Rackspace Private Cloud Security

NETWORK DDOS PROTECTION PRODUCT TERMS

In addition to any other terms and conditions of Customer's Agreement with Rackspace, these Product Terms shall apply when Customer purchases Rackspace Network DDoS Protection Service (the "**DDoS Protection**" or the "**Services**").

1. SERVICES OVERVIEW. Network DDoS Protection is a subscription-based service that provides Customer-specified, profile-based monitoring of Customer's network activity to detect malicious traffic flooding or distributed-denial-of-service attacks ("**DDoS Attacks**"), and the activation of countermeasures to minimize the impact of a DDoS attack upon Customer's legitimate network traffic. The DDoS Protection platform is deployed within a shared, multi-tenant hardware infrastructure, and performs both Customer-specified, profile-based monitoring and mitigation, and monitoring and mitigation according to Rackspace network security standards. The Services are available in a standard edition ("**Network DDoS Protection**") and an advanced edition with additional services as described herein ("**Network DDoS Protection - Advanced**").

2. RACKSPACE NETWORK DDOS PROTECTION SERVICE.

2.1. Rackspace Configuration Requirements & Compatibility. Before completing the provisioning of DDoS Protection, Rackspace shall perform a final check of the Customer Configuration to determine compatibility with the Services and compliance with the Rackspace Configuration Requirements. Certain traffic types and hardware configurations are not compatible with DDoS Protection. Customer understands and agrees that if the Customer Configuration does not meet the Rackspace Configuration Requirements, Rackspace may cancel Customer's order and refund any unused fees previously remitted to Rackspace for the Services.

2.2. Change to Customer Configuration. If, after implementation of the Services Customer makes changes to its Customer Configuration that are not supported by DDoS Protection (or which otherwise impact the functionality of the Services), then Rackspace shall advise Customer of Services' limitations resulting from such changes. Following such advice from Rackspace Customer may elect to continue the Services subject to such limitations, or Customer will have the option, for limited a period of 90 days, to elect discontinuation of the Services upon 90-days' notice.

2.3. Customer Services Profile. Each Services subscription includes a Customer-specific profile that defines the list of protected IP addresses, protocols, mitigation countermeasures, and other configuration specifications associated with the supported Customer Configuration (a "**Services Profile**"). To complete the provisioning of DDoS Protection and the Services Profile, Customer shall designate the IP addresses within scope of monitoring and any additional configuration requirements as reasonably requested by Rackspace. Network DDoS Protection is limited to one Services Profile in one data center region and a maximum of eight (8) public IP addresses. Network DDoS Protection Advanced customers can define up to two Service Profiles in up to two data center regions and a maximum of 100 IP entries per Service Profile (i.e., IP addresses or IP ranges in CIDR notation) for each Customer subscription.

2.4. Mitigation & Auto Mitigation. In the context of a detected DDoS attack, "**Mitigation**" means that traffic to the protected IP addresses shall be redirected through Rackspace's mitigation systems with countermeasures applied for the purposes of limiting the impact on legitimate traffic; and when the attack subsides, the as-needed mitigation terminates while the always-on monitoring remains active. If Customer has opted in to auto-Mitigation, then the system shall auto-Mitigate based on the rules in the Services Profile when an attack is detected. If Customer has opted out of auto-Mitigation and Customer detects an attack, then the Mitigation functionality will not be activated unless requested by Customer.

© 2019 Rackspace US, Inc. – Global Product Terms – 20 July 2024 Revision – OT# 46383

2.5. Changes to IP Address(es). Customer shall notify Rackspace if Customer wishes to modify the IP addresses that are being protected by the Services.

2.6. Insufficient Mitigation & Traffic Blocking. Customer understands and agrees that due to the complexity and sophistication of DDoS Attacks, not all DDoS Attacks will be effectively detected and/or mitigated within all Customer Configurations and that not all Services Profiles as initially configured will be adequate to address all DDoS Attacks. If Customer believes that DDoS Protection is not satisfactorily detecting and/or mitigating against DDoS Attacks, then, upon Customer request, Rackspace will engage with Customer on a reasonable efforts basis to provide support, troubleshooting and/or Services improvements. Customer understands and agrees that absolute protection against a DDoS attack may not be possible without interference with Customer's legitimate network traffic, and that Rackspace will seek to achieve an acceptable level of malicious traffic blocking without unreasonable interference with Customer's normal, intended network traffic. If, in Rackspace's sole judgment and discretion, the reconfiguration of Customer's Services Profile to an acceptable level is excessively complex or time consuming, then Rackspace may charge Customer its then-active professional rates for these services.

2.7. Mitigation Capacity. Rackspace does not set limits on mitigation capacity on a per-customer basis. The limits to Rackspace's mitigation capacity depend on the type and nature of attacks and varying limitations across overall network capacity, data center architecture and the particulars of the Customer Configuration.

2.8. Traffic Blocking. If an attack impedes Rackspace's ability to operate the Rackspace network or negatively impacts other Rackspace customers, Rackspace may null route Customer's traffic, engage in upstream blocking, suspend access to the Customer Configuration, or take other measures as necessary to protect Rackspace's network and other customers (collectively "**Traffic Blocking**") without prior notice. If Rackspace has determined that Traffic Blocking is imminently necessary or if Rackspace has already initiated Traffic Blocking, then Rackspace shall notify Customer promptly and engage with Customer to consider measures, to the extent available and practicable, to re-establish attack mitigation and connectivity to the Customer Configuration.

2.9. NETWORK DDoS MITIGATION SERVICE ADVANCED. In addition to the services described in the previous sections, DDoS Mitigation Service Advanced, includes the following premium managed services, performances, and features, as indicated and priced within Customer's Service Order:

(1) Live troubleshooting during an attack.

(2) Multiple traffic profiles.

(3) Region coverage for up to 2 DC Regions per Subscription.

(4) Ad Hoc Reporting at Customer's request.

3. SERVICES LIMITATIONS.

3.1. Latency & Optimization. Customer understands and agrees that during a DDoS attack, and following a DDoS attack, the network may experience increased latency across all affected IP addresses. Rackspace may be able to provide professional services, at additional cost, to assist Customer with minimizing such latency, but cannot guarantee that the Services shall alleviate latency during a DDoS attack. Customer's use of these Services does not change or enhance Customer's SLA terms for network performance as provided for with other Rackspace Services.

3.2. Disclaimers. Customer understands and agrees that due to the complexity and sophistication of DDoS attacks, not all DDoS attacks will be effectively detected and/or mitigated within all Customer Configurations, and Rackspace does not assume, and expressly disclaims all liability for any losses, harms or damages to Customer or third parties due to unavailability of Customer's servers or the performance of the Services. Customer acknowledges that the use DDoS Protection may also result in some legitimate traffic being filtered from Customer's website(s). Rackspace may discontinue Customer's use of DDoS Protection at any time by giving reasonable advance notice if Rackspace determines, in Rackspace's sole discretion, that the website(s)

and/or domains for which Customer has requested the Service pose an undue risk to Rackspace's network or other customers.

4. DDOS PROTECTION SERVICE SLAs.

4.1. Provisioning SLA. Rackspace shall deploy and activate DDoS Protection within one Business Day of receiving all necessary information Rackspace requests from Customer ("**Provisioning SLA**"). If Rackspace fails to meet this Provisioning SLA, Customer is eligible for a credit of 100% of Customer's set-up fee for DDoS Protection. If Customer's set-up fee has been waived, this Provisioning SLA shall not apply.

4.2. Mitigation SLA. Rackspace guarantees that within: (i) five minutes of us receiving an alert confirming detection of an attack; or (ii) 30 minutes of Customer's request via phone, Rackspace shall initiate the mitigation functionality of the Services ("**Mitigation SLA**"). If Rackspace fails to meet the Mitigation SLA, Customer is eligible for a credit of 10% of Customer's then current monthly fee for DDoS Protection for every additional, lapsed five-minute period during which Rackspace fails to activate the Services protection functionality (i.e., beyond the initial five or 30 minutes as applicable). This Mitigation SLA shall not apply to Customer's who opt-out of auto-Mitigation.

4.3. SLA Exclusions. With respect to all indicated SLAs, Customer is not eligible to request a credit for a failure to meet an SLA which results from denial-of-service attacks, viruses, or malware, hacking attempts, or any other circumstances that are not reasonably within Rackspace's control. Customer is not eligible for a credit during the on-boarding phase of the Services. To be eligible for a credit, Customer's use of the Services to which the applicable SLA applies must be adversely affected. Credit remedies identified in specific currency amounts are awarded in the amount matching the currency on the Customer's invoice.

4.4. Credit Request Process. Customer shall request a credit in writing via a support ticket no later than seven days following the relevant event. Rackspace shall contact Customer within 30 days to approve or reject the claim or to request more information. If the claim is approved, the credits will be applied to future invoices and unused credits shall not be refunded. Time-based metrics are determining using the times recorded within the Rackspace ticket system. Time periods commence upon either Rackspace or Customer opening a ticket or, when applicable, the time recorded in a Rackspace monitoring system. If Rackspace opens the ticket on behalf of Customer request made by telephone, there may be delay in opening the ticket.

5. FEES, INVOICING AND PAYMENT.

5.1. Pricing. Pricing for the Services will be in accordance with Rackspace's then-current rates, as indicated in Customer's Service Order. Subject to pricing increase as may be permitted by the Agreement, Customer pricing shall remain in effect throughout the term, until expiration of the applicable Service Order; and upon renewal, pricing may be increased to the then-current services rates.

5.2. Services Fees. An initial one time, set-up Fee may be applicable for initial provisioning of the Services, based on the scale, complexity of the Customer Configuration, and/or number of IP addresses, as indicated in the Service Order ("**Set-up Fee**"). Customer's monthly subscription Fees for DDoS Protection are based on the edition of the Services, and the total number of IP addresses within the Customer Configuration ("**Monthly Fees**"). Customer may scale the Services by ordering additional IP addresses in which case the Monthly Fees will be revised accordingly. Fees for additional consulting or engineering services, per Rackspace's then-current professional services rates, may be applicable as described herein. ("**Professional Services Fees**").

5.3. Invoicing and Payment. The one-time Setup Fee will be invoiced upon execution of the Service Order. The Monthly Fees will be invoiced on a monthly recurring basis in advance; and invoicing will begin upon the commencement of the Services implementation. Professional Services Fees, when applicable, will be invoiced as incurred. All Fees are non-refundable and are payable in accordance with the terms of the Agreement.

6. TERM & TERMINATION.

6.1. Initial Term; Renewal Term. The initial term ("**Initial Term**") of these Services shall be identified in the applicable Service Order. Unless otherwise specified, the term begins upon commencement of the Services implementation. Upon expiration of the Initial Term, the Services shall renew as indicated in the Agreement.