SERVICE DESCRIPTION: SS DDOS

PART A – SERVICE OVERVIEW

Security Services (SS) DDoS is a volumetric service designed to filter certain network traffic in our network to assist you in managing the potential impact of denial of service (DOS), distributed denial of service (DDOS) and other agreed attacks against your Internet service. The SS DDoS Service achieves this by comparing network traffic flows to your Internet service with agreed profiles of normal traffic patterns, behaviour, and standard protocols.

PART B – SS DDOS SERVICE

1. THE SS DDOS SERVICE

1. 1 The SS DDoS Service will consist of the following service components:

- Sensors in the One New Zealand Internet network take samples of traffic and send statistics to centralised collectors for analysis;
- Monitoring and detection devices receive the statistics from the sensors, correlate them and identify whether a traffic pattern matches a specific traffic profile associated with DoS or DDoS;
- Mitigation control will initiate a mitigation action, which can be:
  - Re-directing traffic to our Cleaning Centres, these will be on our Network or part of Cloud Scrubbing.
  - Black holing (dropping) of traffic associated with a specific source or destination IP address, i.e. if the size of the attack is beyond our cleaning centres capabilities.
- Our Cleaning Centre performs packet-by-packet inspection and removes DDoS originated traffic data;
- Traffic Profile – you specify IP ranges and or prefixes to be your specific profile, traffic data is baselined over an agreed tuning period between you and us;
- Traffic Re-Injection - we will re-inject ‘cleaned’ traffic back into a destination Internet point of presence;
- 1 Arbor Cloud mitigation per year is included (covers 1 or more attacks within a continuous 72 hour period). Additional mitigations are available POA (Price on Application).

2. SERVICES PROVIDED

We will perform the SS DDoS Services set out in this Service Description in accordance with the service levels outlined in paragraph 5 of this Service Description and the SS Service Management Services Service Description.

2. 1 Monitoring and Mitigation

The SS DDoS Service provides a Denial of Service monitoring and mitigation service. An example of the detection and mitigation process is as follows:

- Aggressor launches an attack from the Internet at a specific client target (e.g. your web server);
- Sensors in the One New Zealand Internet network sample network traffic and send traffic statistics to the monitoring/detection system;
- The monitoring/detection system correlates the statistics and detects a Denial of Service threat and sends an alarm to our Cyber Defence Centre as well as our One New Zealand NOC (Networks operations Centre);
- Mitigation is triggered automatically based on your business requirements

- The mitigation option will re-direct traffic to our Cleaning Centres. The attack traffic will be filtered out and legitimate traffic will be re-injected to the network;
- If the scope of the attack is such that it is degrading overall service delivery, we reserve the right to discard (black hole) your traffic.

2. 2 Management Functions

We perform standard management functions, as detailed in SS Service Management Service Description.

Management functions specific to the SS DDoS Service include:

- the monitoring of Cleaning Centres, where appropriate; and
- the customer security contact will be notified of critical service impacting events, where appropriate.

2. 3 Reporting

Standard reports as defined by us for the SS DDoS Service and as may be updated from time to time are provided on a monthly basis. Content may include a summary of any DDOS activity identified during the month, traffic profiling and summary per site, any identified traffic patterns that fall outside the normal range and any alerts to the misuse of internet protocols such as TCP SYN attacks.

2. 4 Technical Support

As part of on boarding we will agree the relevant alerting for your specific traffic volume data.

3. SERVICE LIMITATIONS

3. 1 The SS DDoS Service can only be used with a One New Zealand Internet service provided by us.

3. 2 We do not guarantee that the SS DDoS Service will mitigate all attacks against your Internet service and we are not liable for any loss that you may suffer as a result of SS DDoS failing to prevent an attack. In particular, SS DDoS may not provide any protection or assistance to you arising out of an attack on your Internet service if:

- the distributed attack is an application level attack that is not detectable from traffic flows and not threatening the capacity of your Internet service; or
- the distributed attack occurs prior to the completion of the on boarding period and the formal activation of the SS DDoS Service.

3. 3 SS DDoS is designed to limit malicious network traffic to your Internet service. If SS DDoS detects an attack, then you acknowledge and agree that:

- certain network traffic may be blocked from reaching your Internet service or be discarded in our network;
- while a mitigation is running, your Internet service will continue to be available with a possible increase in network latency.

3. 4 In the instance where the Cleaning Centres and/or Arbor Cloud capacity is exceeded, One New Zealand reserves the right to work with our International peering partners and filter traffic upstream from the One New Zealand network. We are not liable for any loss that you may suffer as a result of SS DDoS blocking or limiting network traffic due to an attack.

3. 5 In the event your usage patterns (including bandwidth, number of users, performance or resilience requirements) changes from what you have advised in the configuration template, additional charges may apply.

3. 6 We will have sole administration rights over our Cleaning Centres.

3. 7 Any work undertaken to isolate problems that are initially thought to originate from the provision of the SS DDoS Services that are subsequently found not to be within the scope of this Service Description may incur additional charges on a time and materials basis as set out in the Pricing Schedule.

3. 8 Service level commitments will not apply where delays in fault resolution occur as a result of hardware or software you own and not having appropriate maintenance agreements in place.

3. 9 We reserve the right to change the type and/or brand of hardware and/or software used to provide the SS DDoS Service if we deem such a change is necessary to maintain the integrity of the Service.

4. YOUR RESPONSIBILITIES

4. 1 You must:

- Provide reasonable assistance and information to us to enable us to deliver the SS DDoS service to you;
- Report all incidents relevant and pertaining to the SS DDoS Service known to you to the Enterprise Service Centre;
- Obtain and maintain (at your own cost) appropriate equipment, software, telecommunications services, Internet access and other services or resources needed to use the SS DDoS Service;
- Not use the SS DDoS Service in any way that may adversely affect the efficiency, security, use or operation of your Internet service;
- Not sell, resell or provide the SS DDoS service (or any part of it) to other people without our prior written approval; and
- Comply with all relevant laws, regulations and regulatory requirements relating to your use of the SS DDoS Service.

4. 2 You must notify One New Zealand in the event you intend to perform, or request that a third party performs on your behalf, any penetration testing of the SS DDoS Service. If you fail to notify us you may be liable for any reasonable costs we incur.

4. 3 You must ensure the information detailed in the SS DDoS customer configuration template, which must be completed prior to implementation, is accurate and up to date. You must update us regarding any changes to relevant systems, personnel, processes and policies that are likely to affect the delivery of the SS DDoS Service.

4. 4 You will follow our Move, Add, Change process, as detailed in SS Service Management Service Description.

4. 5 You will notify us of any planned outages to your network.

4. 6 You will promptly notify us if you believe that any changes in your business will change the use of our Services. For example, if you run a promotion that will increase email or web traffic.

4. 7 If you are using IP prefixes not registered to One New Zealand there is a requirement to update registration information in APNIC to confirm authorisation for One New Zealand to register the prefixes with Arbor Cloud and for Arbor Cloud to advertise the routes. Our Security Operations personnel will work with you to make the required changes. These updates will need to remain for the lifetime of the SS DDoS Gold service, and One New Zealand agrees to reverting any changes with APNIC at the termination of the service.

5. SS DDOS SPECIFIC SERVICE LEVELS

In addition to the service levels detailed in the SS Service Management Service Description there are specific service levels relating to our SS DDoS Service which are set out below. For the avoidance of doubt the Service Centre Service Description does not apply to the SS DDoS Service.

5. 1 The service levels set out in the table below are indicative targets only. We will not be liable to you for any failure to meet a service level.

Description of Service Level	**Service Level** (Indicative Target only)
Service Availability[1]	99.99%
Notification to customer of a significant attack against a protected customer site.	We will notify you within 30 minutes of an attack being identified by our Cyber Defence staff

Description of Service Level	Service Level (Indicative Target only)
Local cleaning centre time frame to begin filtering and commence redirecting traffic	Auto-mitigation of agreed and predefined customer critical managed objects (eg.websites) will commence within 1 minute. All other customer managed objects (eg. network ranges) will commence auto-mitigation after 2 minutes, depending on profile of traffic and how sustained it is.
Cloud Scrubbing cleaning centre time frame to begin filtering and commence redirecting traffic once decision to mitigate is agreed with the Customer.	BGP route announcement if customer or One New Zealand has to make routing changes within 5 minutes. Auto-mitigate initiated by cloud signalling within 1 minute. Note that there will be a time period required for BGP routing announcements from the Arbor Cloud cleaning centre to propagate throughout the Internet. This can typically take up to 5 minutes.
Implementation of any standard changes. A standard change is a minor configuration change to existing SS DDoS Services[2]	We will acknowledge your request within one Business Day and will implement the change within five Business Days
Incident Resolution targets	As described in the SS Service Management Service Description
NOTES 1. Service Availability means the period of time the Service is monitoring, detecting, filtering and reporting attacks, in each case, within the specifications and the configuration parameters of the Service. Service Availability is measured monthly on a rolling 12 months basis, and excludes the period of any and all planned outages and maintenance. 2. If configuration changes are more than a standard configuration change, we may charge you for the change at the Additional Work Rates specified in the Pricing Schedule.	

5. 2 The incident resolution targets for the SS DDoS Service are set out in SS Service Management Service Description.

5. 3 Attacks will be attended to in a priority order depending on the degree of impact the attack has on your Internet service (**Incident Severity**), as categorised in the SS Service Management Service Description. We will (acting reasonably) determine the Incident Severity of any attack. We will notify you of the Incident Severity we have assigned to any incident you report to the Enterprise Service Centre.

5. 4 We will commence measuring the response time from the time we become aware of the incident.

PART C – PRICING

6. PRICING OVERVIEW

6. 1 Refer to the Pricing Schedule for details of the applicable Charges.

PART D – DEFINITIONS

7. DEFINITIONS

In this Service Description in addition to the terms defined elsewhere in the Agreement, the following defined terms will apply to this Service Description:

Cleaning Centres means our threat mitigation systems.