CenturyLink Service Guide

DDoS Mitigation Service

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 Security 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. This SG applies to the following service packages:

DDoS Mitigation 1.0
DDoS Mitigation 2.0
DDoS Mitigation 3.0
DDoS Appliance Service 1.0
DDoS Appliance Service 2.0

Version	Previous	Section Modified	Date
SEC-20180301-SG-DDoSMitigationService	SEC-20141015-SG-DDoSMitigationService	All	March 1, 2018

Table of Contents

Service Description

1. **Service Description:** DDoS Mitigation Service is a CenturyLink provided service (the "Service"). The Service provides managed network-based distributed denial of service ("DDoS") detection and mitigation with 24/7 response to DDoS attacks for Customers who receive Qualifying Internet Services from CenturyLink. CenturyLink can also provide mitigation services without detection for internet services Customer receives from other internet service providers ("Third Party Networks"). Because this is a network-based service, DDoS mitigation equipment is not required in the Customer's environment. The standard features of the Service consist of the installation, configuration, administration, monitoring & detection, maintenance and support for the components listed in subsection 1.1 below. The Service is subject to the DDoS Mitigation service level agreement ("SLA") located at http://www.centurylink.com/legal/ which is subject to change from time to time effective upon posting. For Customer's claims related to Service deficiencies, interruptions, delays or failures, Customer's exclusive remedies are limited to those remedies set forth in the SLA..

1.1. Service Components:

1.1.1. **Attack Detection:** Monitoring and detection includes automatic detection of Events for Customers who have a Qualifying Internet Service from CenturyLink only. There is no Event detection component with Third Party Networks. Customer traffic is monitored continuously. Mitigation of Customer traffic begins after detected Events are determined to be Incidents and Customer has provided Mitigation approval, as further detailed in subsection 1.1.2 below.

1.1.2. **Initiation of Mitigation:** Customer must approve Mitigation by: (i) providing verbal permission for each Incident, (ii) pre-authorizing CenturyLink to manually initiate Mitigation for each Incident, or (iii) pre-authorizing CenturyLink to configure systems to auto initiate Mitigation for Incidents. If Customer selects the verbal permission option, Customer can call the CenturyLink support team to begin Mitigation or CenturyLink will contact Customer to obtain approval when a detected Event is determined to be an Incident. Customers using Third Party Networks may only utilize option (i) providing verbal permission to CenturyLink to commence Mitigation and cannot pre-authorize using options (ii) or (iii). CenturyLink will not initiate Mitigation until verbal permission is received. For Qualifying Internet Services, and Customers who select either the pre-authorized permission option or the auto-mitigate option, Customer must provide CenturyLink written notice via a change ticket in Control Center or Savvisstation.com, as applicable, of its pre-authorized permission to begin Mitigation. Customer may later withdraw pre-authorized permission via a change ticket. Change tickets require 24 hours advance notice. Customer will pre-authorize which Mitigation countermeasures CenturyLink may deploy, subject to CenturyLink's approval. Customer understands that additional countermeasures beyond the pre-authorized countermeasures may be required to Mitigate the Incident, which may require CenturyLink to contact Customer's Site Contact.

1.1.3. **Diversion of Attack-Traffic to a CenturyLink cleansing center:** Once approved by Customer as per Section 1.1.2 above, CenturyLink will divert traffic to a cleansing center. CenturyLink reserves the right to route traffic to a cleansing center in a different region and/or country in its reasonable discretion. Customer expressly acknowledges and consents to (1) such transfer of traffic across country borders and/or (2) CenturyLink's, its affiliates and authorized third party's access to Customer's traffic information (e.g. port, flow, protocols, IP address) in order for CenturyLink to provide the Service hereunder. CenturyLink is not responsible for security/protection of the forward traffic since the level of security/protection of the traffic and traffic design coming into the scrubbers is solely at the Customer's discretion. In addition CenturyLink is not responsible for any loss or corruption of data or information. CenturyLink's obligations related to data are exclusively governed by the Security and Compliance section of the applicable Agreement.

1.1.3.1. **For Customers who use a Qualifying Internet Service:** CenturyLink will take the additional action to divert attack traffic to a CenturyLink cleansing center for filtering/mitigation.

1.1.3.2. **For Customers who use Third Party Networks:** For internet transport on Third Party Networks, there are two options for diverting traffic to a CenturyLink cleansing center:

1.1.3.2.1. **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 Security Operations 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 the modification of DNS.

1.1.3.2.2**. Domain Name Service ("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 Guidelines for the Customer to follow.

1.1.4. **Forwarding of Cleansed Traffic:** Once the Customer's traffic is cleansed of malicious packets, CenturyLink will forward the traffic back to its original destination. This process is different depending on whether the traffic originated on a Qualifying Internet Service or a Third Party Network, and the method used to divert traffic to the CenturyLink cleansing center. Forwarding methods include the following:

1.1.4.1. **Qualifying CenturyLink Network:** Traffic that originates on the Qualifying Internet Services, is forwarded to the cleansing center via BGP, and is returned to the CenturyLink core router nearest the Customer via MPLS tunneling.

1.1.4.2. **Third-Party Networks**

1.1.4.2.1. **Where BGP was used to divert traffic:** Traffic that originates on Third Party 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. Customer must enable a GRE tunnel at that router's end of the connection. As a part of this Service, CenturyLink provides Guidelines for the Customer to follow.

1.1.4.2.2. **Where DNS was used to divert traffic:** Traffic that originates on Third Party 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 Network Address Translation ("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 NAT rerouting process, and forwarded to the Customer's destination IP addresses via the internet. CenturyLink provides Guidelines for the Customer to follow.

1.1.4.2.3. CenturyLink is not responsible for security/protection of the cleansed traffic transferred back to its original destination since the level of security/protection of the traffic and traffic design coming into the scrubbers is solely at the Customer's discretion.

1.1.5. **Discontinuation of Mitigation:** CenturyLink will discontinue Mitigation at the Customer's verbal request or until CenturyLink reasonably determines that the DDoS attack has subsided. 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). When CenturyLink determines that the DDoS attack has subsided, CenturyLink will attempt to notify Customer. If CenturyLink is able to contact Customer, Customer will have the option at that time to discontinue Mitigation or continue Mitigation for up to an additional four hours. At the end of the four hours, CenturyLink will discontinue Mitigation as long as another attack has not occurred. If CenturyLink is unable to contact Customer, CenturyLink will continue Mitigation for another four hours, after which point CenturyLink will discontinue Mitigation as long as another attack has not occurred.

1.2. **Installation:** CenturyLink will provide the 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, 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.

1.2.2. **Subnets:** CenturyLink recommends that subzones be broken down by function (Web, DB, etc.) so hosts within each subzone 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 require Customer to provide a change request by contacting the CenturyLink Security Operations Center.

1.4. **Administration:** CenturyLink will provide the 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.

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

1.6. **Maintenance and Support:** CenturyLink will provide the 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 will attempt to 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 Customer doesn't respond and/or doesn't allow for retuning in a timely manner, then the Service may be less effective at detecting and mitigating attacks until the retuning is accomplished and no SLA credits will be deemed to apply. 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.

2 **Customer Responsibilities:** In addition to the responsibilities listed below, 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 below and 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. CenturyLink shall not be liable for any failure to perform in the event Customer does not fulfill Customer's responsibilities and requirements as detailed herein and in the event of Customer's errors or omissions in setting up the environment.

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 used to deliver CenturyLink services. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test DDoS attacks, penetration testing or external network scans on CenturyLink's network without the prior written consent of CenturyLink.

2.3. **Mitigations:** Customer is responsible for requesting that CenturyLink end a DDoS mitigation as defined in the Discontinuation of Mitigation section of this document.

2.4. **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 CenturyLink provided managed security services, as applicable.

2.5. **Change Request:** Customer must request changes by contacting the CenturyLink Security Operations Center. Customer must provide complete authentication credentials to the CenturyLink Security Operations Center when requesting changes.

2.6. **Third Party Networks:** Customer whose traffic originates on Third Party 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. Failure to do so may result in CenturyLink's inability to provide the Service. Customers using a Third Party Networks for internet transit are responsible for detecting DDoS attacks on their public-facing IP addresses, and must notify the CenturyLink Security Operations Center if they chose to divert their traffic to a CenturyLink DDoS Mitigation cleansing center. Customers may purchase CenturyLink's optional DDoS Appliance Service which is an on-site DDoS appliance with detection and mitigation capabilities. It provides a viable means for enabling attack detection on Third Party Networks. Customers must order DDoS Mitigation in order to purchase DDoS Appliance Services. See the "Optional DDoS Appliance Services" section of this document for more details. DDoS Appliance Service will work with the three internet options.

2.7. **GRE Tunneling:** Customer must be able to enable a GRE tunnel on the router that the cleansed traffic is returned to.

2.8. **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.

2.9. Neither Customer nor its representatives shall attempt in any way to circumvent or otherwise interfere with any security precautions or measures of CenturyLink relating to the Service or any other CenturyLink equipment.

2.10. With respect to the DDoS Appliance Service, Customer acknowledges and agrees that CenturyLink's ability to provide the DDoS Appliance Service is limited to currently supported configurations (including but not limited to related operating systems, hardware or software). If any configuration or version is identified as "unsupported" or not compatible by CenturyLink or a vendor, the DDoS Appliance Service is subject to all of the following conditions and/or requirements: CenturyLink, in its reasonable discretion may elect to charge the Customer for any support or additional tasks/work incurred by CenturyLink resulting from Customer's continued use of unsupported configuration until Customer purchases the required and supported upgrades or extended support at an additional cost from the vendor. CenturyLink will need to apply software updates to the managed DDoS Appliance from time to time in order to provide the DDoS Appliance Service. When the appliance hardware ages over time to the degree that it can't support such software upgrades or the hardware itself goes into a more costly extended support state or an end of support state, additional service fees may apply for extended support or replacement of the appliance with a currently supported version. Customer's failure to do so may result in CenturyLink's inability to provide the Services and CenturyLink shall have no liability therefrom.

2.11. For a Customer owned DDoS appliance, the Customer is responsible for any software or hardware changes required by CenturyLink to maintain compatibility with the DDoS Service.

2.12. Customer consents to CenturyLink's and its affiliates or subcontractors' use and transfer to the United States, or other countries, data or information (including Customer Contact information such as names, phone numbers, addresses and/or email addresses) of the Customer for the sole purpose of: fulfilling its obligations

under the Agreement; and (ii) providing information to Customer about CenturyLink's products and services. Customer represents that it will ensure that all information provided to CenturyLink is accurate at all times and that any business contact has consented to CenturyLink's processing of such information for the purposes identified herein.

3. **Optional DDoS Appliance Service.** At Customer's option and expense, Customer can choose to separately purchase the DDoS Appliance Services for an additional fee. Contact your sales representative for additional information.

3.1. DDoS Appliance Service: Enhances the network-based DDoS Mitigation solution with DDoS Appliance Service which is a device provided by CenturyLink ("DDoS Appliance") situated between Customer's firewall and the Internet router. CenturyLink facilitates this service remotely. The DDoS Appliance Service requires a separate Service Order and can only be purchased if Customer also purchases CenturyLink DDoS Mitigation 1.0, 2.0, or 3.0. The DDoS appliance has an automatic traffic by pass mode if there is a failure. This allows traffic to pass through as if the appliance wasn't there. In this case, the attack traffic would be signaled to the DDoS Service for mitigation. The DDoS Mitigation Service SLA does not apply to the DDoS Appliance Service. The DDoS Appliance Service is provided as is and as available.
DDoS Appliance Service 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 DDoS Appliance can be installed at Customer's premises or within a CenturyLink managed environment. The DDoS Appliance provides both an "always on" mode and additional Layer 7-type protection of sites with greater than normal need for high availability. Customer's access to the appliance is limited to self-configuring certain mitigation settings.

Customers who purchase DDoS Appliance Service have the option to purchase Hardware Security Module ("HSM") as an added feature. HSM can be installed in the DDoS Appliance to decrypt SSL packets, inspect, and drop attack traffic while re-encrypting non-attack traffic to send on. This option carries additional fees.

3.1.1. **DDoS Appliance Installation at Customer Premises**: If the DDoS Appliance is installed at Customer's premises, CenturyLink will ship the DDoS Appliance and the Bypass Switch(es) if applicable, to Customer. Customer is responsible for installing the appliance, as instructed by CenturyLink. Once network connectivity is established, CenturyLink will remotely complete configuration of the DDoS Appliance. Customer's access to the appliance is limited to self-configuring certain mitigation settings/controls, specifically for modifying the inspection and Mitigation functions of the appliance; but CenturyLink exclusively will retain the administrative level access needed to configure the DDoS Appliance for compatibility with the CenturyLink environment. Customer is solely responsible for the results of its actions with and to the DDoS Appliance. At the end of the applicable Service Term, Customer shall promptly return the appliance to CenturyLink in the same condition as installed.

3.1.2. **DDoS Appliance Installation in CenturyLink Managed Hosting Environment**: If the DDoS Appliance is installed within a CenturyLink managed hosting environment, CenturyLink (either directly or through a third party) will perform the physical installation and network connectivity activities referenced above.

4. **Signaling from Customer Owned and Managed DDoS Appliance**: CenturyLink will allow Customer to provide specific Customer owned and managed DDoS Appliances within certain parameters as approved by CenturyLink. CenturyLink will specify devices that Customer is permitted to use with CenturyLink's DDoS Mitigation Services if Customer wishes to use a Customer owned and managed DDoS Appliance ("Customer Owned Appliance"). Customer must cooperate with CenturyLink to confirm that CenturyLink DDoS Mitigation Service can accept signaling from the Customer Owned Appliance. For compatibility with CenturyLink's DDoS Mitigation infrastructure, Customer must keep the Customer Owned Appliance 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 Appliance. Customer is responsible for keeping up to date the maintenance and security subscription(s) of its Customer Owned Appliances. CenturyLink is not responsible for any signaling errors created by Customer Owned Appliances. CenturyLink provides no warranty nor makes any

guarantees that traffic diversion, or Customer Owned Appliance signaling, will operate effectively if Customer Owned Appliances are used with CenturyLink network-based DDoS Mitigation Service.

5. Additional Terms

5.1. Flat-Fee Charges for Network-based DDoS Mitigation Services: An install fee and fixed monthly fee are assessed for each instance of the Service unless a Customer has a different billing plan expressly agreed by CenturyLink.

5.2. 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 Service Order. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges.

5.3. Consent to Access and Use Customer Information: Customer authorizes CenturyLink or its authorized vendor and expressly consents to CenturyLink's and/or its vendor's access, use and transfer of Customer's contact information and traffic information, including ports, protocols, IP address, header and content information associated with packets IPS, add more to the list here associated with Customer's IP-network traffic from, to, and/or between domestic US locations and international locations solely in connection with its provision of Service hereunder.

5.4. Customer acknowledges that the Services endeavor to mitigate security incidents, but such incidents may not be mitigated entirely or rendered harmless. Customer should consider any particular Service as just one tool to be used as part of an overall security strategy and not a guarantee of security.

Tables

Table 1.0 Roles and Responsibilities

Activity	Task	CenturyLink	Customer
Design/Planning	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.	X	
Installation	Provide all required information requested during the DDoS Mitigation Service consultation.		X
	Provide a topology of Customer's existing network prior to security review and provisioning of the Service.		X
	Provide CenturyLink with sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service.		X
	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.		X
Configuration	Provision the DDoS Mitigation Service, during business days, and apply the initial policy if required.	X	
	Customer requests for configuration changes are in accordance with response times in the SLA.		X
	Contact Customer for any reconfiguration or	X	

Activity	Task	CenturyLink	Customer
	retuning of the policy.		
Administration	Manage all system administration passwords for DDoS Mitigation system(s).	X	
	Coordinate and facilitate non-CenturyLink network Internet trafficking.		X
Monitoring	Automatic detection of attacks for Customers who have internet access from CenturyLink.	X	
	The Customer may also contact the CenturyLink Security Operations Center to request that their traffic be placed into protect mode in response to a suspected attack.		X
	Provide notifications about currently active DDoS Mitigations.	X	
	Request to end an active DDoS mitigation		X
Maintenance and Support	Upgrade software or hardware to maintain the latest versions in operation.	X	
	Allow CenturyLink to make Service upgrades.		X
	Allow CenturyLink to put Customer's traffic into protect mode to retune and improve the effectiveness of the Service.		X
	Provide an English-speaking technical contact with current, complete and accurate contact information that is reachable 24/7.		X
	Request changes by contacting the CenturyLink Security Operations Center.		X
	Use CenturyLink's standard procedures, to notify CenturyLink of the initial and later changes to the information used by CenturyLink to configure the Services.	X	
	Ensure that all Customer permissions of any kind needed for the delivery of the Service		X

Activity	Task	CenturyLink	Customer
	are in place at all times.		
	Notify CenturyLink in advance of any Customer network topology or system changes that may affect the Service or the effectiveness of the DDoS Mitigation system policy.		X
	Permit CenturyLink to divert traffic to a CenturyLink cleansing center for filtering/Mitigation.		X
	For Customers who also use CenturyLink Qualifying Internet Services, divert traffic to a CenturyLink cleansing center for filtering/Mitigation.	X	
	For Customers who use non-CenturyLink internet services, divert traffic to a CenturyLink cleansing center for filtering/Mitigation.	X	X
	Perform filtering/Mitigation of DDoS attack traffic.	X	
	Forward cleansed traffic to Customer.	X	
	For GRE based cleansed traffic delivered to Customer, configure the far end of GRE tunnel on Customer's equipment.		X

Definitions

Bypass Switch: A Bypass Switch provides additional 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 Security Operations Center: The primary organization in CenturyLink supporting the DDoS Mitigation and DDoS Appliance services.

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 abnormality detected by the CenturyLink DDoS Mitigation Service that could represent a DDoS attack. An Event does not necessarily constitute an actual security Incident, and must be investigated further to determine its validity.

Guidelines: There are applicable technical guidelines provided by CenturyLink to Customer for informational purposes only. These Guidelines are not contractually binding, however, customer's failure to configure any of the applicable methods described in the Guidelines will affect CenturyLink's ability to provide the Services. Some examples of these Guidelines are the GRE Tunneling Guidelines and DNS-Diversion Guidelines.

Incident: Any single Event or collection of Events that have been reasonably determined to be a DDoS attack by CenturyLink DDoS mitigation systems and/or CenturyLink analysts reviewing the data.

Mitigation: The attempted removal of DDoS traffic from good traffic using CenturyLink-supplied mitigation equipment located in CenturyLink's network.

Qualifying Internet Services: The following CenturyLink Internet services are compatible with the Service: CenturyLink IQ® Networking Internet Port, CenturyLink-provided Network-Based Security, and CenturyLink Hosting Area Network (HAN) Internet Service.