

5 Zone DDoS PROTECTION SERVICE

Provided by: SURE Business, part of Cable & Wireless Communications Guernsey

Cable & Wireless Communications 5 Zone DDoS Protection (“the Service”) provides a solution to protect our customer’s sites against Distributed Denial of Service (DDoS) attacks by analysing incoming traffic, detecting attack conditions and blocking malicious traffic whilst letting genuine traffic through.

The Service is provisioned using 5 Zones.....

These 5 Zone DDoS Protection Service Specific Terms and Conditions should be read in conjunction with the CWCG Data Centre General Terms and Conditions and C&W Guernsey General Terms and Conditions all of which apply. Where there is conflict, these Service Specific Terms and Conditions supersede all other Terms and Conditions.

1. Definitions and Interpretation

The Data Centre General Terms and Conditions include other 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 Professional Services**” means the C&W technical services team, chargeable on an hourly rate.

“**C&W IP Network**” is the C&W IP network (AS8680), from which the customer receives internet access.

“**C&W Operations Team**” means the C&W dedicated operations team tasked with monitoring the Service and Incident Response

“**CWCG**” means Cable & Wireless Communications 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.

“**DDoS Attack**” means a service impact due to DDoS traffic directed at the Customer’s IP Network.

“**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.

“**Incident Response**” means the response by the C&W Operations Team to an alert raised by the monitoring of the Service.

“**Incident Response Procedure**” means the procedure outlined in the Service Level Agreement severity table as set out in paragraph 6.

“**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 Service which contains IP Address and server information for the group of protected equipment and provides protection for that equipment only.

2. The Service

2.1 Provision of the Service

a. The Service consists of the following:

- Implementation of up to 5 dedicated cleaning zones in a resilient network of cleaning appliances.
- A reporting option in which further reports are made available via the C&W portal.

b. The Customer’s Authorisation Form will specify Customer’s chosen Service option to either contact the Customer for further direction or automatically begin the cleaning process.

c. In the event that C&W detects an IP traffic anomaly (as set out in the SLA severity table in paragraph 6), C&W will follow the agreed Incident Response Procedure.

d. Customer may specify up to 15 separate IP address range / IP addresses per cleaning zone.

e. Once cleaning is initiated, all traffic destined to the specified zone of the Customer’s network will be re-directed by C&W to the C&W resilient network of DDoS cleaning appliances.

f. C&W will determine when the cleaning should process should be terminated once the DDoS Attack has been deemed to have been mitigated.

g. The C&W resilient network of DDoS cleaning appliances enables the following types of traffic filtering:

- Packet filtering
- Anti-spoofing
- Statistical analysis
- HTTP analysis and authentication
- Monitoring and Detection

2.2 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.

Cleaning and Mitigation

2.3 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 Service in any calendar month. Further changes requested by You will be charged according to paragraph 7 below.

Maintenance

2.8 - In the event of a hardware failure, We will repair or replace Our equipment within three Business Days based on reasonable endeavour's.

2.9 If We determine that an emergency security change is required, or if You do not respond to Our 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 Endeavour's to contact Your technical contact prior to making any security change or equipment upgrades under these circumstances.

2.10 Configuration

a. C&W will configure the Customer's IP address range / IP addresses to enable protection by the C&W resilient network of DDoS cleaning appliances.

b. Customer will advise C&W of the IP address range / IP addresses to be protected and more detailed information as required by C&W from time to time.

c. A period during which normal or non-DDoS Attack Customer traffic patterns and parameters are established for future use is required in order to better identify anomaly traffic and reduce false positives during a DDoS attack.

d. C&W will work with the Customer during the DDoS Attack to further tune the protection zone in order to better identify anomaly traffic and reduce false positives during a DDoS attack.

2.11 Upgrades

a. C&W may periodically require an upgrade of the network of cleaning appliances to ensure the latest versions of DDoS cleaning hardware and software are in operation. If C&W determines, in its sole discretion, that an upgrade is necessary, C&W will work with Customers to schedule a time to make necessary changes. Customer must allow C&W to make changes within five business days of receipt of the request from C&W.

b. If C&W determines that an emergency security change is required, or if Customer does not respond to a C&W request to perform an upgrade, C&W will make the changes during a normally-scheduled maintenance window. C&W will make commercially reasonable attempts to contact the Customer's technical contact prior to making any security change.

2.12 Services not included

a. The service neither offers nor provides:

- Permanent archival and storage of log files relating to the source of the DDoS Attack.
- Forensics and investigations relating to the source of the DDoS Attack
- Legal case preparation relating to the source of the DDoS Attack.
- Security consulting services (e.g. security policy design, security auditing, penetration testing, contingency / disaster recovery planning, etc)

2.13 Reporting

a. Post-attack analysis reports are available on request one business day after the attack is resolved.

b. C&W will provide Customer with near real-time reports providing traffic analysis specific to the IP address range / IP addresses protected by the Service.

2.14 Service provision requirements

a. In order to take the Service, Customers must:

- Have a connection to the C&W IP Network (AS8680)
- Provide C&W with IP configuration detail and related topology as required
- Specify the IP addresses / IP ranges that they wish the DDoS protection to be activated for, including the protocols, services and applications active on these IP addresses (e.g. Machine 10.10.10.23, Web server, TCP port 80 (HTTP) and port 443 (HTTPS))
- Enable changes to Customer-owned routers and BGP routes as recommended by C&W Operations Team

- Have no root or administrator access to cleaning service
- Providing a technical point of contact and business point of contact with defined authority in the Customers organization 24 hours a day, 7 days a week
- Accept a maintenance window as specified by the maintenance schedule of the C&W Operations Team.
- Failure by Customer to comply with any of the specified above requirements, singly or in any combination, may result in the cancellation of the service.

3. Export Control

3.1 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 licenses 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.

3.2 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.

3.3 For US Government personnel using the Service in the Bailiwick of Guernsey or United Kingdom, US Government restricted rights will apply.

4. Liability

4.1 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 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.

4.2 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.

5. Charges, billing and payment

a. The following categories of charges apply to the Service

- Service componentDescriptionCategory of charge
- InstallationInstallation, port and configurationNon-recurring charge (NRC)
- ManagementMonitoring, management, maintenance and configuration changes (Customer-requested or initiated by C&W and approved by Customer)Monthly recurring charge (MRC)

b. The amounts for each category of charges will be specified in Customer's Authorisation Form

6. Service Level Agreement

C&W DDoS Protection is activated as per the parameters described in the table below.

Cleaning capability Measurement Measurement

Severity 1: Alert Level 'high'

Potential major service impact. Incident Response procedure initiated within 15 minutes, based on agreed incident Response parameters 99.5% of Severity 1 attacks rerouted to cleaning capability C&W DDoS Protection started within agreed response time. Customer contacted for direction or cleaning process started within 15 minutes of receipt of High Alert

Severity 2: Alert Level 'Medium' or 'Low' Customer advised via customer portal 99.5% of Severity 2 attacks made available to the customer on C&W web portal Near real-time traffic profiling report on C&W web portal All online reports are near real-time

Severity 3: Non-urgent changes/a Changes complete within 7 working days.

6.1 SLA severity definitions

a. Severity 1: Threat Level 'High' as identified by the C&W network monitoring component. This includes, but shall not be limited, to the following threats.

Service down or major service impact, caused by:

- Flood attacks, such as: TCP, UDP, ICMP, Spoofed SYN Flood, Non-Spoofed SYN Flood, FIN, SYNACK Flood (Spoofed and Non-Spoofed), Ping Flood, Smurf Flood, Combined UDP/TCP/ICMP.
- Fragmentation attacks, such as: IP/UDP, IP/ICMP, IP/TCP
- HTTP attacks, such as: Connection Flood (Client attack), http errors 404 etc., http half connections
- BGP Attacks
- DNS Attacks

It shall be limited to the maximum capability of the C&W DDoS Protection network.

b. Severity 2: Threat Level 'Medium' or 'Low' as identified by the C&W network monitoring component. This will include non-service impacting traffic anomalies

c. Severity 3: Threat Level 'Non-urgent' as identified by the C&W network monitoring component

6.2 Non-urgent configuration changes

a. C&W will perform a maximum of three non-urgent configuration changes per month. After these are exhausted, changes requested by the customer will be charged at C&W Professional Services security consulting rates

6.3 Incident Response

a. In the event of a DDoS attack, the actions of the C&W Operations Team will be pre-determined as outlined in the Authorisation Form. Customer is responsible for ensuring the correct contact and required actions noted in this Authorisation Form are kept fully up to date by contacting the C&W account representative.

b. Cleaning is not fully automated unless specifically requested by Customer in the Authorisation Form.

If We respond and work on a Critical Change request and it is subsequently found not to be a Critical 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 & Wireless Communications 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 Cable & Wireless Communications 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 the Service

Fault Support Via Contact Centre on 151, 24 hours per day

Fault over 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.

7. Configuration Changes

If We respond and work on a Critical Change request and it is subsequently found not to be a Critical 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 & Wireless Communications 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 Cable & Wireless Communications 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 the Service

Fault Support Via Contact Centre on 151, 24 hours per day

Fault over 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.

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:

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. Data Centre General Terms and Conditions

See CWCG Data Centre General Terms for additional clauses under each of the above headings and in particular for the following:

- Special Provision of ServiceUse of Service
- Connection of Equipment to the ServiceSecurity
- Domain NameCharged Domain name
- The NetworkCommon Gateway Interface
- Intellectual property RightsConfidentiality
- Acceptable Use PolicyExport Control
- Fault RepairTerm of Service
- Temporary ServiceInterconnection
- PaymentDeposits and Payments in Advance
- DefaultCancellation
- SuspensionTermination
- Call Monitoring and RecordingAccommodation, Power and Lightning Protection
- Information and PermissionsAccess to Premises
- Complaints and ArbitrationAssignment
- CopyrightDuration and Entire Agreement
- LiabilityMatters Beyond Reasonable Control
- NoticeUse of Information
- SeverabilityVariation
- WaiverLaw

Issue 2- December 2010