DDoS Protection

This Schedule sets out provisions with respect to the Customer's subscription to the Products and/or Services described herein as provided by Rogers Communications Canada Inc. ("**Rogers**"), details of which are stipulated in the Product Quotation. This Schedule is an attachment to and forms an integral part of the Customer's Rogers for Business Agreement (the "**Agreement**") with Rogers. The Customer agrees to be bound by the terms and conditions set out in the Agreement, which include without limitation this attachment and any other attachments to the Agreement. Capitalized terms used but not defined herein shall have the meanings ascribed to them in the Agreement.

Part I. Product Description

This Product Description pertains specifically to DDoS Protection Services supplied by Rogers to the Customer. The primary goal of a Distributed Denial of Service (DDoS) attack is to render the website/ IP address(es) of the victim inaccessible to the rest of the Internet. This can be done in two basic ways:

- Via a volumetric attack, which simply focuses on 'flooding' the bandwidth of a customer at the infrastructure layer, and
- Via a more sophisticated and targeted attack that focuses on the weaknesses of individual applications.

By far, the vast majority of DDoS attacks are volumetric in nature and Rogers DDoS Protection Services are focused on blocking volumetric attacks. Rogers delivers DDoS Protection Services for businesses which use Rogers Internet Services product suite. The Customer can leverage the scalability and cost effectiveness of Rogers DDoS Protection platforms and protect their business from DDoS attacks.

Rogers will position traffic sensors and data scrubbers outside the Customer's network perimeter Rogers DDoS Protection systems learn normal traffic and routing behavior across networks and devices. These systems are also updated to recognize well-known attack profiles and compare the Customer's traffic patterns with such data. These Rogers' traffic sensors will passively watch the Customer's data; when detecting a potential attack, they will begin to intercept all the data intended for a particular Customer network and pursue one of two courses of actions: either they will catch and drop the data intended towards the location via access-lists or Black Hole routing, effectively taking the victim IPs off the Internet (Rogers **DDoS Protection**), or they will sanitize, or 'scrub' the data, to ensure only legitimate data is passed through (Rogers **Enhanced DDoS Protection**). Scrubbing is the process where malicious traffic is identified and blocked, while legitimate traffic is allowed to pass to the Customer's location.

DDoS Protection Services will only be available where the Customer purchases Rogers Internet Services, excluding Rogers Volume Internet Services, Rogers Internet Services provided over Cable access and Rogers Internet Services to non-Canadian Sites. DDoS Protection Services are compatible with all access speeds of Rogers Internet Services, including burstable options. Burstable protection will be provided by Rogers **Enhanced Burtsable DDoS Protection**

Part II. DDoS Protection Service Types

The three types of DDoS Protection Services are listed below and described in Diagram 1 below, along with the features available in each service type:

1. **DDoS Protection:** With the DDoS Protection package, Rogers will provide the Customer with a shared managed object in the DDoS Protection systems that dictates the DDoS Protection policies that will be applied to the Customer. The policies will be aligned with the nature and bandwidth speed of the Rogers Internet Service the Customer has purchased. The shared managed object selected by Rogers to dictate the Customer's DDoS Protection policies may include some or all of the following elements:
    - Detection of the volumetric attacks
    - Malicious traffic drop in the network

- Security parameters and policies
- Basic monthly reporting which shows the number of attacks

2. **Enhanced DDoS Protection:** With Enhanced DDoS Protection Services, Rogers will provide the Customer with a dedicated (customer specific) managed object in the DDoS Protection systems that dictates the DDoS Protection policies that will be applied to the Customer, which the Customer may elect to customize. The policies will be verified by Rogers to ensure that they are consistent with the overall security architecture and design of the Customer's network. The dedicated managed object selected by Rogers and customized by the Customer to dictate the Customer's DDoS Protection policies may include some or all of the following elements:
    - Detection of the volumetric attacks
    - Selective traffic drop
    - Mitigation with scrubbing (see limitation below)
    - Unique customer attack detection policy per customer
    - Unique mitigation parameters and policies per customer
    - Advanced monthly reporting which shows the number of attacks, source and destinations, durations, bandwidth impact.

3. **Enhanced DDoS Protection for Burstable Internet:** With Enhanced Burstable DDoS Protection Services, Rogers will provide same services as Enhanced DDoS Protection Services. The Customer will be offered Enhanced Burstable DDoS Protection Services when they purchase Rogers Burstable Internet Services.

Diagram 1 – Features by DDoS Protection Service Type

Feature	DDoS Protection	Enhanced DDoS Protection	Enhanced DDos Protection for Burstable Internet
Mitigation with Black Holes (2 simultaneous mitigation sessions)	X	X	X
Mitigation with Scrubbing or custom ACLs (2 simultanious mitigation sessions) (see limitation below)		X	X
Shared policies	X		
Dedicated and custom policies per Customer		X	X
Ability for Rogers NOC to mitigate	X	X	X

The features listed in Diagram 1 above are more fully described below:

a. **Mitigation with black-holes –** This feature supports black-holing of a targeted IP as mitigation technique. The exact method would be chosen by Rogers in order to optimize overall network efficiency and response times. Black-hole mitigation is the process in which traffic destined to a particular network is routed to a Black Hole and dropped silently instead of its intended destination. During Black Hole mitigation, any traffic targeted to the victim (Black Holed destination) will be dropped, and the destination will be isolated from the Internet.

b. **Mitigation with Scrubbing or custom ACLs–** Scrubbing is the process in which malicious traffic is identified and dropped, while legitimate traffic is allowed to reach its destination. During scrubbing, the traffic for the Customer's host(s)/ networks is directed to threat management systems which look at each packet and which make a decision whether to pass (forward) or drop the packet based on its characteristics.
Based on parameters such as source/destination IP address, protocols and ports, there can be custom ACLs deployed when the attacks are not suitable for other types of mitigation methods. This would ensure that cleaning centers are always available and optimized for sophisticated attacks. For DDoS attacks reaching or exceeding a bandwidth of 5Gbps, Rogers will employ the black-hole mitigation described above, which will impact all of Customer's destination traffic.

c. **Shared Managed objects (Profiles) –** For Shared Managed object, the detection and mitigation policies are defined based on pre-set profiles and criteria. When shared managed objects are used, there are no Customer-specific policy updates.

d. **Unique custom policies per Customer –** When the Customer purchases Enhanced DDoS Protection Services, the Customer may have custom requests on the detection and mitigation policies. The changes may be applied after the review and approval of the Rogers' security operations team.

e. **Dedicated Managed objects –** When Enhanced DDoS Protection is purchased, the Customer will receive dedicated managed object for detection and mitigation policies. Each such dedicated managed object would have the Customer's specific and configurable detection and mitigation policies. The Customer will communicate its desired managed object via the form attached to this Schedule as Annex "A". This completed form must be received by Rogers prior to the activation of the Enhanced DDoS Protection Services, or Rogers will select the Rogers-recommended default settings upon activation. The Customer will then have sixty (60) days to communicate its desired dedicated managed objects via the completed form. After such date, any Customer-directed customization of the managed objects may be subject to a one-time charge.

f. **Ability for Rogers NOC to mitigate –** When the Customer is under attack, Rogers security operation personal can contact the Customer for mitigation recommendations. Only where the Customer has purchased Enhanced DDoS Service can these detection/mitigation policies be changed.

Part III. DDoS Protection Terms and Conditions

1. **Termination Fees.** If the Customer terminates the DDoS Protection Services for any reason other than as permitted under the Agreement, or if Rogers terminates the DDoS Protection Services for cause as permitted under the Agreement, the Customer shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:
   (a) fifty percent (50%) of the average monthly charges for the terminated Service(s) (as determined over the previous three months) multiplied by the number of months remaining in the Service Term from the effective date of termination;
   (b) any cost which Rogers must continue to pay to third parties for the remainder of the applicable Service Term as a result of the early termination of the applicable Services that exceeds the amount set out in (a) above, and
   (c) a lump sum representing the amortized remainder of any waived or discounted installation or one-time charges associated with the terminated Service(s) in consideration of the Customer's commitment to the Service Term for such Services.

   Where the Customer terminates the Services prior to the expiration of the applicable Service Term, the Customer must either return all Rogers Equipment associated with the Services to Rogers, or pay Rogers for the fair market value of such Rogers Equipment.
   Such termination liability shall be payable on the effective date of any and all terminations.

2. **Minimum Contract Period.** DDoS Protection Services must be purchased in conjunction with Rogers Internet Services or added to the Customer's existing Rogers Internet Services. The Service Term for DDoS Protection Service can be less than the Service Term for Rogers Internet Services, but cannot be longer than the Service Term for Rogers Internet Services. Upon expiry of the initial Service Term for DDoS Protection Services, the DDoS Protection Services will renew on a monthly basis until the earlier of their termination by the Customer in accordance with the terms of the Agreement or the cancellation or termination of the Customer's Rogers Internet Services. For greater certainty, cancellation or termination of the Customer's Rogers Internet Services for a particular Customer Site will constitute automatic termination of the Customer's DDoS Protection Services at that Site and/or for the IP addresses associated with that Site in the Customer's DDoS Protection profile.

3. **Invoicing.** Monthly recurring charges for DDoS Protection Services are invoiced monthly, in advance on the first of each month, with overage charges invoiced monthly in arrears. Charges for DDoS Protection Services will commence as of the Service Effective Date. In the first month the charges will be prorated for the number of days in the month after the Service Effective Date. Rogers will, by way of invoice or otherwise, notify the Customer of the Effective Date. Service level credits will be applied to Customer's invoice within two billing cycles after Rogers' approval of a Customer's request.

4. **DDoS Protection in combination with Burstable Internet Services.** Rogers Burstable Internet Services can only be combined with the Enhanced DDoS Protection Services. The rates for Enhanced DDoS Protection

Services for Rogers Burstable Internet Services will have two components and the monthly recurring fee for the Enhanced DDoS Protection Services will be the sum of these two components:

- **The flat fee** is based on the minimum committed bandwidth rate for the Customer's Rogers Business Internet
- **Burstable bandwidth fee** is based on the bandwidth overage amount that the Customer utilized in excess of the minimum committed bandwidth in a particular month. The bandwidth overage amount would be multiplied by the corresponding per Mbps DDoS Protection Services rate as set out in the Product Quotation.

5. **Enhanced DDoS Protection.** The Enhanced DDoS Protection Service requires an initial base-lining process. During this stage, the Customer's network and traffic behaviors are monitored and analyzed by Rogers' systems for 4 to 8 weeks, depending on the traffic profile and patterns. During this period, Rogers' technical teams may work with the Customer to understand the Customer's precise needs and traffic behaviours in order to optimize the attack detection and mitigation policies. Any attacks against the Customer during the base-lining period would be detected based on general policies and best practices, and mitigation would be executed by Rogers' security experts. Customer understands that notwithstanding the base-lining of its traffic, for DDoS attacks reaching or exceeding a bandwidth of 5Gbps, Rogers will employ black-hole mitigation on all of Customer's traffic.

6. **Mitigation Duration.** Unless Rogers and the Customer mutually agree otherwise, the mitigation period for a DDoS attack would cease when the attack alert is no longer present in the DDoS detection systems. If subsequent mitigations occur within 24 hours of the initial mitigation period (the "mitigation window"), the initial mitigation session can re-start using the same mitigation window. The DDoS Protection Services and Enhanced DDoS Protection Services include a maximum of twenty-four (24) mitigation windows per year.

7. **Additional Work.** Work requested by Customer and performed by Rogers or its Contractors that is outside the scope of this Product Description, including any Customer-requested emergency changes and provisioning activities, will be billed to Customer at Rogers' then current time and material rates. Work requested and performed outside of Rogers' normal business hours (see below) will be subject to an additional charge, to be quoted upon request.

8. **Disclaimer.**

a) The DDoS Protection Services are provided on an "as is" basis. In addition to any disclaimer contained in the Agreement, Rogers expressly disclaims any and all liability in connection with any DDoS attack, cybersecurity incident, computer virus infection, computer or data breach, including, without limitation, those resulting in loss or corruption of data, which occur notwithstanding the provision of the DDoS Protection Services. Customer acknowledges that Rogers does not warrant that the services will operate in an uninterrupted and error-free manner. During a Subscription Period, Rogers may migrate the DDoS Protection Service to an alternative service or technology as long as the alternative service or technology provides materially similar functionality as the DDoS Protection Service. The definition of "Service" includes such alternative service.

b) Customer understands and agrees that DDoS Protection Services may require the use of various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. Customer authorizes Rogers and Subcontractor to perform such services and functions, and all such tasks and tests reasonably necessary to provide the DDoS Protection Services, on network resources with the internet IP addresses identified by Customer. Customer represents that it has all right and authorization required to permit Rogers and the Subcontractor to provide the DDoS Protection Services on such network resources.

c) Customer acknowledges that the provision of the DDoS Protection Services may result in service interruptions or degradation of the Customer's systems or services and Customer accepts such risks and consequences. Customer consents and authorizes Rogers and Subcontractor to provide the services specified herein in connection with the Customer's systems.

Part IV. Monitoring and Notifications

Monitoring of and notification for this DDoS Protection Services will be performed as described below:

Upon being hit by a DDoS attack, the DDoS Protection system will generate a written alert to the Customer informing that the Customer is under a known DDoS attack, and that mitigation is already under way.

A second alert will be issued to the Customer to notify the Customer that the DDoS attack has subsided, and that their Rogers Internet Services should be returning to normal operating conditions. Outages to the Customer's Rogers Internet Services caused by a DDoS attack, and any impact to the Rogers Internet Services' performance caused by the intervention of DDoS Protection Services, each constitute "Acceptable Downtime", as that term is defined in the Customer's Rogers Internet Services SLA.

Part V. Change Management

Rogers will proactively manage the implementation of the Customer's DDoS Protection system configuration changes, and the application of software upgrades and patches on the DDoS Protection systems.

Change Management includes complete management of configuration changes, as requested by the Customer (up to a maximum of three (3) requests per month) or required by Rogers. With Change Management, Rogers will provide a four (4) Business Hour SLO to respond to Customer requests to change their dedicated managed object policies where the Customer has purchased Enhanced DDoS Protection Services.

Part VI. Service Level Objectives ("SLO")

Service Level Objective (SLO):

The SLOs set out in Table 1 below are applicable to the uptime and availability of the Enhanced DDoS Protection Services and Enhanced DDoS Protection for Burstable Internet Services. Planned outages of the DDoS Protection Services, provided the Customer has been notified at least twenty-four (24) hours in advance of the planned outage, will not count towards the SLO calculation.

Table 1 – Enhanced DDoS Protection Services Availability SLOs

Description	Service Level Objective
Service Availability	99.97%
Mean Time to Repair (MTTR)	24 Hours

The SLOs set out in Table 2 relate to the time to acknowledge and complete Change Management requests made by authorized Customer contacts contacting Rogers Customer Care. These SLOs apply where the Customer has purchased Enhanced DDoS Protection Services or Enhanced DDoS Protection for Burstable Internet Services

Table 2 – Enhanced DDoS Protection Services Change Management SLOs

Description	Service Level Objective
Change Request – Acknowledgement	30 minutes within Business Hours
Change Request – Completion	4 Hours within Business Hours

Part VII. Definitions

The following definitions are used in this Product Schedule. Any capitalized terms not defined below are defined in the Agreement.

1. **Black Hole –** refers to places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient.

2. **Business Hours –** From 9:00am to 5:00pm, local time, on Business Days**.**

3. **Business Days** – Monday to Friday, excluding statutory holidays observed locally.

4. **Canadian Site –** a Customer Site within the borders of Canada.

5. **Mean Time to Repair (MTTR) –** means the average length of time it took to repair a DDoS Protection system during a specific month. MTTR metrics are measured solely against outages on Rogers DDoS Protection systems, and exclude access and Internet service related elements. MTTR metrics are based solely on outage statistics collected by the Rogers Reporting System.

   MTTR is calculated as follows:

   Total amount of validated System Outage Time (in minutes) during a specific calendar month as measured by Rogers (not including maintenance and planned outages), divided by the total number of outage incidents on the Customer's DDoS Protection system during a specific calendar month, and divided by sixty (60) (for hours).

6. **Service Availability –** means the percentage of time during a specific calendar month, that the Rogers DDoS Protection systems were available to pass traffic. DDoS Protection Service Availability is based on ticket information from the Rogers Reporting System:

   Rogers continuously monitors each DDoS Protection Node for availability. If an Out of Service condition is detected on a specific DDoS Protection system Node, that specific DDoS Protection system will be deemed to be unavailable for the length of the outage. Availability is calculated as the total number of minutes that the DDoS Protection system for a Customer's Site(s) was unavailable during a specific month, divided by the total number of minutes in the specific month, multiplied by hundred (100) (for the percentage).

7. **Site** - means a geographic location where one or more of the Customer's Services is delivered.

Annex "A"

Rogers Enhanced DDoS Protection Services - Customer Managed Object Form

Instructions:

- Please complete this form or all Enhanced DDoS Protection orders.
- Page 1 must be completed and in full and this form must be signed or this order cannot be completed.
- The Solutions Architects to return the completed form to R4B CSO Operations CIS.

1	Customer Name:	
2	Service ID:	
3	Please list the IP Address(es) that should be protected by Rogers DDoS Protection Services:	
4	Does your network use NAT for a server or host? If yes, please include the list of IP address(es) that is being used by NAT.	
5	List each web facing service(s) your network uses and the associated IP address for each service.	
6	Are there any IP addresses outside your network (in the public Internet) you define as trusted source networks? If yes, what are the network addresses?	
7	Please include the names and contact information of your technical primes that Rogers can contact if required.	

Host detection values: The following contains the list of recommended values from Rogers however should you want to customize these values please fill out indicate these values in the below table. If you chose not to specify a customized value Rogers will configure the service using the recommended threshold.

Type	Recommended Trigger Rate	Recommended High Severity Rate	Customer Preferred Trigger Rate	Customer Preferred High Severity Rate
Total Traffic (bytes)	95% of the bandwidth	130% of the bandwidth		
Total Traffic (packets)	50 Kpps	1 Mpps		
Chargen Amplification (bytes)	20 Mbps	25 Mpbs		
Chargen Amplification (packets)	20 Kpps	25 Kpps		
CLDAP Amplification (bytes)	20 Mbps	25 Mbps		
CLDAP Amplification (packets)	20 Kpps	25 Kpps		
DNS	5 Kpps	10 Kpps		
DNS Amplification (bytes)	20 Kpps	25 Mbps		
DNS Amplification (packets)	20 Kpps	25 Kpps		
ICMP	1 Kpps	2 Kpps		
IP Fragment	5 Kpps	10 Kpps		
IP v4 Protocol 0	5 Kpps	10 Kpps		
IP Private	5 Kpps	10 Kpps		
L2TP (bytes)	20 Mbps	25 Mbps		
L2TP (packets)	20 Kpps	25 Kpps		
mDNS (bytes)	20 Mbps	25 Mbps		
mDNS (packets)	20 Kpps	25 Kpps		
memcached Amplification (bytes)	20 Mbps	25 Mbps		
Memcached Amplification (packets	20 Kpps	25 Kpps		
MS SQL RS Amplification (bytes)	20 Mbps	25 Mbps		
MS SQL RS Amplification (packets)	20 Kpps	25 Mbps		
NetBIOS (bytes)	20 Mbps	25 Mbps		
NetBiOS (packets)	20 Kpps	25 Kpps		
NTP Amplification (bytes)	20 Mbps	25 Mbps		
NTP Amplification (packets)	20 Kpps	25 Kpps		
rpcbind (bytes)	25 Mbps	25 Mbps		
rpcbind (packets)	20 Kpps	25 Kpps		
RIPv1 (bytes)	20 Mbps	25 Mbps		
RIPv1 (packets)	20 Kpps	25 Kpps		
SNMP Amplification (bytes)	20 Mbps	25 Mbps		
SNMP Amplification (packets)	20 Kpps	25 Kpps		
SSDP Amplification (bytes)	20 Mbps	25 Mbps		
SSDP Amplification (packets)	20 Kpps	25 Kpps		
TCP Null	5 Kpps	10 Kpps		
TCP RST	5 Kpps	10 Kpps		
TCP SYN	5 Kpps	10 Kpps		
TCP SYN/ACK Amplification (bytes)	20 Mbps	25 Mbps		
TCP SYN/ACK Amplification (packets)	20 Kpps	25 Kpps		
UDP	50 Kpps	75 Kpps		

Authorized Customer Name and Title: _____ Date: _____

Important: If you cannot print and sign this form, please send an e-mail confirming that you approve these thresholds.

[1] – The trigger rate (measured in kilo-packets per second) is the threshold that must be passed before Rogers' internal support teams will be alerted of a potential issue. No action will be taken against incoming traffic at this time.

[2] – If this threshold is breached for a period longer than the severity duration, **Rogers will begin to clean the traffic**. Setting a low severity duration can lead to additional false positives.

Appendix A – Definition of Terms

Host detection misuse types		
Misuse Type	**Type of Traffic**	**Can Help Detect**
Total Traffic*	The total traffic (in bps) for a given host. *This should be verified by the customer based on their traffic pattern. Default assumes no single host sends or receives more than 50% of the total Internet bandwidth	Host attacks that do not follow a known attack pattern *This should be verified by the customer based on their traffic pattern. Default assumes no single host sends or receives more than 75% of the total Internet bandwidth
Chargen Amplification	chargen traffic (in bps or pps) with the UDP and/or TCP protocol and source port 19	chargen (Character Generator Protocol) reflection/amplification attacks
DNS	DNS traffic (in pps) with the TCP and/or UDP protocol and destination port 53 traffic	Floods of DNS traffic
DNS Amplification	DNS traffic (in bps or pps) with the UDP protocol and source port 53	DNS reflection/amplification attacks
ICMP	IPv4 and IPv6 Internet Control Message Protocol traffic (in pps)	IPv4 ICMP and ICMPv6 packet-flooding attacks
IP Fragment	Traffic (in pps) with the IP fragment flag	TCP and UDP fragmentation attacks Note: TCP and UDP fragmentation attacks are often associated with chargen, DNS, SNMP, SSDP, and MS SQL RS amplification attacks.