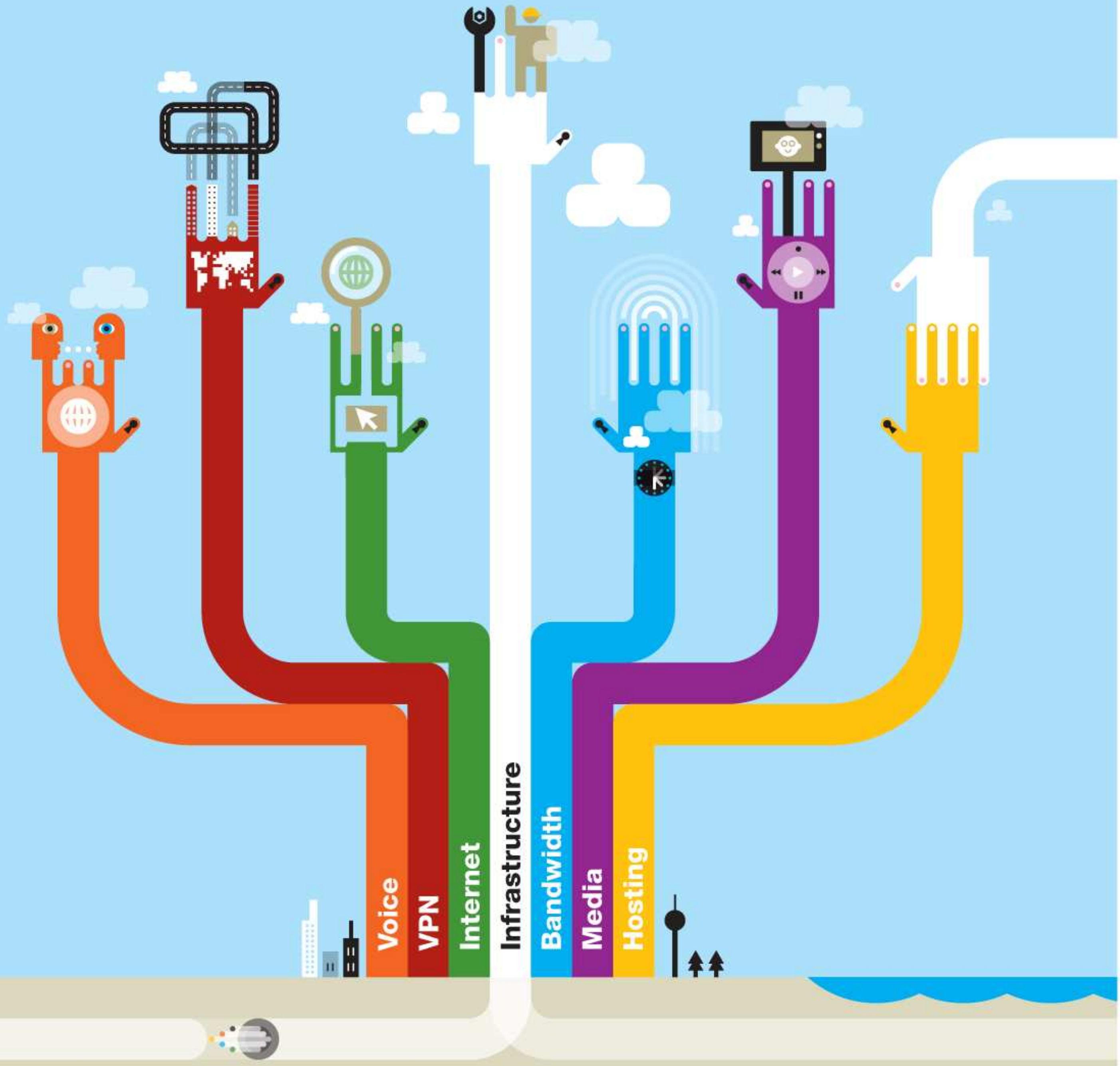
Service Description
DDoS Mitigation Service

interoute
from the ground to the cloud



Interoute, Walbrook Building, 195 Marsh Wall, London, E14 9SG, UK
Tel: +800 4683 7681 Email: info@interoute.com

www.interoute.com

Contents

Contents

1 Introduction

This document outlines the Distributed Denial of Service Mitigation service (DDoS Mitigation Service) and value proposition for you. This is an enterprise service only. It is intended to answer all the questions you are likely to encounter on a sales call. Should you need any further clarification, please call Jeff Finch our Security Services Product Manager.

2 An Overview

Any enterprise that uses the Internet for its core business has a nightmare scenario where it is no longer able to gain revenue due to its systems being down due to attack. Some types of online businesses are more likely to suffer these attacks than others. However all enterprises will recognise that without this type of mitigation service there is a risk that their business and its revenue could be compromised.

2.1 Introduction to DDoS Attacks

DDoS attacks are attempts to make a computer or network device unavailable to legitimate users. A common attack method is to bombard an attack target with massive volumes of requests to open a connection. The target host cannot cope with such a large number of session requests and simply stops responding, rendering it useless. The DDoS attack also swamps a customers Internet connection, blocking traffic from legitimate sources.

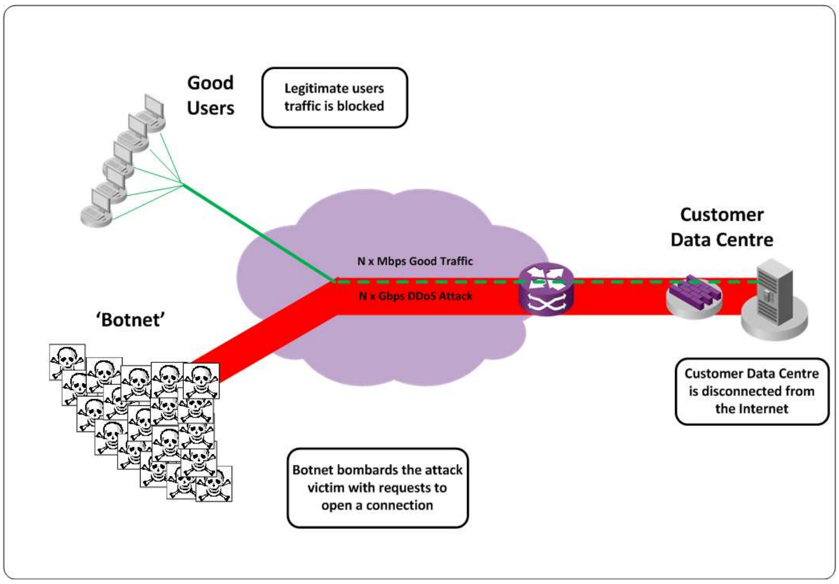

Good Users
Legitimate users traffic is blocked
Customer Data Centre
N x Mbps Good Traffic
N x Gbps DDoS Attack
'Botnet'
Customer Data Centre is disconnected from the Internet
Botnet bombards the attack victim with requests to open a connection

Figure 1: High-Level DDoS Attack

The reasons for DDoS attacks vary, however common motivations are political, competitive, criminal, social activism or even a disgruntled ex-employee. The person who wants to attack a specific individual or organisation (the sponsor) is rarely the same person who actually conducts the DDoS attack. The sponsor typically pays an unrelated attacker to initiate and control the attack.

A common attack method is for an attacker to use thousands of compromised Internet connected computers to form a 'botnet' which simultaneously send multiple requests to open a network session with a host or network device owned and operated by the attack target. As the attack grows the traffic generated by the botnet aggregates and begins to swamp the targets Internet connection and hosts machines, effectively disconnecting them from the Internet and rendering them useless.

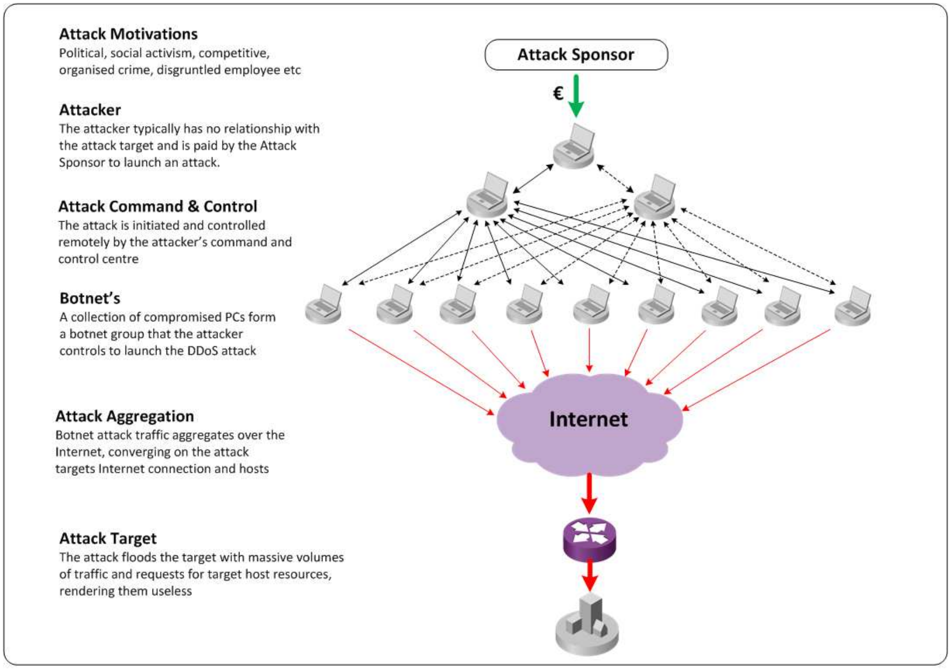

Attack Motivations
Political, social activism, competitive, organised crime, disgruntled employee etc
Attacker
The attacker typically has no relationship with the attack target and is paid by the Attack Sponsor to launch an attack.
Attack Command & Control
The attack is initiated and controlled remotely by the attacker's command and control centre
Botnet's
A collection of compromised PCs form a botnet group that the attacker controls to launch the DDoS attack
Attack Aggregation
Botnet attack traffic aggregates over the Internet, converging on the attack targets Internet connection and hosts
Attack Target
The attack floods the target with massive volumes of traffic and requests for target host resources, rendering them useless
Attack Sponsor
€
Internet

Figure 2: Typical structure of DDoS Attacks

2.2 Implications of DDoS Attacks

DDoS attacks are unfortunately a fact of life on today's Internet, with the frequency, size and sophistication of attacks increasing each year. For example, in 2002 the largest reported attack was400Mbps, however by 2009 this had increased to 49Gb (as reported by Arbor Networks). It is not unusual in these attacks to see packet requests between 1.2m and 2.4m per second. DDoS attacks can have serious implications for enterprises.

From an enterprises perspective a DDoS attack can render their Internet connection or targeted host(s) useless within seconds, effectively disconnecting them from the Internet.

A content provider or content distribution networks (CDNs) business is all about being able to reliably and consistently deliver an increasing array and volume of content types to end users without any degradation to service quality. In an increasingly competitive content/CDN market, where the cost of switching between providers is relatively low, DDoS attacks represent a significant threat to a content providers and CDNs ability to deliver their content to end users.

From an ISPs perspective DDoS attacks carry the following risks:

- Backbone, upstream and peer connections become congested impacting unrelated customer services and potentially increasing Interoute's upstream costs.
- Network switch and router resources are consumed potentially causing outages

- Unrelated customers suffer outages caused by an attack, impacting their relationship with Interoute, potentially breaching SLAs and consequently resulting in service credits being due to the customer
- Negative PR

3 What is the service

3.1 General description and positioning

This service is for enterprise customers only.
Interoute's DDoS Mitigation Service is a cloud-based service that provides customers Interoute Internet connections and Internet facing hosts with Mitigation against the threat of DDoS attacks. During an attack a customer's traffic is redirected through our DDoS Mitigation platform which intelligently identifies and drops malicious attack traffic in our core network before it reaches a customer port where it will cause the most damage.

Historical techniques for dealing with DDoS attacks, such 'black hole' routing, stopped all traffic from reaching the DDoS attack target. Whilst 'black hole' routing is effective at protecting a site or data centre it can also achieve the same result as the DDoS attack because it blocks all traffic, good and bad.

Interoute's DDoS Mitigation Service uses Network Collectors and Threat Management Systems located at strategic POPs in our IP backbone, to analyse, identify and discard malicious DDoS attack traffic before it reaches a customers port. By dropping the malicious traffic in our backbone the customers Internet connection and hosts do not become saturated with DDoS attack traffic and can remain operational.

3.2 How does DDoS Mitigation Work?

DDoS Mitigation works by re-directing Internet traffic destined for a customer's host or network infrastructure through a number of Threat Management Systems (TMSs). The TMSs analyse a customers traffic flow based on peak traffic rates, attack signatures and packet inspection techniques based on protocols, IP addresses, port numbers and other data to identify and drop malicious DDoS attack traffic.

Normal Operating Conditions
Under normal operating conditions customers' traffic will flow to/from the Internet via the most direct path across Interoute's IP backbone, as illustrated below:

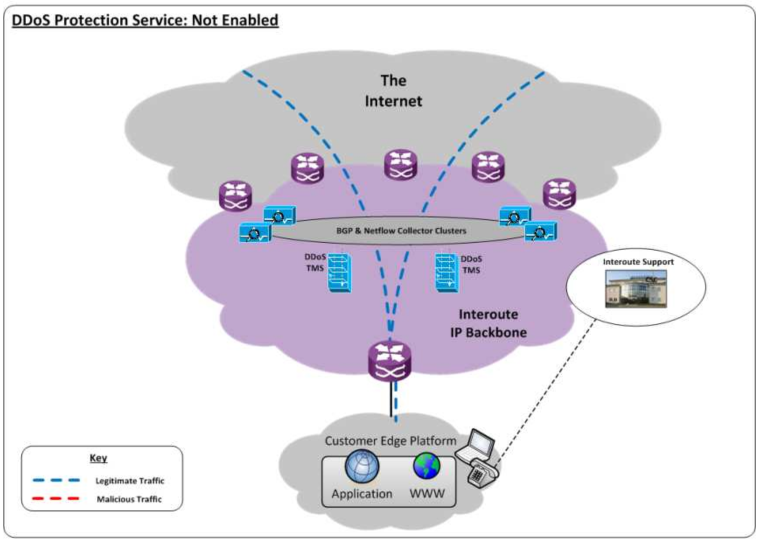


Figure 3: Normal Operating Conditions – Before an attack

A common attack method is to saturate a target device with massive volumes of traffic or requests for computer resources. As the attack traffic grows the customers Internet connection quickly becomes saturated, blocking legitimate traffic and effectively disconnecting the customer from the Internet.

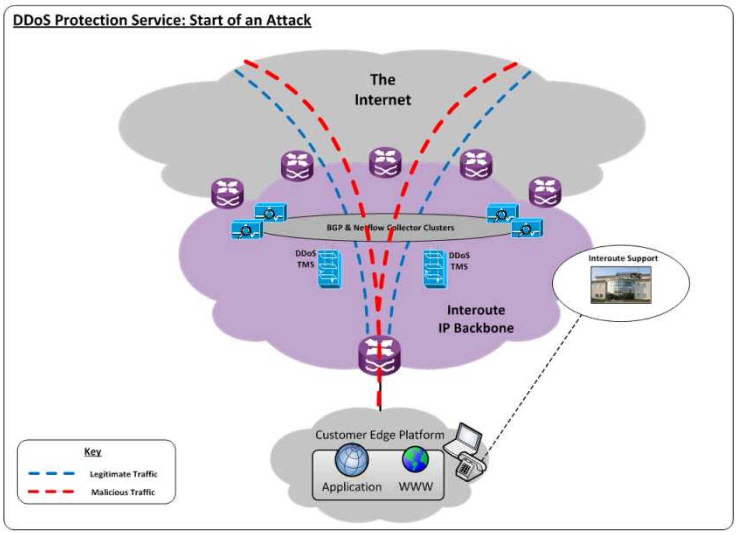


Figure 3: The start of an attack

Attack Detection & Service Enablement

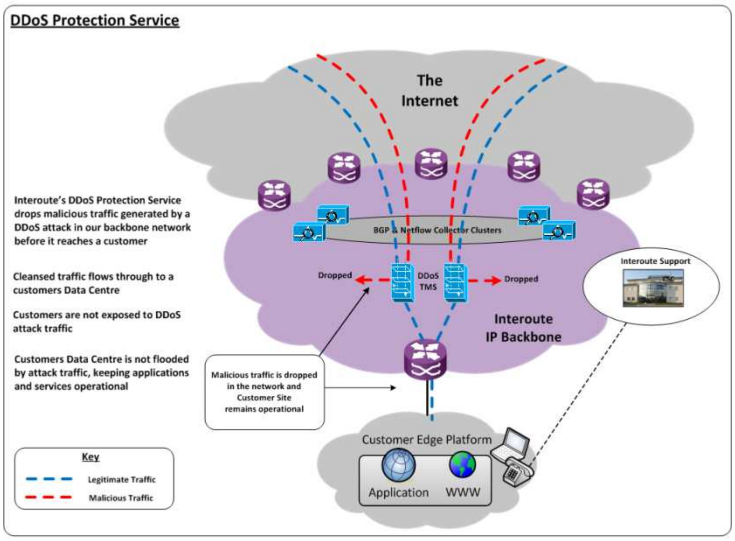
When an attack is detected the customer contacts the Interoute Customer Service Centre (CSC) to request that their DDoS Mitigation Service is enabled, quoting their DDoS Mitigation Service ID (SID). A task will be raised to enable DDoS Mitigation, which will only be triggered by customer consent, ensuring that Mitigation is not activated and traffic is not re-directed due to non malicious activity known to the customer, such as large file transfers, a special event that causes a large increase in traffic or network testing.

If Interoute detects a volumetric attack we will contact the customer’s designated authorized person to advise that an attack is occurring and confirm that it is acceptable to enable DDoS Mitigation.

From opening a trouble ticket DDoS Mitigation is enabled within 60 minutes. Once enabled a customer's traffic is redirected through the TMSs in our IP backbone.

Cleaning and Mitigation

When DDoS Mitigation has been enabled, a customer’s traffic is redirected through Interoute’s IP backbone so that it flows through our DDoS Mitigation Platform. The customers traffic flow is analysed using complex filters to detect network layer anomalies that could be associated with a high bandwidth ‘flood’ attack or ‘cloaked’ application layer attacks. Once detected the malicious traffic is discarded by the TMS in our IP backbone where there is plenty of bandwidth without interrupting the flow of legitimate traffic destined for a customers Internet port.



Interoute’s DDoS Protection Service drops malicious traffic generated by a DDoS attack in our backbone network before it reaches a customer

Cleansed traffic flows through to a customers Data Centre

Customers are not exposed to DDoS attack traffic

Customers Data Centre is not flooded by attack traffic, keeping applications and services operational

Malicious traffic is dropped in the network and Customer Site remains operational

Figure 4: DDoS Mitigation Enabled

Unprotect

Once the attack has finished Interoute will contact the customer to confirm that their traffic can be set to unprotect by a NOC engineer. From this point a customer’s traffic will return to its normal routing path.

DDoS Mitigation Service Architecture

Interoute’s DDoS Mitigation Service is based upon clusters of BGP and Netflow Collectors and Threat Management Systems (TMS) which are all deployed at strategic locations within our IP backbone.

The BGP and Netflow Collectors are part of a network wide security and traffic monitoring platform that collects key network and application layer performance data and metrics, enabling security threats to be quickly identified. When unusual network or application behaviour is captured, such as a large spike in traffic or application anomaly cause by a 'cloaked attack' an alert is generated. An unusual level of network or application behaviour will generate an alarm in the Interoute NOC for further analysis and action. The collectors are installed as two redundant clusters in secure facilities at geographically diverse locations in Interoute's network.

The TMSs provide network and application layer analysis and mitigation to discriminate between legitimate and malicious traffic. The TMSs identify and surgically discard DDoS attack traffic, before it reaches the customers Internet port without interrupting the flow of legitimate traffic.

Each TMS supports a throughput of up to 10Gbps and there are currently two deployed within our backbone, enabling Interoute to protect customers against DDoS attacks that generate up to 20Gbps of peak traffic.

Reporting
Post-attack reports are available on request that will provide the customers with a per attack summary and attack statistics.

This will provide customers with a real-time view of their traffic and associated attack statistics, including:

- Alerts
- Alert dashboard
- Application report
- GeoIP data (country, region, cities etc)
- IP packet information (header, ports etc)
- Top talkers (internal, external etc)

4 Commercials

4.1 Pricing

The pricing structure for DDoS Mitigation is based on the following factors, all of which will be selectable options in the Security Services Price Tool:

- The number of Managed Objects
- Standard Service (Enhanced Service is specific to customers and based on CDD requests).

4.2 Managed Objects

Interoute's DDoS Protection Service provides customers with protection against DDoS attacks based on autonomous system number (ASN) or IP addresses. These details are captured in a customer specific network-based software element on our DDoS Protection Service call a 'Managed Object'.

Each individual Managed Object can be configured to protect an ASN or blocks of IP addresses, but not both.

If a customer has their own ASN they can choose whether they wish to be protected at the ASN or IP address level. For customers who do not have their own ASN they must be protected at the IP address level.

Typically, a single managed object will be sufficient for an enterprise customer. However customers may want to choose multiple managed objects dependent on where they see the potential risk from attack.

4.3 DDoS Pricing

The following Billing plans are available for Interoute's DDoS Mitigation Service:

- An initial non-recurring charge
- A monthly fixed rate charge for the term of the contract

The non recurring charge is a fixed fee that is payable on a per customer basis. It is important to note that the non recurring charge is payable on acceptance of order and not refundable. The monthly fixed rate charge is based upon the number of managed objects that a customer requires to be protected.

4.4 Ordering

The service is ordered via an order form and standard terms and conditions. For the order to progress a Data Capture Form will be required with the following information.

The customer's autonomous system number or IP addresses to be protected are captured using an Interoute DDoS Mitigation Data Capture Form which will be provided to customers by their account team. An example of the information to be captured is as follows:

EXAMPLE 1: Managed Object for IP address blocks

Description	ACME protection for external facing hosts & network		
	ASN	**IP Address / Subnet Mask**	**Description**
1	N/A	220.1.1.0 / 24	Ecommerce systems
2	N/A	221.1.1.0 / 24	Web & mail systems
3			

EXAMPLE 2: Managed Object for an ASN:

Description	[ACME protection for corporate ASN]		
	ASN	**IP Address / Subnet Mask**	**Description**
1	12345	N/A	ACME ASN
2			
3			

Figure 6: Example Customer DCF

5 How is the service implemented and supported

Interoute's DDoS Protection Service is managed by our NOC in Prague on a 24x7x365 basis. The customer is not required to change any of their existing infrastructure to make the service operational.

DDoS attacks can occur very quickly and require a very fast response from Interoute's Operations teams. Our priorities when managing DDoS attacks are as follows:

1. Protect our related and unrelated customer services
2. Use all reasonable endeavours to keep customers services operating as normally as possible .

Interoute's approach to managing DDoS attacks brings together the necessary technical, commercial, legal and marketing functions to effectively manage the implications of a DDoS attack to our network and our customers.

Action / Function	Responsibility / Purpose
M3 Operational Response	A team that includes the necessary representatives to technically, commercially and legally manage Interoute's response to the attack, provide regular status updates internally and to customers, engage marketing to manage external communications if required, etc
Enable Customers DDoS Protection (applicable if the customer has purchased DDoS Protection)	Protect the customers infrastructure by enabling their DDoS protection
Protect connections to upstream networks	Request upstream providers to 'black hole' customer traffic if there is a risk of Interoute's upstream connections becoming congested.
Protect Interoute backbone network	Implement 'Black holing' of customer traffic and filtering at the edge of Interoute's network if there is a risk that our own network could be compromised.
Disconnect customer from Interoute network	If at any point there is a risk that Interoute's own network could be compromised Interoute reserves the right to shutdown the customers port(s) until it is safe to reconnect the customer. This action could be undertaken whilst other measures are implemented (e.g. enabling black holing).

Table 2: Support Response

6 Contractual

The terms and conditions for Interoute's DDoS Mitigation Service offers the following service levels:

- Service Installation (credit backed)
- Service Availability (credit backed)
- Critical and Non-critical Incident Response (target, non-credit backed)
- Service Enabling Response (target, non-credit backed)

7 Key benefits

Key benefits of Interoute’s DDoS Protection Service are as follows:

1. Customers Internet Services remain operational even when being attacked, maximising the availability of the customers website, on-line services and applications

2. Interoute’s DDoS Mitigation discards malicious traffic within our IP backbone before it reaches the customer where it would do the most harm.

3. Provides customers with a key service that positively contributes to a customer’s business continuity planning (BCP) processes.

4. Affordable insurance against the threat of DDoS attacks

5. Integrated with our Internet Services, all of which is managed by Interoute’s CSC/NOC 24x7x365, providing customers with a single point of contact, management and accountability.

6. Interoute’s DDoS Protection leverages Interoute’s massive next generation pan European IP backbone, which has the scale to effectively respond and protect against DDoS attacks.

7. Interoute’s DDoS Protection Service is priced as a simple monthly recurring fee with no hidden usage based charges.