solutions to protect customer's infrastructure from current and future attacks," says Christian A. Christiansen, Vice President, Security Products & Services research at IDC.

Some of the trends predicted include volumetric attacks being the preferred mode of DDoS attacks due to their effectiveness and relative ease of execution with botnets that can send a bandwidth flood, crippling most enterprise infrastructures. But with that, advanced hybrid attacks that include application layer and encrypted traffic, are also expected to increase.

Jeff Wilson, principal analyst for security at market research firm Infonetics Research ^[2] points out, "DDoS prevention appliances are the first line of defense against brute-force attacks. With the number, size and coverage of DDoS attacks on the rise, we expect revenue for DDoS prevention solutions to grow in the healthy double digits through 2014."

- 87% of all attacks monitored in 2013 lasted less than one hour
- 54% of attacks in 2013 were over 1Gb/sec, up from 33% in 2012

According to their estimation, Global DDoS prevention appliance revenue grew 30 percent in 2012, to \$275 million and will continue to grow at a 25 per cent CAGR from 2012 to 2017, thanks to the transition to IP and data, massive increases in capacity, and a new role as a juicy and highly visible target for attacks.

Vodafone Business Services

Being Ready to Face DDoS Challenge

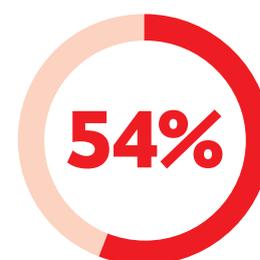
This increasing threat and as well as the increasing criticality of the web for brand promotion and marketing activities, the demand for on premise equipment market is expected to increase too, though cloud-based solution is another emerging trend as it provides protection against advanced application and SSL-based attacks as well as large-scale volumetric attacks, the IDC report goes on to say.

The Research and Market findings to show an increasing demand for cloud services as one of the major trends. Cloud services help lower cost, offer easy installation and operations, making it the preferred choice of SMEs especially. Even large enterprises with on-premise security services are now switching to the cloud model.

As a result of this, development perpetrators of DDoS attacks will have additional targets. DDoS prevention solution providers are forging partnerships to address the evolving nature of attacks and enhance the protection, where quality of protection plays a major role.

3Arbor Networks' ^[3] analysis of the market trends in third quarter 2013 shows DDoS attack size accelerating rapidly:

- 54% of attacks were over 1Gb/sec, up from 33% in 2012
- 37% of attacks were in the 2-10 Gb/sec range, up from 15% the previous year
- 44% growth in proportion of attacks over 10 Gb/sec, to 4% of all attacks
- More than 350% growth in the number of attacks monitored at over 20 Gb/sec, as compared to the whole of 2012
- For 2013, an average DDoS attack stood at 2.64Gb/sec, up 78% from 2012
- 87% of all attacks monitored so far this year last less than one hour
- Largest monitored and verified attack size increases significantly to 191Gb/sec



54% of attacks in 2013 were over 1Gb/sec, up from 33% in 2012

Vodafone Business Services

Being Ready to Face DDoS Challenge

350% growth in the number of attacks monitored at over 20 Gb/sec in 2013 over 2012

A layered approach that combines on-premise and cloud based protection against the full spectrum of DDoS attacks seems the best option under the circumstances.

High-valued services such as managed security are important due to the increasing complexity of the size, frequency and complexity of DDoS attacks making security and availability top priorities of organisations. Since traditional security products such as firewalls or intrusion prevention systems cannot prevent volumetric and application-layer DDoS attacks, products providing layered protection are now available.

The attack techniques have become technologically more advanced. Not only is the connection bandwidth the target, but all the components of an organisation's network that form the security infrastructure, such as Firewall/IPS devices, also become the targets. Applications such as HTTP, HTTPS, VoIP, DNS and SMTP are also targeted for DDoS attacks. Such multi-vector attacks are difficult to defend against, and serve their purpose effectively.

The growing access to resources on the Internet has also enabled even novices to benefit from do-it-yourself attack tools to generate and execute a DDoS attack successfully.

These shared resources and multi-tenant nature of IDCs help attackers cause much collateral damage. Since most IDCs run high-profile, mission-critical applications, they become ripe targets for extortion. Virtualization of data centres, while beneficial to customers, also compounds security challenges.

DDoS attacks can be of three types:

- Volumetric Attacks are aimed at saturating the link within the target network or between the target network and the rest of the Internet.
- State – Exhaustion Attacks aim to block the connection state tables present in many infrastructure components such as load-balancers, firewalls and the application servers themselves.
- Application Layer Attacks isolate applications or service at Layer-7. They are the deadliest kind as they can be very effective with capability of one attacking machine generating a low traffic rate.

Businesses Prepare for DDoS Attacks

An article by Eric Chan, Regional Technical Director, Southeast Asia & Hong Kong, Fortinet, in the magazine 'Networks Asia',^[4] says that one of the first steps is creating visibility. A comprehensive window to give IT administrators a bird's view of the organization's entire IT environment, and complete control is the first step to protect against attacks.

The second step is to be able to identify the offensive ISPs to counter attacks in a specific manner.

The protection device needs to be able to assess the nature and severity of a threat and suggest appropriate solutions to counter the threat.

Reporting tools and a logging and correlation mechanism will help IT administrators of ready businesses assess the overall threat better and evaluate the security position of their organization.

Enough bandwidth to withstand spikes in traffic, bandwidth management features to implement policies and allocate predefined bandwidth based on user, group, time of day and other criteria, addressing complex IT infrastructure in mixed, multi-platform and multi-tenant environments – the list seems long and the demands for security high.

But with experience and exchange of knowledge, best practices have emerged enabling developing solutions that address this long list of security requirements of organisations.

Mike Paquette, chief strategy officer of Corero Network Security in Enterprise Systems Journal lists the following four best practices that can help businesses ready their systems to mitigate the effects of DDoS attacks.

Step 1: Create a DDoS response plan

Have a clear security strategy to protect against and counter the effects of a DDoS. Plan the security infrastructure in advance with your ISP. This is critical since usually, by the time the attack reaches the data center, the network infrastructure is already overwhelmed and it is too late to mitigate the situation. A network-based DDoS protection of the ISP can stop these attacks on time. Plan for steps for mitigation and have in place disaster recovery measures.

Step 2: Layer your DDoS defense

Create a data centre edge-based DDoS protection system so that operators can customize detection and mitigation for the unique applications running in their data centre. Also create an on-premise DDoS defense solution since increasingly, DDoS attacks target application layers.

Step 3: Protect information

Information management and security are critical to protect Web applications. Create and implement a data protection strategy. Ensure password policies and implement stringent authentication tools. Also provide comprehensive network security with firewall, intrusion prevention, and DDoS defence as key parts of the infrastructure in which the Web application server is deployed.

Step 4: Protect DNS infrastructure

The Internet domain name system (DNS) is a distributed naming system that enables easy recall of websites rather than complicated IP addresses (e.g. 192.168.0.1). Because it is distributed, many organizations use and maintain their own DNS servers to make their systems visible on the Internet.

Evolve a DNS infrastructure protection plan with DNS service providers since these are also targeted by DDoS attacks to deny access to the service. The mechanism is similar to protecting other Web applications and DDoS defense should be deployed in the DNS infrastructure.

It's necessary to evolve a DNS infrastructure protection plan with DNS service providers since these are also targeted by DDoS attacks to deny access to the service.

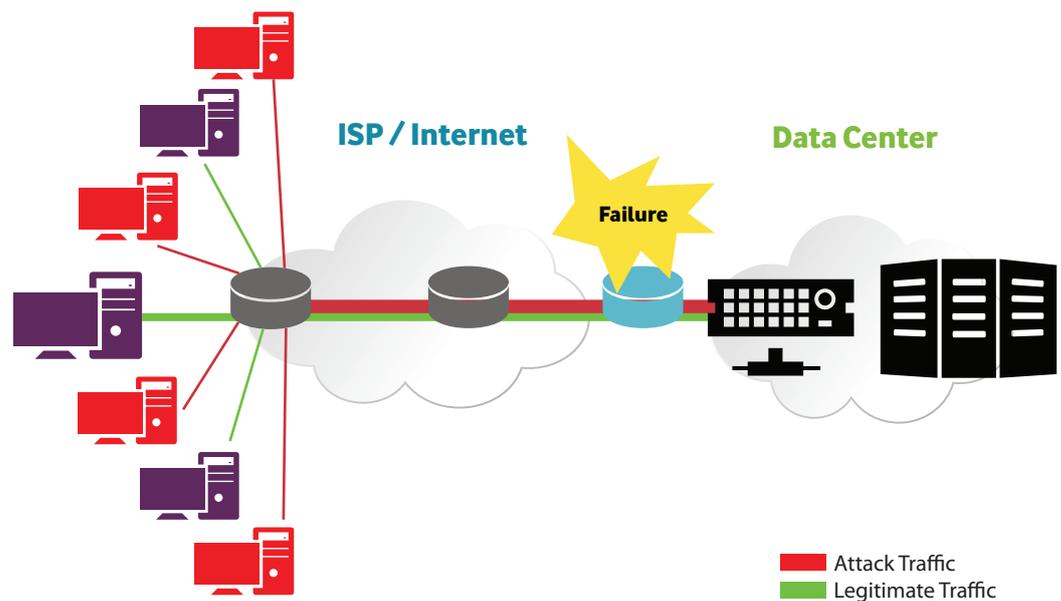
Vodafone Business Services

Being Ready to Face DDoS Challenge

The Limitations of Firewall and IPS Devices

Familiar with security threat of other nature – such as data thefts, hacking, etc., - organisations have beefed up their security with products such as firewall, intrusion prevention system (IPS) and web application firewall (WAF). Many a time, the general perception is that these devices are enough to protect their organizations from DDoS attacks as well. Though these devices are essential for sound security, they cannot counter the evolving DDoS attacks, which are becoming smarter.

While IPS devices block break-in attempts and protect data, firewalls are more of policy enforcers to prevent unauthorized access to data and services. They are critical security tools but cannot assure network availability during DDoS attacks. The table below provides other reasons why traditional, on-premise security products such as firewall and IPS devices do not offer adequate DDoS attack protection:



Firewall and IPS Solutions Vis-à-vis DDoS

Limitations	Resulting Challenges
Vulnerable to DDoS Attack	<ul style="list-style-type: none"> • Because these devices are in-line, stateful devices, they are vulnerable and targets of DDoS attacks. • First to be affected by large flood or connection attacks.
Failure to ensure availability	<ul style="list-style-type: none"> • Built to protect against known (versus emerging) threats. • Designed to look for threats within single sessions, not across sessions.
Protection limited to certain attacks	<ul style="list-style-type: none"> • Address only specific application threats. • By default, they must allow common attack traffic such as TCP port 80 (HTTP) or UDP port 53 (DNS). Do not handle attacks containing valid requests.
Deployed in wrong location	<ul style="list-style-type: none"> • Very close to servers. • Too close to protect upstream router.
Incompatible with cloud DDoS protection systems	<ul style="list-style-type: none"> • Fail to interoperate with cloud DDoS prevention solutions. • Increase time for response to DDoS.
Lack of DDoS Expertise	<ul style="list-style-type: none"> • Require skilled security experts. • Demand knowledge of attack types before attacks.

Vodafone's security infrastructure provides Macro- and micro-level visibility-enabling proactive identification of threats and improving network performance.

As we can see, the firewall and IPS devices themselves become targets since they are designed to track every packet over every connection, they will be the first points of failure and choke even during moderate DDoS attacks.

DDoS solutions must protect asymmetric traffic that occurs due to inbound and outbound traffic from a single connection crossing different interfaces

Building a DDoS Solution

Firewalls and IPS/IDS devices often flaunt DDoS feature such as load balancers that can offer some relief from traffic floods. Your Telecom Service Provider too can help by blocking high volume traffic. But these may not solve the real problem.

While building a DDoS protection service, ready businesses consider the following factors.

- Ways to be accessible online at all times without impacting link performance.
- Cloud-Based DDoS protection should block high volume flood attacks to the enterprise, though the identification of the attack and setting up the mitigation may take a few minutes.
- State-less Inspection to counter the vulnerability of traditional perimeter security devices (firewalls and IPS) that rely on tracking session state to enforce security policies and leaves them open to attacks designed to exhaust session state.
- Application Layer Protection to include the organization's Web servers and applications that run on them, protecting them from attacks targeted at them.
- Intelligent identification of Web Crawlers that are customised to mine enterprise websites for information or terms used to rank the sites during user searches. Sometimes Web crawlers behave like bots, causing some security vendors to block them.
- Customize policy settings since attacks can be targeted, giving no time to plan and act. The DDoS platform should enable easy capture of packets and use them for custom policy creation.
- Botnet Detection & Mitigation to handle the ever-changing nature of botnets by updating information daily for that day's threats. This way, security solutions can avoid preventing all bots, or letting harmful ones get through. Understanding bot behaviour is important for effective protection.
- Automated and Advanced DDoS Protection is important since organizations can find any downtime costly. The solution should automatically detect and prevent DDoS attacks with little or no user interaction—before services are degraded. It also offers simple fallback plans and resolution techniques when attacks cannot be readily identified and mitigated to speedup resolution. Moreover a good solution should recognize legitimate CDN traffic and will not accidentally block it.
- Visibility, Alerts & control to provide real-time visibility into attacks, blocked hosts and even packets. It should be flexible enough to allow operators to alter attack counter-measures and thresholds if required. It should alert security engineers of ongoing attacks that are blocked, as well as other network events that may require their attention.
- Real-Time and Historical Attack Forensics and Reporting in real time will help operators visually understand the actions taken by the appliance. Besides documenting these actions in audit logs, it should provide forensic reports detailing blocked hosts, host countries of attacks and historical trends. These easy-to-understand reports can also be given to peers or management to educate them on the threats to service availability and the steps taken to address the attacks.
- Asymmetric Traffic due to redundant links and ISPs can occur due to inbound and outbound traffic from a single connection crossing different interfaces. DDoS solutions must deliver complete protection for asymmetric traffic.

Managed DDoS Service from Vodafone



Vodafone, a global telecom service provider, offers solutions for DDoS mitigation. Arbor Peakflow SP, a network-wide infrastructure security, measurement and traffic-monitoring platform that addresses all critical requirements has been implemented, ensuring its customers first level protection against targeted or generic DDoS attacks. These include:

- Flow and Deep Packet Inspection (DPI) technologies,
- Macro- and micro-level visibility—enabling proactive identification of threats and improving network performance.
- Infrastructure Security for proactively detecting and mitigating network-wide anomalies. The Infrastructure Security functions include:
 - Detection, trace back and analysis of network anomalies that may be the result of DDoS attacks.
 - Analysis of dark IP traffic to determine infected hosts within the network.
- Vodafone Managed DDoS solution scales with its multi-tier detection architecture of collectors.
- The Portal Interface (PI) device provides a central reporting and management platform for managed services.
- Peak flow Collector Platform collects Net Flow Statistics from multiple routers and acts as a correlation engine syncing data sets between all network collectors and the PI system.
- Peak flow Threat Management System (TMS) is a vital component of the Peakflow Vodafone solution. It is a carrier-class Intelligent DDoS Mitigation System (IDMS) for multi-service converged networks that speeds remediation by coupling high-level threat identification with packet-level analysis.
- Vodafone will configure Managed Object in Peak flow CP.
- When a DDoS attack destined towards the Customer Managed Object occurs, the Peak flow SP system will detect a network anomaly and will subsequently trigger an alert in the system.
- The Peakflow SP system will then advertise a more specific route announcement to the Cleaning Centre Gateway Diversion router, thereby diverting the traffic destined towards the Customer Managed Object into the TMS for appropriate surgical mitigation.
- The TMS will perform the necessary counter measures for the type Customer Managed Object under protection, and will surgically mitigate clean traffic from attack traffic.
- After mitigation by the TMS, clean traffic is sent back to separate Cleaning Centre Re-Injection Gateway router. Traffic would then get routed towards the destination PE adjacent to client.
- The clean traffic will be forwarded towards the appropriate Customer Edge router or Aggregation router and finally make its way towards the Customer Managed Object.
- Traffic from the Customer Managed Object will traverse its normal path back into the Internet.
- When the Peakflow system detects that the DDoS attack has stopped, it will withdraw its more specific route announcement towards the route reflector, which will subsequently update the Core and send traffic towards the Customer Managed Object via its normal route.

References

- 1 Denial of Service Attacks Surge and Expose Enterprise Infrastructure Vulnerabilities and New Needs, says IDC
<https://www.idc.com/getdoc.jsp?containerId=prUS24044213>
 - 2 Research and Markets on Global Distributed Denial of Service (DDoS) Market 2012-2016
<http://www.infonetics.com/pr/2012/2H11-DDoS-Prevention-Appliances-Market-Highlights.asp>
 - 3 Arbor Networks releases global DDoS attack trends data
<http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5026-arbor-networks-releases-q3-global-ddos-attack-trends-data>
 - 4 A multi-layered approach to combating DDoS attacks: Networks Asia
<http://networksasia.net/article/multi-layered-approach-combating-ddos-attacks-1372683826>
-

<https://www.vodafone.in/ReadyBusiness>

Vodafone Business Services. This document is issued by Vodafone in confidence and is not to be reproduced in whole or in part without the prior written permission of Vodafone. Vodafone and the Vodafone logos are trademarks of the Vodafone Group. Other product and company names mentioned herein may be the trademarks of their respective owners. The information contained in this publication is correct at the time of going to print. Such information may be subject to change, and services may be modified, supplemented or withdrawn by Vodafone without prior notice. All services are subject to terms and conditions, copies of which may be obtained on request.



Join Us

 [company/vodafone-india](https://www.linkedin.com/company/vodafone-india)

 [#ReadyBusiness](https://twitter.com/ReadyBusiness) | [@VodafoneIN_VBS](https://twitter.com/VodafoneIN_VBS)

 [Vodafone Business Services](https://www.youtube.com/VodafoneBusinessServices)