CenturyLink Technology Solutions Service Guide

DDoS Mitigation Service 2.0

This CenturyLink Service Guide ("SG") sets forth a description of DDoS Mitigation Service 2.0 ("Service") offerings by CenturyLink, including technical details and additional requirements, if any. This SG is subject to and incorporated into the Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedules, or Service Orders to SSG, shall mean SG.

<table>
<thead>
<tr>
<th>Version</th>
<th>Previous</th>
<th>Section Modified</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC-20141015-SG-DDoSMitigationService2.0</td>
<td>SEC-20140911-SG-DDoSMitigationService2.0</td>
<td>All</td>
<td>October 15, 2014</td>
</tr>
</tbody>
</table>
Table of Contents

Service Description ................................................................................................................................................................. 3

Tables and Appendices ............................................................................................................................................................. 10

Table 1.0 Roles and Responsibilities .................................................................................................................................... 10
Appendix A Service Level Agreement .................................................................................................................................... 12
Table 2.0 Target Response Times and Credits ....................................................................................................................... 12
Response Times SLA Remedies ............................................................................................................................................... 15
SLA Process .............................................................................................................................................................................. 15
Definitions ............................................................................................................................................................................... 16
Service Description

1. **Service Description:** DDoS Mitigation Service 2.0 is a CenturyLink provided service (the “Service”). The Service provides managed network-based distributed denial of service (“DDoS”) mitigation with 24/7 response to DDoS attacks for Customers who receive Internet services from either CenturyLink or from other Internet service providers (ISP). Because this is a network-based service, DDoS mitigation equipment is not required in the Customer’s environment. The standard features of the Service consists of the installation, configuration, administration, monitoring, maintenance and support for the components listed in section 1.1. The Service Level Agreement (SLA) associated with this service guide is detailed in Appendix A.

1.1. **Service Components:**

1.1.1. **Attack Detection:** Attack detection includes automatic detection of attacks for customers who have internet access from CenturyLink. Customer traffic is monitored continuously. Mitigation (filtering) of Customer traffic begins after the CenturyLink DDoS attack-detection system determines that a DDoS attack (targeting the Customer’s protected site) is underway and Customer has provided approval to divert their traffic to a CenturyLink cleansing center.

1.1.2. **Attack-Traffic Diversion:** For Customers of the Service who also use CenturyLink internet services, CenturyLink will take the additional action to divert attack traffic to a CenturyLink cleansing center for filtering/mitigation.

1.1.3. **Non-CenturyLink Network:** For internet transport on non-CenturyLink networks there are two options for diverting traffic to a CenturyLink cleansing center:

1.1.3.1. **Border Gateway Protocol:** If the Customer is the registered owner (registered with ARIN) of the IP address space to be protected, then it is possible for CenturyLink to utilize Border Gateway Protocol (BGP) for traffic diversion. In this case, after the Customer contacts the CenturyLink Service Center and requests their traffic be diverted to a cleansing center, CenturyLink will advertise to the internet a new route for the affected IP address range using BGP. The Customer must allow CenturyLink to advertise at least a /24 (or larger, as in a /23 or /22) IP block, since a /24 is the smallest address block that can be diverted with BGP. If the Customer does not own the IP address space to be protected, or if a /24 cannot be advertised by CenturyLink via BGP, then diversion must be done through modification of DNS (Note: At the present time, using BGP to redirect is not available to CenturyLink Network Services customers located in the Asia-Pacific region; however, CenturyLink Customers who use third-party networks in this region may qualify to have their traffic redirected using BGP if the aforementioned requirements are met.)

1.1.3.2. **DNS:** If the IP address space that the Customer wishes to protect with the Service is provided by a third-party, then DNS modification must be used to divert the affected traffic to CenturyLink’s network (and to one of its cleansing centers) for filtering/mitigation. In this case, the Customer must modify their DNS settings such that the affected URL(s) resolves to the IP address of CenturyLink’s cleansing center. As a part of this Service, CenturyLink provides a “DNS-Diversion Guidelines” document for the Customer to follow.

1.1.4. **Forwarding of Cleansed Traffic:** Once the Customer’s traffic is cleansed of malicious packets, it must be forwarded from the CenturyLink cleansing center to its original destination. This process is based upon whether the traffic originated on CenturyLink’s network, or a third-party network, and the method in which the traffic is diverted to the CenturyLink cleansing center. Forwarding methods include the following:

1.1.4.1. **CenturyLink Network:** Traffic that originates on CenturyLink’s AS3561 network, and is forwarded to the cleansing center via BGP, is returned to the CenturyLink core router nearest the Customer via MPLS tunneling.

1.1.4.2. **Third-Party (or non-AS3561) Networks (where BGP was used to divert traffic):** Traffic that originates on third-party (non-CenturyLink) networks, and is forwarded to the cleansing center via BGP, is returned to a router that the Customer specifies, via GRE tunneling. For this return
method, the Customer is responsible for managing and owning, and must be in control of the router that the cleansed traffic is returned to, and must enable a GRE tunnel at that router’s end of the connection. As a part of this Service, CenturyLink provides a “GRE Tunneling Guidelines” document for the Customer to follow.

1.1.4.3. Third-Party Networks (where DNS was used to divert traffic): Traffic that originates on third-party (non-CenturyLink) networks, and is forwarded to the cleansing center via DNS, is returned to a router that the Customer’s specifies, via GRE tunneling as described above, or via NAT rerouting. NAT rerouting is used in situations where the customer is unable to create a GRE tunnel termination point on their router. In this case, the cleansed traffic is “relabeled” via the NATting process, and forwarded to the Customer’s destination IP addresses via the internet. As a part of this Service, CenturyLink provides a “GRE Tunneling Guidelines” document for the Customer to follow.

1.2. Installation: CenturyLink will provide installation tasks marked with an “X” in the CenturyLink column in Table 1.0 Roles and Responsibilities

1.2.1. DDoS Mitigation: A DDoS mitigation system, residing on CenturyLink’s network, is configured to filter ingress DDoS traffic targeting a single subnet within a physical Customer location with a maximum of 10 subzones (see “subzone” in Definitions below), and a maximum total of 16384 public IP addresses (additional subnets, subzones, locations, and/or IP addresses requires the purchase of additional instances of the Service). The Service is designed to filter the Customer’s ingress traffic during DDoS attacks up to the available mitigation capacity of the Service. However, due to the changing nature of this type of attack, CenturyLink cannot guarantee that in all instances the Service is capable of providing filtering up to the purchased service level. This Service is an attack mitigation service rather than a preventive service.

1.2.2. Subnets: It is suggested that subzones be broken down by function (Web, DB, etc.) so hosts within each subnet share similar traffic types and patterns. A set of subzones constitutes a “blanket zone”; each blanket zone is tuned separately. The first subzone will contain the entire IP address ranges the Customer wishes to be protected under this Service. Additional subzones may be created during install (not to exceed 10 total subzones per service instance). Subzones exceeding the maximum number of 10 that are customarily provided require the purchase of an additional instance of the Service. Note: Subzones with overlapping IP addresses cannot be put into protect mode at the same time.

1.3. Configuration: CenturyLink will provide configuration tasks marked with an “X” in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.3.1. Configuration Changes: Customer requests for configuration changes are subject to the defined response times for Service levels.

1.4. Administration: CenturyLink will provide administration tasks marked with an “X” in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.4.1. System Administration: CenturyLink will manage all system administration passwords for DDoS mitigation system(s). Customer will not have access to DDoS mitigation system passwords or be able to make direct changes to the DDoS mitigation system configurations. Customer must instead submit change requests to CenturyLink to make configuration changes.

1.4.2. Response Notification: CenturyLink’s target response notification for this Service is defined in Appendix A, Table 2.0 Response Times.

1.5. Monitoring: CenturyLink will provide monitoring tasks marked with an “X” in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.5.1. Time to Notify Goal: The Time to Notify Goal is measured from the time an Incident is detected by a system-generated alarm (“Initial DDoS Alarm”) to when CenturyLink attempts to verbally notify
Customer of the Incident. Customer may request CenturyLink to notify Customer through either a phone call or e-mail. A phone call notification is available for high priority alerts. E-mail notification is available for low, medium and high priority alerts. The Time to Notify Goal applies only to DDoS Mitigation Service with Attack Detection.

1.5.2. **Time to Mitigate:** If Customer has provided all the necessary information to initiate Mitigation, the Time to Mitigate Goal is measured from Customer Approval to the actual initiation of Mitigation. “Customer Approval” means: (i) the time CenturyLink receives verbal permission from Customer to initiate Mitigation or (ii) the Initial DDoS Alarm for Proactive DDoS Mitigation Service if Customer has pre-authorized CenturyLink to initiate Mitigation. If Customer has pre-authorized CenturyLink to initiate Mitigation, but additional countermeasures that were not pre-authorized are required to mitigate the Incident, the verbal permission Time to Mitigate Goal will apply to the additional countermeasures that were not previously pre-authorized. Initiation of Customer pre-authorized Mitigation may be done by an authorized CenturyLink employee or as an automated initiation by the system (“Auto-Mitigation”). Customer chooses which mode to use.

1.5.3. **Active Migrations:** CenturyLink will notify Customer once per day about Customer's active DDoS mitigations. If Customer requests that a mitigation stay in place for a period longer than one day, CenturyLink may notify Customer about each active mitigation at the end of that extended period rather than once per day.

1.6. **Maintenance and Support:** CenturyLink will provide maintenance and support tasks marked with an “X” in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.6.1. **Protect Mode:** CenturyLink may periodically request that the Customer’s traffic be placed into protect mode to retune and improve the effectiveness of the Service. This normal maintenance procedure is not expected to have any impact on the Service. If CenturyLink determines a retuning is necessary, CenturyLink may contact Customer, to schedule a time to make necessary arrangements. Customer must work with CenturyLink to schedule these changes within five business days of receipt of the request from CenturyLink. If CenturyLink determines that an emergency security change is required, CenturyLink will make the changes deemed necessary as quickly as possible and will use commercially reasonable efforts to contact the Customer’s technical contact prior to making said change.

1.6.2. **Service Upgrades:** CenturyLink may periodically upgrade software or hardware to maintain the latest versions in operation. If CenturyLink determines an upgrade is necessary, CenturyLink will work with Customer to schedule a time to make necessary changes, preferably during the normally scheduled CenturyLink maintenance window. Customer must allow CenturyLink to make these changes within five (5) business days of receipt of the request from CenturyLink, or CenturyLink’s obligation to provide this Service in accordance with this CenturyLink Service Guide will be suspended until Customer grants CenturyLink the access CenturyLink requires to make such changes. If CenturyLink determines that an emergency security change is required, CenturyLink will make the change as quickly as possible. CenturyLink will make commercially reasonable attempts to contact the Customer's technical contact prior to making said change.

2. **Customer Responsibilities:** Customer is responsible for all tasks marked with an "X" in the Customer column in Table 1.0 Roles and Responsibilities. Customer acknowledges and agrees that its failure to perform its obligations set forth in Table 1.0 may result in CenturyLink’s inability to perform the Services and CenturyLink shall not be liable for any failure to perform in the event of Customer’s failure.

2.1. **Third Party Software:** If any third-party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

2.2. **Testing:** Customer shall not attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service or any devices used to deliver CenturyLink services. Without limiting the
foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test firewall attacks, penetration testing or external network scans on CenturyLink’s network without the prior written consent of CenturyLink. Testing: Customer shall not attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service or any devices used to deliver CenturyLink services. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test firewall attacks, penetration testing or external network scans on CenturyLink’s network without the prior written consent of CenturyLink.

2.3. **Access to Customer Environments:** CenturyLink may require access to Customer’s staging environment that matches production configuration in order to test configuration stability prior to implementing software changes. A successful test on the staging system does not guarantee success on the production system. The Services do not include the development of a comprehensive change control process. There may be incompatibilities between a Service and particular Customer environments which cannot be resolved. In such cases, CenturyLink reserves the right to withdraw the Service from those particular environments, but only to the extent necessary to resolve the incompatibility and without modifying either party’s obligations with regard to unaffected environments.

2.4. **Reconfiguration:** If a Service requires reconfiguration or retuning for any reason, including reducing false positives and nuisance alerts, CenturyLink will contact Customer, if necessary, to schedule the activity (typically during normal maintenance windows) and Customer agrees to cooperate with CenturyLink to schedule such activity. If CenturyLink determines that an emergency security change is required, CenturyLink will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.

2.5. **Mitigations:** Customer is responsible for requesting that CenturyLink end a DDoS mitigation. If the mitigation was put in place via auto-mitigation, the CenturyLink DDoS mitigation system will automatically end the mitigation when it detects that the attack has ended (unless it has been modified in which case it is no longer considered an auto-mitigation). If Customer wants the auto-mitigation to stay in place for a longer period of time, Customer must contact CenturyLink to request that an auto-mitigation be changed to a manual mitigation that does not end until Customer request to end it.

2.6. **Customer Technical Contact:** Customer must provide and maintain an English-speaking technical contact with current, complete and accurate contact information that is reachable 24/7. This contact is the primary point-of-contact for the Service’s event notifications and should be authorized to consent to make, or direct, changes to the Customer’s security infrastructure or architecture, including managed security services, as applicable.

2.7. **Change Request:** Customer must request changes by contacting the CenturyLink Service Center. Customer must provide complete authentication credentials to the CenturyLink Service Center when requesting changes. The current process definition for password authentication and modification is available at http://www.CenturyLink.com/support/contact.

2.8. **Third Party Networks:** Customer whose traffic originates on third-party (non-CenturyLink) networks, or whose sites are located in the Asia-Pacific region, are responsible for preparing their infrastructure for the Service as described in the respective guidelines documents and in this document.

2.9. **Third Party ISP:** Customer using a third-party ISP for internet transit are responsible for detecting DDoS attacks on their public-facing IP addresses, and must notify the CenturyLink Service Center if they chose to divert their traffic to a CenturyLink DDoS mitigation cleansing center. Customers may purchase CenturyLink’s optional “On-Site DDoS Detection and Mitigation” Service as a viable means for enabling attack detection on third-party networks. See “Optional Security Services” section of this document for more details.

2.10. **GRE Tunneling:** Customer is responsible for managing and owning, and must be in control of the router that the cleansed traffic is returned to, and must enable a GRE tunnel at that router’s end of the connection.

2.11. **Access to Customer Environments:** CenturyLink may require access to Customer’s staging environment that matches production configuration in order to test configuration stability prior to implementing software changes. A successful test on the staging system does not guarantee success on the production system. The Services do not include the development of a comprehensive change control process. There may be
incompatibilities between a Service and particular Customer environments which cannot be resolved. In such cases, CenturyLink reserves the right to withdraw the Service from those particular environments, but only to the extent necessary to resolve the incompatibility and without modifying either party’s obligations with regard to unaffected environments.

2.12. **Reconfiguration**: If a Service requires reconfiguration or retuning for any reason, including reducing false positives and nuisance alerts, CenturyLink will contact Customer, if necessary, to schedule the activity (typically during normal maintenance windows) and Customer agrees to cooperate with CenturyLink to schedule such activity. If CenturyLink determines that an emergency security change is required, CenturyLink will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.

2.13. **Changes to System**: Customer must notify CenturyLink at least five business days in advance of any network topology or system changes that may affect the Service or the effectiveness of the DDoS mitigation system policy. Failure to notify CenturyLink of system changes may result in the inability to monitor traffic or the generation of false alerts, where applicable. CenturyLink will work with the Customer to resolve chronic false positives and other nuisance alerts; however, if alerting issues are not resolved satisfactorily, CenturyLink may modify the DDoS mitigation system configuration to reduce repetitive alarms caused by Customer actions that are not indicative of security incidents. Alerting is available only when the Customer uses the Service in conjunction with CenturyLink internet services.

3. **Additional Services**: At Customer’s option and expense Customer can choose to have CenturyLink complete one or more of the tasks in Table 1.0 with an “X” in the Customer column and/or the services listed below. The items can be added to the standard Service (described in Section 1.0) for an additional fee described in a separate Statement of Work (“SOW”) or Service Order. Contact a sales representative for additional information.

3.1. **On-Site DDoS Detection and Mitigation**: A solution to the network-based DDoS mitigation solution that includes an in-line DDoS Mitigation device (“On-Site Device”) at Customer’s premises, situated between Customer’s firewall and the Internet router. On-Site DDoS Mitigation includes 24x7 attack detection and mitigation of DDoS attacks. If traffic reaches a preconfigured threshold, an alert is sent to CenturyLink to signal that network-based mitigation is required. The On-site Device can be installed at Customer’s premises or at a hosting facility. The premises appliance provides for more timely protection of sites with greater than normal need for high availability, and gives CenturyLink the ability to provide a proactive DDoS detection and mitigation service to sites on third-party networks.

3.2. **Installation at Customer Premises**: If the On-Site Device is installed at Customer’s premises (or within a CenturyLink hosting facility), CenturyLink will ship the On-Site Device, the bypass switch(es) if applicable, and supporting infrastructure, to Customer. Customer is responsible for installing the equipment, as instructed by CenturyLink. Once network connectivity is established, CenturyLink will remotely complete configuration of the On-Site Device. Customer may elect to have direct access to the configuration controls of the On-Site Device, specifically for modifying the inspection and mitigation functions of the device; but CenturyLink exclusively will retain the administrative level access needed to configure the On-Site Device for compatibility with the CenturyLink environment. Customer is solely responsible for the results of its actions with and to the On-Site Device.

3.2.1. **Installation at CenturyLink-Managed Hosting Facility**: If the On-Site Device is installed within a CenturyLink managed hosting facility, CenturyLink will perform the physical installation and network connectivity activities referenced above.

3.2.2. **Customer-Owned-and-Managed On-Site Devices**: CenturyLink will specify devices that Customer is permitted to use with DDoS Mitigation Service if Customer wishes to use a Customer-owned-and-managed On-Site Device (“Customer-Owned Device”). Customer must cooperate with CenturyLink to confirm that CenturyLink DDoS Mitigation Service can accept signaling from the Customer-Owned Device. To ensure compatibility with CenturyLink’s DDoS Mitigation infrastructure, Customer must keep the Customer-Owned Device updated on software versions that are specified and supported by CenturyLink. Customer must purchase at least one instance of CenturyLink network-based DDoS Mitigation Service for each Customer-Owned Device. Customer is responsible for keeping up to date
maintenance and security subscription of its Customer-Owned Devices. CenturyLink is not responsible for any signaling errors created by Customer-Owned Devices. CenturyLink provides no warranty nor makes any guarantees that traffic diversion, or Customer-Owned Device signaling, will operate effectively if Customer-Owned Device are used with CenturyLink network-based DDoS Mitigation Service.

3.2.3. **On-Site DDoS Detection and Mitigation Charges:** The On-Site DDoS Detection and Mitigation is provided as an optional, add-on service to DDoS Mitigation Service 2.0, at an additional, fixed monthly fee. Traffic that is cleansed by the dedicated Arbor Pravail APS appliance is NOT subject to the Service’s hourly cleansing fee. The hourly cleansing fee applies only to traffic that is redirected to a CenturyLink’s cleansing center. If the Customer’s appliance causes the CenturyLink network-based DDoS service to redirect Customer’s traffic to one or more CenturyLink DDoS mitigation cleansing centers, then the Customer is responsible for paying all related fees associated with traffic scrubbing and cleansing-center usage (see “Flat-Fee and Usage-Based Charges” section in this document).

3.3. **Additional Optional Security Services:** Additional optional Security-related services are available through CenturyLink’s Professional Services organization, and are not included with the Service. For more details regarding the services, please contact your CenturyLink sales representative.

4. **Additional Terms**

4.1. **Flat-Fee and Usage-Based Charges for Network-based DDoS mitigation:** In addition to a flat monthly fee, CenturyLink will invoice Customer for the Service for each hour that Customer’s traffic is in mitigation (i.e. flowing through one of the CenturyLink cleansing centers). A separate flat fee, and a separate hourly fee, is assessed for each instance of the Service. Further details regarding hourly fees are as follows:

4.1.1. **Usage Identification and Calculation:** A usage charge is generated for every mitigation event that lasts longer than 15 minutes. The Customer is not billed for any mitigation that lasts 15 minutes or less. Billing of the first hour occurs when the mitigation lasts longer than 15 minutes; however the first 15 minutes are not free, rather they are included in the first hour’s charge; hour two is charged as soon as the mitigation event lasts more than 60 minutes, hour three after 120 minutes, etc. Usage is timed in seconds, rather than minutes, therefore 15 minutes and one second is when usage becomes billable for the first hour. Usage is charged at an hourly rate, therefore any partial hour is rounded up and billed at a full hour.

4.1.2. **Month End:** At the end of each month, usage is ‘closed’ and billed. If mitigation is in force when time crosses into another month, whatever usage has accrued, through the last second of the month, is billed for that month. When calculating usage month-over-month, for a single usage event, the 15 “free” minutes will only be accounted for once, in the first month. If the total duration of the multi-month mitigation is greater than 15 minutes, then the mitigation must be billed according to the total duration, in the applicable month.

4.1.3. **Mitigated Traffic:** If traffic is mitigated for 10 minutes in month one, plus 16 minutes in month two, then nothing is billed for month one, and one hour is billed for month two; 16 minutes in month one, and three minutes in month two, then one hour is billed for month one; and nothing is billed in month two.

4.2. **Ports and VLANs:** For CenturyLink Managed Hosting environments any Ports and VLANs in addition to those included in the standard CenturyLink design shall be subject to incremental charges as set forth in the relevant Order Form. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges.

4.3. **Service Limitations:** At the present time, the detection capability of this Service is not available to CenturyLink Customers located in the Asia-Pacific region.

4.4. **Service Interference:** Customer shall not attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service or any devices used to deliver CenturyLink services. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test DOS/DDoS attacks; penetration testing or external network scans on CenturyLink’s network without the prior written consent of CenturyLink.
4.5. **Customer Acknowledgements**: Customer acknowledges that this Service is just one tool to be used as part of an overall security strategy, and not as a total solution. If the Customer wants to expand their overall security strategy, they should contact their designated CenturyLink account executive for information regarding additional CenturyLink security services.
# Tables and Appendices

## Table 1.0 Roles and Responsibilities

<table>
<thead>
<tr>
<th>Activity</th>
<th>Task</th>
<th>CenturyLink</th>
<th>Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design/Planning</td>
<td>Conduct an initial Service set-up consultation with the Customer. The purpose of this consultation is to develop the Customer’s DDoS mitigation alert policy, determine the appropriate response procedure, answer Customer questions regarding the DDoS Mitigation Service, and define the Customer’s subzones.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>Provide all required information requested during the DDoS Mitigation Service consultation.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide a topology of Customer existing network prior to security review and provisioning of the Service.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide CenturyLink with sufficient system passwords, privileges and access to allowCenturyLink to install, configure, monitor and modify the Service</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Purchase and maintain a reliable, stable and always-on, high speed connection to the public internet (i.e., DSL, T1, cable modem etc.) and/or a standard (POTS) telephone line (with direct inward dialing) for each Customer Site to enable CenturyLink to perform remote network management functions of equipment used to provide the Service</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td>Provision the DDoS Mitigation Service, typically during the business days, and apply the initial policy if required.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customer requests for configuration changes in accordance with response times per service level</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contact Customer for any reconfiguration or</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td>Task</td>
<td>CenturyLink</td>
<td>Customer</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>retuning of the policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration</td>
<td>Manage all system administration passwords for DDoS mitigation system(s).</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Coordinate and facilitate non-CenturyLink network Internet trafficking</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Automatic detection of attacks for Customers who have internet access from CenturyLink</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Customer may also contact the CenturyLink Service Center to request that their traffic be placed into protect mode in response to a suspected attack.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Provide notifications about currently active DDoS mitigations</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Request to end an active DDoS mitigation</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Maintenance and Support</td>
<td>Upgrade software or hardware to maintain the latest versions in operation.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allow CenturyLink to make Service upgrades</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Allow CenturyLink to put Customer’s traffic into protect mode to retune and improve the effectiveness of the Service.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Provide an English-speaking technical contact with current, complete and accurate contact information that is reachable 24/7.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Request changes by contacting the CenturyLink Service Center.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Use CenturyLink’s standard procedures, to notify CenturyLink of the initial and later changes to the information used by CenturyLink to configure the Services.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure that all Customer permissions of any kind needed for the delivery of the Service</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix A Service Level Agreement

#### Table 2.0 Target Response Times and Credits

<table>
<thead>
<tr>
<th>Description</th>
<th>Goal</th>
<th>Remedy (Credit is applied as a % of the applicable charges for the affected Service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to Notify (applies to DDoS Mitigation Service with Attack Detection only)</td>
<td>15 minutes from Initial DDoS Alarm Maps to SLO P1 (Urgent) - Reference Service desk SLO link off Savvisstation.com, Incident Management section.</td>
<td>• 16 – 30 minutes = 50% of monthly Flat-Fee Charges for Network-based DDoS mitigation • More than 30 minutes = 100% of monthly Flat-Fee Charges for</td>
</tr>
<tr>
<td>Description</td>
<td>Goal</td>
<td>Remedy (Credit is applied as a % of the applicable charges for the affected Service)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Time to Mitigate**      | 15 minutes from Customer’s verbal permission to begin Mitigation  
Maps to SLO P1 (Urgent) - Reference Service desk SLO link off Savvisstation.com, Incident Management section. | • 16 – 30 minutes = 50% of monthly Flat-Fee Charges for Network-based DDoS mitigation  
More than 30 minutes = 100% of monthly Flat-Fee Charges for Network-based DDoS mitigation                                                                                         |
| Status Reporting          | If requested by Customer, CenturyLink will provide Customer with a status report by telephone, or e-mail within 60 minutes after the initiation of Mitigation.  
Maps to SLO P1 (Urgent) - Reference Service desk SLO link off Savvisstation.com, Incident Management section.               | Status Reporting and Change Request objectives are intended to be informational only and do not provide any SLA credits and are not subject to any other Goal in this SLA.                        |
| Change Requests           | Customer may request one routine configuration or policy change per 90 day period. CenturyLink will provide the routine configuration and policy change requests within one business day after the request.  
Customer requests that exceed one request per 90 day period may result in additional charges. A routine change means a change when an attack is not taking place.  
Maps to SLO P2 (High) - Reference Service desk SLO link off Savvisstation.com, Request Management | Status Reporting and Change Request objectives are intended to be informational only and do not provide any SLA credits and are not subject to any other Goal in this SLA.                        |
<table>
<thead>
<tr>
<th>Description</th>
<th>Goal</th>
<th>Remedy (Credit is applied as a % of the applicable charges for the affected Service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>section.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Response Times SLA Remedies

In the event that CenturyLink is unable to provide service within the Target Response Time window outlined above, the Customer’s sole and exclusive remedy shall be a service credit shown in the Remedy column of Target Response Time table for the affected Service for each response time failure. The credits will apply to the applicable charges of the affected Service after application of all discounts and do not apply to monthly recurring charges of other services. The maximum service credits issued in any one calendar month will not exceed 100% of the applicable charges of the affected Service. Cumulative credits in any one month must exceed $25.00 to be processed.

SLA Process

**Remedies:** To be eligible for SLA credits, Customer must be in good standing with CenturyLink and current in its obligations. To receive SLA credits, Customer must request any credit due hereunder by submitting an e-mail to billing@CenturyLink.com within sixty (60) days of the conclusion of the month in which it accrues. Customer waives any right to credits not requested within this sixty (60) day period. Credits will be issued once validated by CenturyLink and applied toward the invoice which Customer receives no later than two months following Customer’s credit request. All performance calculations and applicable service credits are based on CenturyLink records and data.

The applicable SLA provides Customer’s sole and exclusive remedies for any Service interruptions, deficiencies, or failures of any kind.

**Limitations:** This SLA will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under this SLA, for any event that adversely impacts the Service that is caused by: (a) the acts or omissions of Customer, its employees, contractors or agents or its end users; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink; (c) Force Majeure Events; (d) scheduled service maintenance, alteration or implementation; (e) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information; (f) CenturyLink’s lack of access to the Customer premises where reasonably required to restore the Service; (g) Customer’s failure to release the Service for testing or repair and continuing to use the Service on an impaired basis; (h) CenturyLink’s termination of Service for Cause or Customer’s use of Service in an unauthorized or unlawful manner; or (i) improper or inaccurate network specifications provided by Customer.

**Customer Termination Rights:** Customer may terminate the affected Service without cancellation charges if CenturyLink is unable to meet the Goals herein within a 60 day cure period. The 60 day cure period will begin after a trouble ticket is opened. Customer may terminate the affected Service by providing written notice to the Customer Service Center with a courtesy copy to the attention of CenturyLink’s General Counsel within 20 days after the 60 day cure period ends. Such termination will be effective 45 days after receipt of written notice by CenturyLink of termination from Customer, unless Customer requests Service to be continued and establishes a new termination date after 45 days. Customer is responsible for all Service charges until the termination date. If Customer fails to notify CenturyLink in the manner set forth in this section with respect to the applicable termination right, Customer will have waived its right to terminate the affected Service.
Definitions

**Bypass switch:** A bypass switch provides a fail-safe, inline protection for an optional DDoS mitigation appliance. A bypass switch uses a heartbeat packet to protect the network link from the mitigation appliance failure. If the heartbeat packet is disrupted, then the bypass switch removes this point of failure by automatically shunting traffic around the mitigation appliance whenever the appliance is incapable of passing traffic.

**CenturyLink Service Center:** The primary organization for resolving infrastructure issues that is staffed 24/7/365 to respond in a timely manner to incidents and requests pertaining to Customer IT infrastructure.

**DDoS:** A distributed denial-of-service attack in which many systems attack a single target, thereby causing denial of service for users of the targeted system. This typically results in the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

**Event:** A security occurrence detected and reported by the CenturyLink DDoS Mitigation Service. An Event does not necessarily constitute an actual security incident, and must be investigated further to determine its validity.

**Incident:** Any single Event or collection of Events that have been determined by a CenturyLink analyst reviewing the data to potentially be of security consequence. Incidents may include Events that are currently being investigated and actual attacks that may be in progress.

**Mitigation:** The mitigation of DDoS attacks by using CenturyLink-supplied mitigation equipment located in CenturyLink’s network.

**Reasonable Effort:** A fair estimate of an activity, measured with reference to the particular circumstances, scheduling agreements and diligence as might be expected within the grounds of the Service. Just because something is possible and reasonable does not mean CenturyLink has to do it if it is not necessarily reasonable for the business.

**Subnet:** A subnet is a logically subdivision of an IP network that shares a common address component. Devices on the same subnet are have the same prefix and are addressed with a common, identical, most-significant bit-group in their IP address. For example, all devices with IP addresses that start with 1.1.1.* would be part of the same subnet.

**Subzone:** A subzone is a network element that the Service will protect. A subzone can be comprised of a single device (i.e. a network server, client or router), a subnet, multiple subnets, or any combination of the aforementioned.