

Cable & Wireless Guernsey Attack Mitigation Service – Specific Terms and Conditions

C&W ATTACK MITIGATION SERVICE

The C&W Attack Mitigation Service provides You with a solution to help protect Your site against Distributed Denial of Service (DDoS) attacks by analysing incoming traffic, detecting attack conditions and blocking the malicious traffic whilst letting genuine traffic through.

ATTACK MITIGATION SERVICE SPECIFIC TERMS AND CONDITIONS

These C&W Attack Mitigation Service Specific Terms and Conditions should be read in conjunction with the C&W Data Centre General Terms and Conditions. Where there is conflict, these Attack Mitigation Service Specific Terms and Conditions supersede the C&W Data Centre General Terms and Conditions.

1. DEFINITIONS AND INTERPRETATION

The Data Centre General Terms and Conditions include definitions. These definitions are in addition.

“Black Holing” means discarding all data destined for a particular IP Address so that it does not disrupt the flow of data to other IP Addresses.

“Business Day” means a day, Monday through Friday that is a normal working day in the Bailiwick of Guernsey.

“C&W” means Cable and Wireless Guernsey Limited.

“Critical Change” is a change without which there will be a serious business impact on Your online operation.

“Distributed Denial of Service (DDoS)” means a form of electronic attack involving multiple computers, which send repeated requests to a server (web site) generating false traffic and rendering it inaccessible to valid users.

“Event Log” means a log file where an Operating System or a Hosted Application stores information about several events for future analysis.

“Hosted Application” is a World Wide Web or other application hosted at Our site containing World Wide Web, Internet or intranet content.

“Hosting Solution” means a collection of services taken as a single solution provided by Us to You.

“IP Address” means the identifying number of a computer attached to the Internet. Every computer must have a unique IP Address. IP Addresses are written as four sets of numbers separated by full stops: for example 204.171.64.2.

“Non-Critical Change” is a change such as a request for information which has no immediate or significant impact on the running of Your online operation.

“Operating System” means a computer programme installed on a server, which enables Your software and Hosted Applications to run on that server.

“Zone” means a single sub-division of the equipment used to provide the Attack Mitigation Service which contains IP Address and server information for the group of protected equipment and provides protection for that equipment only.

Cable & Wireless Guernsey Attack Mitigation Service – Specific Terms and Conditions

2. PROVISION OF SERVICE

- 2.1 We will provide You with the Attack Mitigation Service. The Attack Mitigation Service comprises two different elements of service – detection of an attack and the cleaning of the traffic directed towards Your site – and includes
 - 2.1.1 installation and maintenance of the Service on the relevant equipment owned by Us;
 - 2.1.2 configuration of a set of pre-defined monitoring parameters as specified by Us;
 - 2.1.3 monitoring of agreed parameters and status information via the Event Log.
- 2.2 **Monitoring and Detection** – This part of the Service provides You with a set level of passive monitoring of the incoming traffic entering Your protected Zone, building a baseline profile of normal traffic patterns and behaviour. Traffic flows are constantly monitored and compared to the baseline, looking for any deviations that might indicate an attack. If any abnormal or unusual behaviour is detected by Us, We will identify the target by its IP Address, start diverting traffic destined for the targeted Zone and begin mitigation.
- 2.3 **Cleaning and Mitigation** - When an attack is detected, traffic destined for the targeted Zone - and only that traffic – will be redirected by Us off the main path for inspection. Diverted traffic will be subjected to multiple layers of statistical analysis, active verification and anomaly recognition to identify malicious sources, reveal abnormal behaviour and discard packets that do not conform to the normal traffic pattern. This traffic cleaning is performed utilising the profiles of Your normal traffic behaviour gathered during the previous learning phase. Whilst traffic cleaning is underway it is envisaged that an increase in latency will occur.
- 2.4 This enhanced Service is designed to increase resilience to DDoS attacks. We will use Our reasonable endeavours to ensure that legitimate traffic is received as normally as possible during an attack, and that the site user experience is affected as little as possible. In an attack countermeasures will be deployed by Us to ensure disruptions to operations are minimised, and measures such as “Black Holing” will only be used by Us if all other measures have been deemed by Us to have failed.
- 2.5 We will work with You to identify when a DDoS attack is occurring and fine tune the Service to achieve maximum DDoS protection with minimum processing overhead and traffic disruption.
- 2.6 We will monitor the appliances used by Us to provide this Service (via ICMP and SNMP) and We will configure them via secure connections.
- 2.7 During the calendar month following the Service Delivery Date We will allow what We consider to be reasonable changes which will be covered by the connection charge. Thereafter We will perform a maximum of one Critical Change and five Non-Critical Changes to the Attack Mitigation Service in any calendar month. Further changes requested by You will be charged according to paragraph 7 below.
- 2.8 **Maintenance** - In the event of a hardware failure, We will repair or replace Our equipment within three Business Days based on reasonable endeavours.
- 2.9 **Upgrades** - We may periodically need to upgrade Our equipment to ensure the latest software versions are in operation. If We determine, in Our sole discretion, that an upgrade is necessary, We will work with You to schedule a time to make the necessary changes. You must allow Us to make these changes within five Business Days of receipt of the request from Us to do so.
- 2.10 If We determine that an emergency security change is required, or if You do not respond to Our

Cable & Wireless Guernsey Attack Mitigation Service – Specific Terms and Conditions

request to upgrade the equipment as in paragraph 2.9 above, We will make the change at a time We consider to be most convenient to You. We will make reasonable endeavours to contact Your technical contact prior to making any security change or equipment upgrades under these circumstances.

2.11 Services not included - Our Attack Mitigation Service neither offers nor provides:

- Hardware redundancy for Our equipment
- Load balancing of traffic or of the Attack Mitigation functionality
- Direct access to Our network security or engineering staff. All initial contact between You and Us must be made with Our Customer Support Centre as outlined in Our “Service Schedule and SLA for Attack Mitigation Services”.
- Permanent archival and storage of log files
- Incident response, forensics and investigations
- Legal case preparation, PR incident support
- Security consulting services (e.g. security policy design, security auditing, penetration testing, contingency/disaster recovery planning, etc)
- Security reporting and analysis
- Permanent filtering or cleaning of traffic

3. SERVICE PROVISION REQUIREMENTS

3.1 In order to provide Our Attack Mitigation Service, the following requirements apply:

- 3.1.1 You will not have access to any Attack Mitigation Service equipment or software;
- 3.1.2 You must specify the IP Addresses and IP Address ranges that You wish the DDoS mitigation to be activated for, by completing a form We will provide to You which will show the protocols, services and applications active on those IP Addresses (e.g. Machine 10.10.10.23, Web server, TCP port 80 (HTTP) and port 443 (HTTPS))
- 3.1.3 You must provide Us with contact details for the departments and/or people We are to contact if We find that You are under attack. If Your Hosting Solution includes appropriate Operating System or Hosted Application management Services, We can be directed to use the same contacts.

4. REPORTING

4.1 The following reporting is provided as part of the Attack Mitigation Service upon request from C&W:

- 4.1.1 Counters and a graph providing high-level overview of each protected Zone, showing current attacks and incoming and outgoing traffic to immediately determine current status
- 4.1.2 Zone-level views provide a log of events for the selected Zone, including attack history, durations and types
- 4.1.3 Historical reports provide a visual record of attacks and associated responses over time for determining attack patterns and allowing verification of successful protection against attacks.

5. EXPORT CONTROL

Cable & Wireless Guernsey Attack Mitigation Service – Specific Terms and Conditions

- 5.1 Delivery of the Service to You may be subject to relevant export control law and regulations. We do not represent that any necessary approvals and licences will be granted. You will provide reasonable assistance to Us to obtain any necessary consent. If, through no fault of Ours, any necessary consent is not granted, then We can terminate this Agreement and the provision of the Service under it (as appropriate) without any liability to You.
- 5.2 You agree to comply with any applicable export or re-export laws and regulations of any country, including obtaining written authority from the US Government if You intend at any time to re-export any items of US origin to any proscribed destination.
- 5.3 For US Government personnel using the Service in the Bailiwick of Guernsey or United Kingdom, US Government restricted rights will apply.

6. LIABILITY

- 6.1 We will not be liable for incidental, indirect, exemplary or consequential damages of any kind, including, but not limited to, damage caused to You due to the operation of the Attack Mitigation Service or damages related to lost data or lost profits, even if We have been advised of the possibility of such damages. Under no circumstances will Our liability exceed the amount You have paid for the Service in any 12 month rolling period, starting on the Service Delivery Date.
- 6.2 This service is designed to protect You and Your end users from DDoS attacks. However, We do not warrant that it shall withstand these attacks on all occasions. We reserve the right to “Black Hole” any of Your traffic as required to protect Our network as a whole.

7. CHARGES

The following categories of charges apply to the Attack Mitigation Service:

Category of charge	Nature of Charge
Installation and configuration Protection (depending on amount of bandwidth protected)	Non Recurring Charge (NRC) Monthly Recurring Charge (MRC)
Relearning of traffic flow following customer equipment configuration change	Non Recurring Charge (NRC)
Make critical change	Non Recurring Charge (NRC)
Make non-critical change	Non Recurring Charge (NRC)

The actual charges are shown on Our relevant Price List, which is available on request from Cable and Wireless Guernsey Limited, PO Box 3, Upland Road St Peter Port, Guernsey GY1 3AB, or by calling Business Sales on 01481 700700.

8. PAYMENT

- 8.1 You shall pay to Us on demand all applicable charges for the relevant Service at rates which are available on request from our office at the above address.
- 8.2 Rental for the Service will start on the Service Delivery Date, unless:

Cable & Wireless Guernsey Attack Mitigation Service – Specific Terms and Conditions

8.2.1 We notify You of a later date for the start of Service when rental will be payable from; or

8.2.2 You use the Service before the Service Delivery Date, in which case rental will be payable from the date You first use the Service.

8.3 Rental is normally payable in advance but We may bill You in arrears. Except for temporary Service, You must pay rental in accordance with Our billing cycle. We will apportion rental on a daily basis for incomplete billing periods

9. GENERAL TERMS AND CONDITIONS

You should refer to the C&W Data Centre General Terms and Conditions and C&W General Terms & Conditions for additional clauses under each of the above headings and in particular for the following:

Special Provision of Service	Use of Service	Connection of Equipment to the Service
Security	Domain Name	Charged Domain Name
The Network	Common Gateway Interface	Intellectual Property Rights
Confidentiality	Acceptable Use Policy	Export Control
Fault Repair	Term of Service	Temporary Service
Interconnection	Payment	Deposits and Payments in Advance
Default	Cancellation	Suspension
Termination	Call Monitoring and Recording	Accommodation, Power and Lightning Protection
Information and Permissions	Access to Premises	Complaints and Arbitration
Assignment	Copyright	Duration and Entire Agreement
Liability	Matters Beyond Reasonable Control	Notice
Use of Information	Severability	Variation
Waiver	Law	

SECTION 2 – Service Schedule and Service Level Agreement

This Cable and Wireless Guernsey Limited Service Level Agreement defines the standard provision target times and level of Fault response for the Attack Mitigation Service in the Bailiwick of Guernsey.

Attack Mitigation Service

Provision of Service	Install within 6 working days of receipt of information required in paragraph 3.1 above.	
Non-Critical Change request	Response: Within 4 working hours	Resolution: Within 8 working hours
Critical Change request	Response: Within 1 hour	Resolution: Within 4 hours

If We respond and work on a Critical Change request and it is subsequently found not to be a Critical

Cable & Wireless Guernsey Attack Mitigation Service – Specific Terms and Conditions

Change We reserve the right to make a charge based on the applicable rate.

We will provide You with the Service on the terms and conditions as stated.

We plan to deliver a working service by the time agreed with You or within the maximum time for provision as stated on the Order Form.

Requests made to us relating to the provision of Service must be made in writing to:

Cable and Wireless Guernsey Limited,
PO Box 3
Upland Road
St Peter Port
Guernsey
GY1 3AB

Notwithstanding and without limiting the generality of clause 30 or 31 of the C&W Guernsey General Terms and Conditions, We will not be liable for any failure to meet the standard provision target times or level of Fault response caused by matters beyond Our reasonable control.

If You require any work for the provision of service to be undertaken outside of Normal Working Hours then a charge will be made based on the applicable hourly rate.

Fault Support for Attack Mitigation Service

Fault Support	Via Customer Support Centre on151, 24 hours per day.
Fault Cover	24 hours per day.
Fault Response	Within 1 hour of receipt of Fault report.
Clear	Resumption of service within 8 hours where replacement hardware is not required as in paragraph 2.8 above.

Where a resolution to Your satisfaction cannot be made at the time of reporting to the Fault then We will ask You to provide Us with a contact telephone number to enable reports on progress with the Fault clearance to be made.

We will:

1. provide advice by telephone
2. carry out tests and diagnostics on the Service
3. if required, visit Your Premises or work to a point in Our network
4. work to resolve the Fault within the agreed time period as stated in the table set out above

If We respond and work on a reported Fault and it is subsequently found not to be a Fault with Our service then a charge will be made based on the applicable rate.

Service Level Target

We will use efforts We consider reasonable to ensure that excluding planned maintenance Your Attack Mitigation Service is available to You 98% of any rolling one year period.