Service Beschreibung DDoS Guard Services

Version / Datum
1.0
17.12.2020

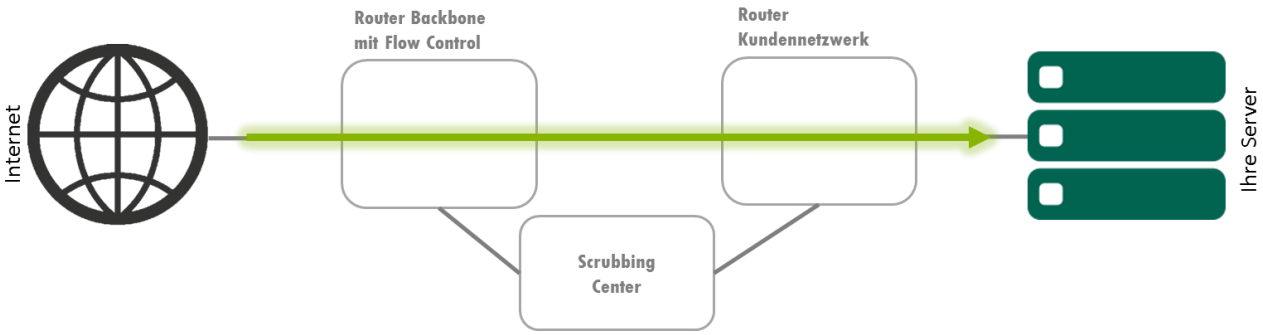
Autoren
Product Management

Inhaltsverzeichnis

1. Servicebeschreibung

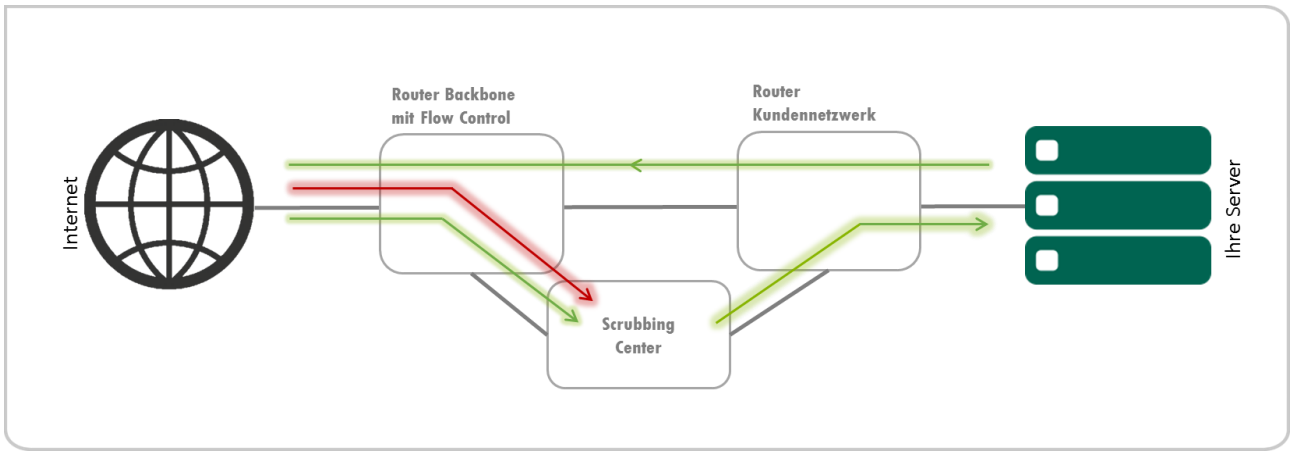
Die Bedrohung durch DDoS Attacken hat sich in den letzten Jahren auf eine breitere Palette von Branchen, Unternehmensgrössen und Infrastrukturen erweitert. Niemand ist mehr immun. Aufgrund der Verfügbarkeit von preiswerten Bot-Netzen und reflektierenden Angriffstechniken gibt es mittlerweile wenig Unterschied zwischen der Industrie und der Grösse und Umfang des Angriffs. Green Datacenter AG (GDC) bietet zuverlässigen Schutz gegen diese lästigen Angriffe.

Mit DDoS Guard erhalten Sie eine automatisierte Abwehrlösung zum Schutz Ihrer Netzwerke. DDoS Guard schützt Ihre Infrastruktur gegen volumetrische Attacken bis zu 3.5 Tbit/s. Geschützt sind alle Services bis OSI Layer 4. GDC bietet den Schutz in den Varianten DDoS Guard und DDoS Guard basic an. Die Optionen „Protection on Demand“ und „Always On“ DDoS Schutz sind auf Anfrage erhältlich und unterliegt nicht dieser Service Description. Eine nähere Beschreibung zu diesen Optionen befindet sich in Kapitel 1.5.



Normaler Modus – Datenstrom wird überwacht

Attacken werden von DDoS Guard automatisch erkannt **(Detection)** und an unser Scrubbing Center umgeleitet **(Diversion-Initiation)**. Im Scrubbing Center wird der Datenstrom gefiltert **(Mitigation)** und sauber über ein NVGRE Tunnel an das Kundennetzwerk weiter geleitet. Weiter wird der Kunde zeitnah durch den GDC Helpdesk kontaktiert und das weitere Vorgehen koordiniert.



Unter Attacke – Datenstrom wird gefiltert

Es ist nicht relevant, wie lange eine DDoS Attacke dauert. Nach jedem Angriff bleibt der Datenstrom über mehrere Stunden im Scrubbing Center. Ein kurzfristig wiederholter Angriff bleibt somit wirkungslos. Der Datenstrom wird erst nach der Abkühlungsphase und nach Absprache mit dem Kunden wieder in den normalen Betrieb übergeben. Dabei werden folgende Bedingungen berücksichtigt:

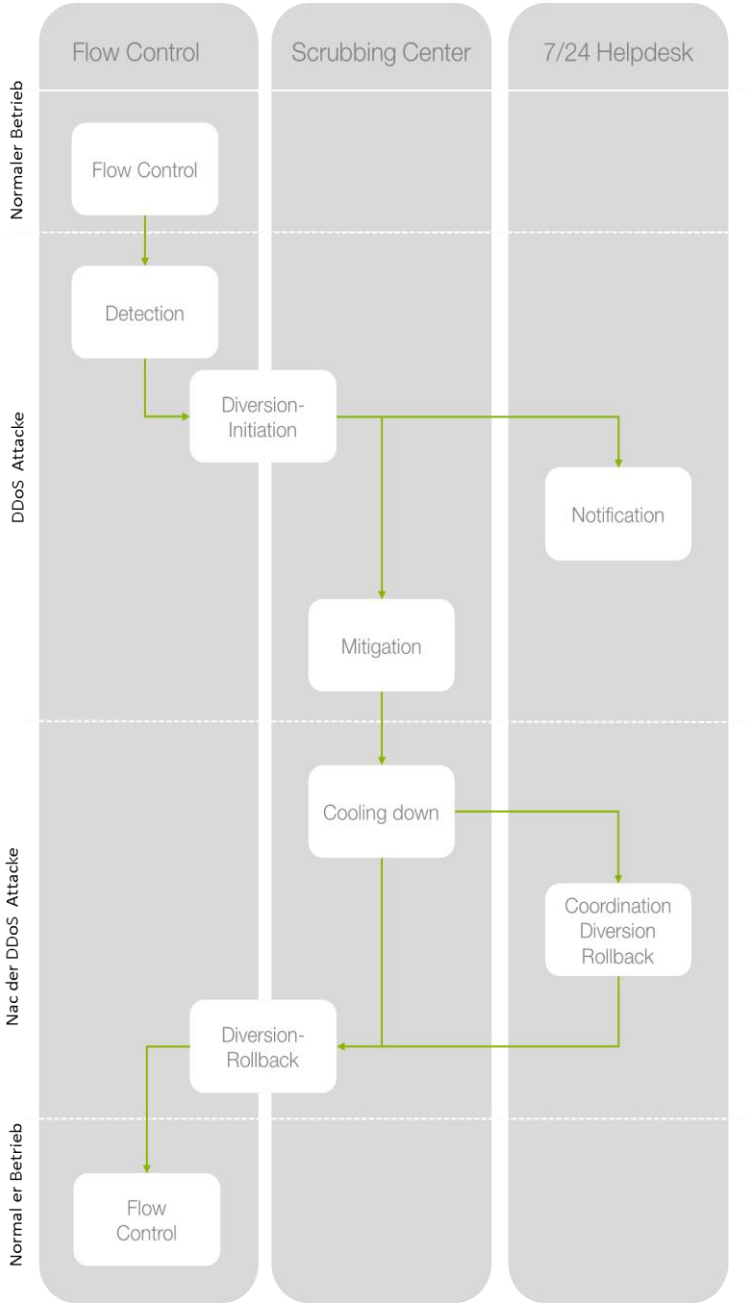
- Das Scrubbing Center stellt in einem längeren Zeitraum von ungefähr 48 Stunden keinen Fluss von bösartigen Datenpaketen mehr fest **(Cooling Down)**.

  → Somit ist auch ein Angriff in mehreren Wellen erfolglos und Ihre Geschäftstätigkeit wird weniger beeinträchtigt

- Die Umstellung in den Normalbetrieb wird in der Nacht oder an den vom Kunden definierten Randzeiten durchgeführt **(Coordination Diversion Rollback nur bei DDoS Guard)**.

  → Kurze Unterbrüche bei der Rücklenkung des Datenstroms vom Scrubbing Center zum Normalbetrieb sind aufgrund des BGB Protokolls leider nicht gänzlich aus zu schliessen. Mit einer koordinierten Umstellung in den Normalbetrieb wird diesem Umstand Rechnung getragen **(Diversion-Rollback nur bei DDoS Guard)**.

1.1 Genereller Ablauf DDoS Mitigation



Kommentar / KPIs

Daten Monitoring
on Layer 4

Zeit bis zur Entdeckung:
sofort

Zeit bis Datenverkehr umgeleitet ist:
1 Minute

Zeit um Kunde zu Benachrichtigen:
SMS/Email – 3 Minuten
Telefon – 30 Minuten

Start Gegenmassnahmen:
UDP / ICMP floods – 5 Minuten
SYN Floods – 5 Minuten
TCP Flag Abuses – 5 Minuten
DNS Reflection – 10 Minuten
DNS Flood Attack – 10 Minuten

«Abkühlung» - Cool Down
ungefähr 48 Stunden

Rücknahme Datenumleitung
auf Kundenverlangen aber nicht später als 48 stunden nach Begin der Attacke.
Diese Rücknahme bedingt eine Abschaltung der Internetverbindung für ca. 3 Minuten und sollte daher ausserhalb der Arbeitszeiten geplant werden.

Traffic Monitoring
auf Layer 4

Zeitlicher Ablauf Mitigation einer DDoS Attacke

* Die Benachrichtigung des Kunden über der laufenden Angriff und die koordinierte Rückschaltung auf den Normalbetrieb erfolgt nur bei DDoS Guard, nicht aber bei DDoS Guard basic.

1.2 Aufbaukomponenten

DDoS Guard besteht aus den folgenden Komponenten:

- *Flow Collector*

  Empfängt die Flowdaten von allen Peering Points und führt die Angriffserkennung durch. Wird eine Attacke erkannt, wird der Datenverkehr des betroffenen Segments via BGP Rerouting zum Scrubbing Center geführt.

- *Scrubbing Center*

  Filtert zu einem Angriff gehörende Daten aus dem Stream und leiten den gesäuberten Datenstrom zur Kundeninfrastruktur weiter.

- *365 x 24 Helpdesk (nicht bei DDoS Guard basic)*

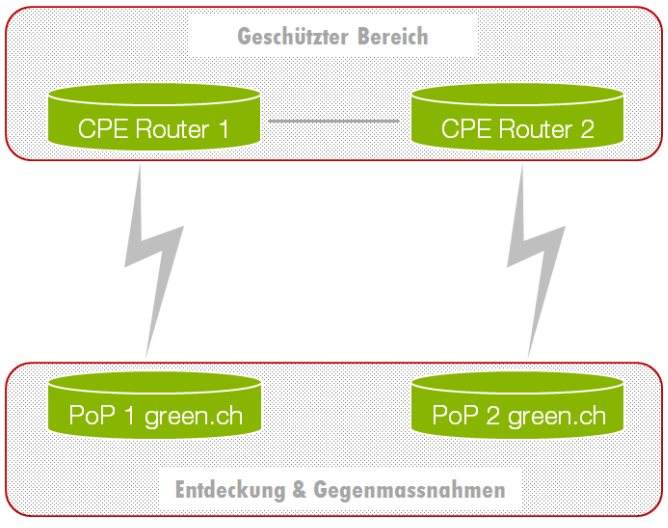
  Überwachungs- und Koordination Stelle. Im Falle einer Mitigation nimmt der 7/24 Helpdesk mit den vereinbarten Eskalationspunkten des Kunden Kontakt auf und stimmt das weitere Vorgehen ab. Dabei werden folgende Punkte mit den betroffenen Stellen überprüft:

  - Grund der Mitigation
  - Zeitliche Dimension der Attacke (Start, tatsächliche Dauer, etc.)
  - Bestimmung des Schweregrads
  - Abwägung bzw. Koordination zusätzlicher Massnahmen falls notwendig

1.3 Produktverfügbarkeit

DDoS Guard kann als Schutz vor DDoS Angriffen für folgende GDC oder Datacenter Connectivity Services eingesetzt werden:

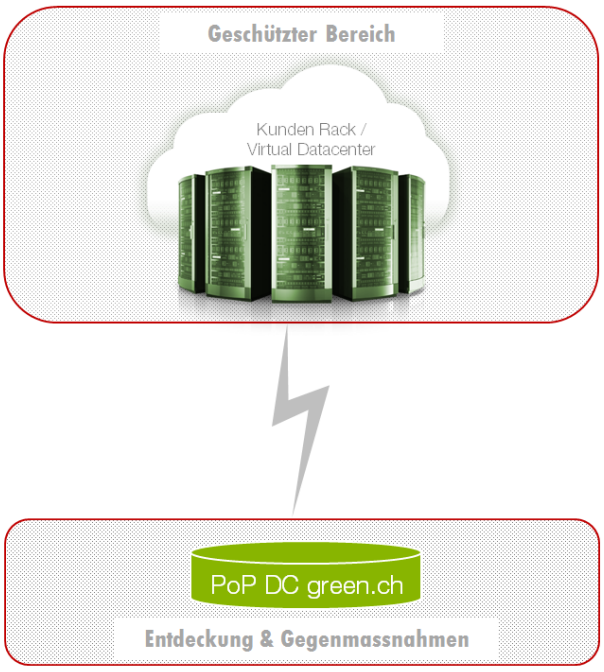
1.3.1 Dedicated Access (Standard, Extended, Premium)



DDoS Guard schützt zuverlässig und automatisiert die Kundeninfrastruktur hinter den dedizierten Leitungen.

Die Detection sowie die Mitigation wird im Backbone von GDC abwickelt. Im Netzwerk des Kunden werden für diese Prozesse keine Ressourcen beansprucht.

1.3.2 Datacenter und Virtual Datacenter Access



Mit Datacenter Access erhalten Sie als Datacenter-Kunde einen hochverfügbaren Zugang ins Internet. Ihre Anbindung erfolgt an einem zentralen schweizerischen Internetknotenpunkt.

DDoS Guard schützt den Anschluss Ihres Kundenracks (ob virtuell oder physisch) und erhöht die Verfügbarkeit Ihrer IT Infrastruktur.

1.4 Service Aufbau

Neben DDoS Guard bietet GDC auch Schutz für Kunden mit kleineren Netzwerksegmenten an. DDoS Guard basic ist noch etwas einfacher aufgebaut und teilt den im Angriffsfall umgeschalteten Adressbereich mit anderen Kunden.

1.4.1 DDoS Guard

Die zu schützenden Objekte werden mit fixen IP Adressen aus einem vordefinierten Range ausgestattet. Sollte bereits ein IPv4 /24 Netzwerk (256 Adressen) auf Kundenseite vorhanden sein, kann dies für DDoS Guard verwendet werden.

Für kleinere Netzwerke müssen die IP Vorgaben von GDC akzeptiert werden. Wird der DDoS Guard Service aufgehoben, verfallen die zugehörigen IP Adressen. Der IP Change ist für alle Netze zwingend. Ausgenommen von dieser Regelung sind unabhängige /24 IPv4 Netzwerke (PI Networks).

1.4.2 DDoS Guard basic

DDoS Guard basic beinhaltet ein von GDC definiertes und zugeteilten /28 IPv4 Segment (16 Adressen).
Es ist Teil eines mit anderen Kunden gemeinsam genutzten /24 Netzwerks.
Die Umschaltung auf das Scrubbing Center bei Angriff erfolgt immer für das ganze /24 Netzwerk – also auch für alle Mitbenutzer. Die die Kontaktaufnahme bei Angriff entfällt und die Rückschaltung wird nach abebben des Angriffs ohne Rücksprache mit den Kunden in den frühen Morgenstunden ausgeführt.

1.4.3 Vergleich DDoS Guard und DDoS Guard basic

Eigenschaft	DDoS Guard	DDoS Guard basic
geschütztes Netzwerk Segment	eigenes /24 Segment (256 Adressen), oder vorhandenes /24 PI- Segment	/28 Segment innerhalb eines gemeinsam genutzten /24 Segment inbegriffen
grössere Adressbereiche	optional weitere /24 Segmente oder grösser	optional grössere Bereiche bis maximal /26 (64 Adressen)
Service Desk	365 x 24	Mo bis Fr 06:00 bis 22:00 Uhr
Notifizierung bei Angriff	Telefonisch und per Mail	keine
Rückschaltung nach Angriff	Koordiniert mit Kunde	Automatisch, in den frühen Morgenstunden
DDoS Dashboard	ja	nein

1.5 Optionen für DDoS Guard

Beide Optionen sind exklusive für DDoS Guard Kunden erhältlich

1.5.1 DDoS Guard – Protection on Demand

Bei „Protection on Demand“ bestimmt der Kunde, wann die Mitigation eines Angriffs beginnen soll. Der Kunde ist in der Verantwortung den Angriff zu bemerken und bei seinem Provider zu eskalieren. Es finden keine automatisierten Prozesse statt.

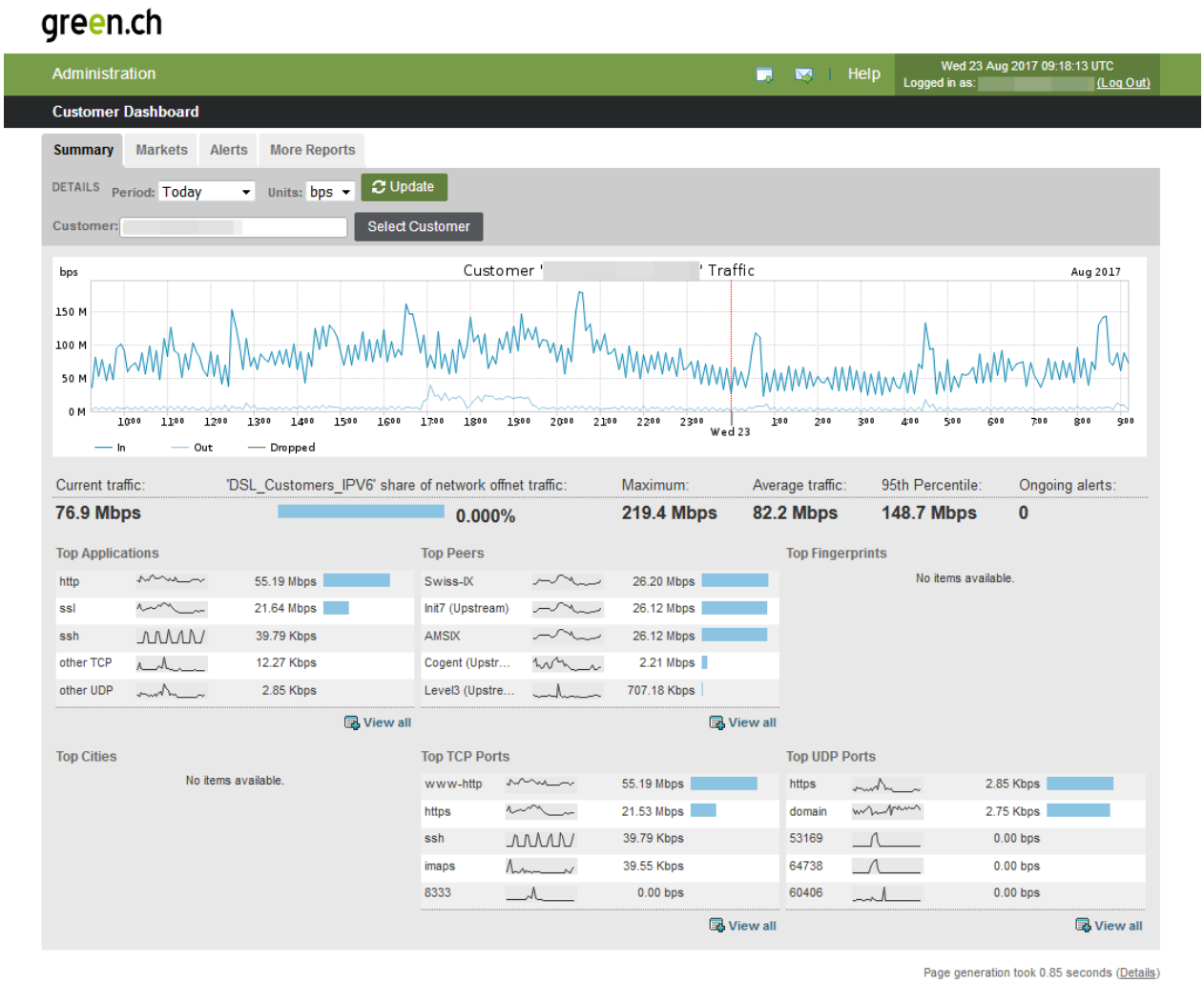
1.5.2 DDoS Guard – Always On

Mit dieser Variante wird der Datenstrom dauerhaft durch das Scrubbing Center geleitet. Angriffe werden sofort erkannt und es geht keine Zeit für die Detection und Diversion-Initiation verloren. Weiter muss auch kein Aufwand bezüglich der Rückführung des Datenstroms in den Normalbetrieb betrieben werden. Die dauerhafte Ressourcenbindung für die Mitigation schlägt sich in den Kosten für den Service nieder.

1.6 Management und Controlling Portale

1.6.1 DDoS Guard Customer Dashboard

Das DDoS Guard Customer Dashboard gibt dem Kunden die Möglichkeit, seine geschützten Connectivity Services zu überwachen. Neben einem Summary Report werden unter anderem auch die Alarme überwacht und protokolliert.



Ansicht DDoS Guard Customer Dashboard

Um detaillierte Information über den Traffic einzusehen, stehen dem Kunden folgende Detail Reports zur Verfügung:

BGB Traffic Information

ASNs (All)
This report shows in and out data for a selected customer, broken down by aggregate ASNs (origin and transit). Select which customer's data is displayed from the Customer drop-down menu.

ASNs (NULL)
This report shows in and out data for a selected customer for locally sourced or destined traffic based upon iBGP-only traffic. Select which customer's data is displayed from the Customer drop-down menu.

ASNs (Origin)
This report shows in and out data for a selected customer, broken down by origin ASNs. Select which customer's data is displayed from the Customer drop-down menu.

ASNs (Peer)
This report shows in and out data for a selected customer, broken down by transit ASNs. Select which customer's data is displayed from the Customer drop-down menu.

NextHop
This report shows source and destination traffic data for a selected customer, broken down by nexthop. You can select which customer's data is displayed from the Customer drop-down menu.

Geographic Information

Cities
This report shows traffic in and out of a selected customer broken down by the backbone city of origin.

Countries
This report shows traffic in and out of a selected customer broken down by the external country of origin.

Regions
This report shows traffic in and out of a selected customer broken down by the external geographic region of origin.

IP Information

ICMP
This report shows the traffic flowing into and out of a given customer, broken down by pairings of ICMP types and ICMP codes.

Packet Size
This report shows traffic flowing into and out of a customer, sorted by packet size.

Protocols
This report shows traffic flowing into and out of a given customer, broken down by IP protocol.

TCP Applications
This report displays the traffic going in and out of a selected customer for the top TCP applications observed, broken down by application port.

UDP Applications
This report displays the traffic going in and out of a selected customer for the top UDP applications observed, broken down by application port.

IPv6

IPv4 vs. IPv6 Comparison
This report provides a comparison for customer managed objects of the total IPv4 traffic versus total traffic IPv6 traffic. Tunneled IPv6 traffic is counted only in the IPv6 summary.

TCP (IPv6) Applications
This report displays the native IPv6 traffic going in and out of a selected customer for the top TCP applications observed, broken down by application port.

UDP (IPv6) Applications
This report displays the native IPv6 traffic going in and out of a selected customer for the top UDP applications observed, broken down by application port.

Network Resources

Peers
This report shows the traffic flowing into and out of a customer, broken down by each peer that you have defined.

Routers
This report shows the in, out, and total traffic by router.

Traffic Through Local Boundary Interfaces
This report shows the in, out, and total traffic for each interface.

Traffic Through Network Boundary Interfaces
This report shows the customer traffic flowing into and out of your network, broken down by network boundary interface.

Traffic with Other Customers
This report shows the in, out, and total traffic for each other customer.

Traffic with Profiles
This report shows in, out, and total traffic by network profile

Security

Baselines
This report visualizes a customer's profiled network baseline over different timeframes.

Fingerprints
This report shows in and out data for a selected customer, by fingerprint.

Services and Applications

All Applications
This report shows the traffic flowing into and out of a customer, broken down by application.

DSCP
This report tracks the amount of traffic for each type of service (TOS) seen for a selected customer as specified by the DSCP (Differentiated Services Code Point) interpretation of the TOS bits.

IP Precedence
This report tracks the amount of traffic for each type of service (TOS) precedence setting seen for the selected customer. The precedence is represented by three bits in the TCP header of a packet. The higher the integer value of these bits, the more precedence is given to that traffic.

RTP Loss
This report shows the average percentage of RTP (Real-time Transport Protocol) packet loss for a given customer, based on services configured. The shaded areas represent a single standard deviation from the mean.

Services
This report shows traffic in and out for a given customer for each service.

TCP Loss
This report shows the average percentage of TCP packet loss for a given customer, based on services configured. The shaded areas represent a single standard deviation from the mean.

Type of Service
This report report tracks the amount of traffic for each type of service (TOS) seen for a selected customer.

Type of Service (DTRM)
This report tracks the amount of traffic for each type of service (TOS) seen for a specified customer as specified by the four TOS bits (3,4,5, and 6) in the eight bit TOS field for each packet.

Toptalkers

Top Talker Destinations
This report shows a traffic graph and a table of the 100 hosts external to a given customer that are consuming the most bandwidth for that customer.

Top Talkers
This report shows a comparison graph and table of the peak traffic rate for the top 100 hosts matching a specified customer.

Transit

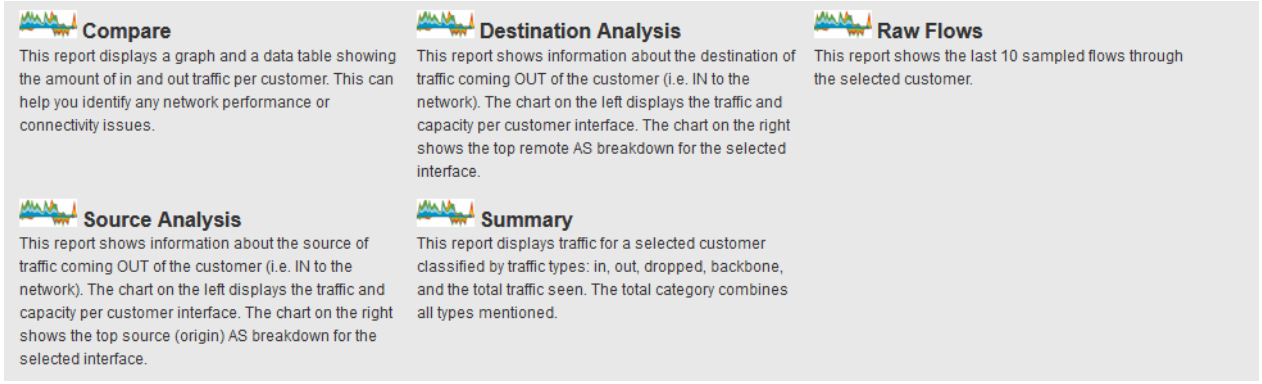
Remote AS
This report shows how much traffic passes in and out of a selected customer and transits the customer through each remote AS. A remote AS is an AS on the opposite side of the customer's network. For traffic IN to the selected customer, this corresponds to any ASes in the BGP route matching the destination of the traffic. For traffic OUT of the selected customer, it corresponds to ASes in the BGP route matching the source of the traffic.

Remote BGP Community
This report shows how much traffic passes in and out of a selected customer through each BGP community for a customer route. For traffic IN to the selected customer, this corresponds to communities for the BGP route matching the destination of the traffic (i.e. the route used to forward traffic to the customer). For traffic OUT of the selected customer, it corresponds to communities for the BGP route matching the source of the traffic.

Remote BGP Nexthop
This report shows how much transit traffic passes in and out of a selected customer through each customer-facing NextHop. For traffic IN to the selected customer, this corresponds to the NextHop for the BGP route matching the destination of the traffic (i.e. that will be be used to forward the traffic to the customer). For traffic OUT of the selected customer, it corresponds to the NextHop for the BGP route matching the source of the traffic (i.e. that the traffic passed from the customer to the monitored network over).

Remote Origin AS
This report shows how much traffic passes in and out of a selected customer and transits the customer through each remote origin AS. A remote origin AS is an origin AS on the opposite side of the customer's network. For traffic IN to the selected customer, this corresponds to the destination AS of the traffic. For traffic OUT of the selected customer, it corresponds to the source AS of the traffic.

Andere

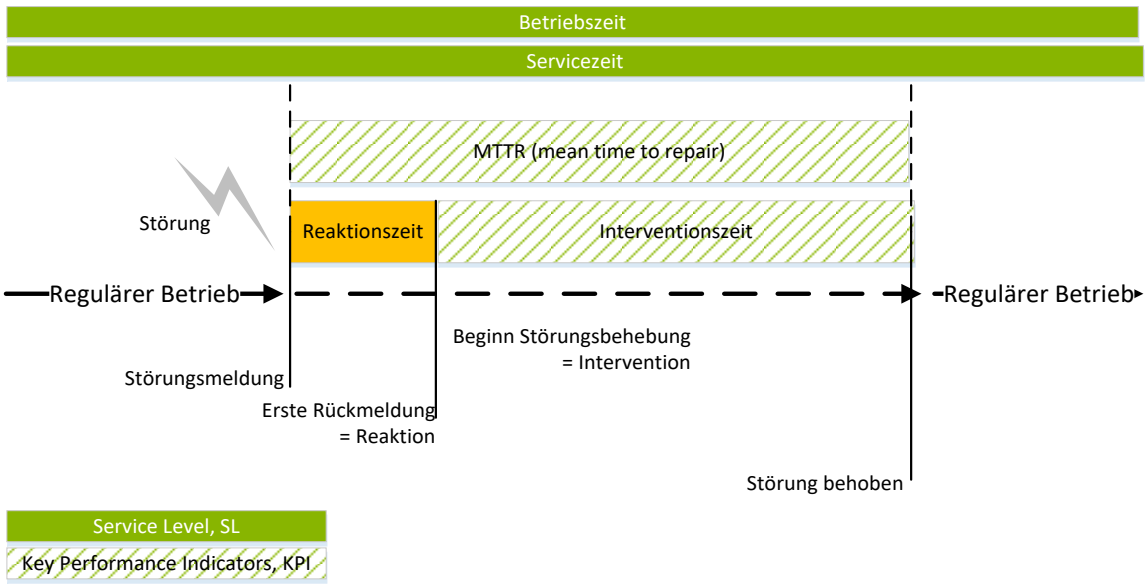

Compare
This report displays a graph and a data table showing the amount of in and out traffic per customer. This can help you identify any network performance or connectivity issues.
Destination Analysis
This report shows information about the destination of traffic coming OUT of the customer (i.e. IN to the network). The chart on the left displays the traffic and capacity per customer interface. The chart on the right shows the top remote AS breakdown for the selected interface.
Raw Flows
This report shows the last 10 sampled flows through the selected customer.
Source Analysis
This report shows information about the source of traffic coming OUT of the customer (i.e. IN to the network). The chart on the left displays the traffic and capacity per customer interface. The chart on the right shows the top source (origin) AS breakdown for the selected interface.
Summary
This report displays traffic for a selected customer classified by traffic types: in, out, dropped, backbone, and the total traffic seen. The total category combines all types mentioned.

2. Service Level Agreement

Das erfolgreiche Outsourcing von IT-Dienstleistungen erfordert eine transparente Definition der Kunden-Lieferanten-Beziehung. GDC und der Kunde werden die zu erbringenden Leistungsqualitäten (nachfolgend „Service Level“) und die vom Kunden zu erbringenden Pflichten im nachfolgenden Service Level Agreement („SLA“) regeln.

2.1 Begriffsdefinitionen

Service Level, SL	festgelegte und messbare Kriterien für die Erbringung einer bestimmten Leistungsqualität durch GDC
Key Performance Indicators, KPI	angestrebte aber nicht verpflichtende Servicemesswerte
Servicezeit	Die Servicezeit ist die Zeit, innerhalb derer die vertraglich vereinbarten Leistungen erbracht werden.
Betriebszeit	Die Betriebszeit ist die Zeit, in der das System grundsätzlich zur Verfügung steht. Die geplanten und angekündigten Wartungsfenster sind nicht Teil der Betriebszeit. Die Betriebszeit beträgt minimal 8‘604 Stunden und berechnet sich wie folgt: 1 Jahr 24/7 = 8‘760 h – 156 h Wartungsfenster. Bei redundanter Architektur werden die beiden redundanten Geräte/Einrichtungen zu unterschiedlichen Zeitpunkten gewartet.
Verfügbarkeit	Verfügbarkeit [%] = 100 * ((Betriebszeit - ungeplante Ausfälle innerhalb der Betriebszeit) / vereinbarte Betriebszeit). Die vereinbarte Betriebszeit enthält nicht die Zeitfenster für geplante Wartungsfenster).
Reaktionszeit	Die Reaktionszeit bestimmt die maximal in Anspruch genommene Zeit zwischen dem Auftreten oder Meldung einer Störung und dem Beginn der Fehleranalyse. GDC ist bestrebt, die angegebenen Reaktionszeiten einzuhalten und Ausfälle sowie Fehler rasch zu beheben. Die Einhaltung der Reaktionszeit kann jedoch nicht in jedem Fall sichergestellt werden. Fristüberschreitungen führen zu keiner Vertragsstrafe und keinen Schadenersatzansprüchen
Mean Time To Repair, MTTR	mittlere Zeit zur Durchführung einer Reparatur bzw. der Wiederherstellung des Betriebs.
Wartungsfenster	Für die Zwecke dieses SLA sind “geplante Wartungen” nötig, um die Services zu erbringen oder die Infrastruktur zu aktualisieren. Geplante Wartungsfenster werden im Voraus festgelegt und auf status.green.ch entsprechend angekündigt. Kunden werden zudem mindestens 48 Stunden vor dem geplanten Serviceunterbruch infolge Wartungsarbeiten informiert. GDC informiert die vom Kunden schriftlich mitgeteilte technische Kontaktstelle per E-Mail über die geplante Serviceunterbrechung und die Art dieses Unterbruchs. Falls eine Wartung erforderlich ist, wird GDC versuchen, diese in einem unserer regelmässigen Wartungsfenster durchzuführen. Diese sind Samstag und Sonntag sowie Dienstag von 05.30 bis 06.30 Uhr. Beim Auftreten von ungeplanten Vor- oder Störfällen hat GDC das Recht, jederzeit und ohne Vorankündigung Notfallwartungen unmittelbar auszuführen. In diesem Falle werden die Wartungsarbeiten auf der Website http://status.green.ch entsprechend veröffentlicht.
Single Point Of Contact, SPOC	Der Single Point of Contact (SPOC) ist die zentrale Anlaufstelle für Kunden und wird durch das Customer Care Center (Support-Hotline 044 330 3535) sichergestellt.



Genereller Ablauf Störungen

2.2 Kundensupport

Die hochqualifizierten, mehrsprachigen Support-Mitarbeitenden der GDC stehen dem Kunden zur Verfügung, um Support-Anfragen und administrative Anfragen über Telefon oder über das Online Ticket-System unter https://contact.green.ch/entgegenzunehmen.
Der Kundensupport steht 365 x 24 telefonisch zur Verfügung– das Business Support Team ist der erste Ansprechpartner für alle Fragen ausser für Fragen zum Vertrieb. Probleme, die nicht mit dem Support Team gelöst werden können, werden zu den zuständigen technischen oder kaufmännischen Mitarbeitenden von GDC weitergeleitet.

2.2.1 Standardmechanismen

Support erfolgt für alle unsere Dienstleistungen über Standardmechanismen:

Online-Support: via Ticket-System https://contact.green.ch/
Live Chat: https://www.green.ch
Die Green Website: https://www.green.ch/support

Als Kunde von GDC erhalten Sie telefonische Unterstützung unter +41 44 330 3535

2.2.2 Pflichten des Supports

- Berechtigungsprüfung des Anfragestellers und des Service Levels
- Den Störfallmanagementprozess und den Fehlerbehebungsprozess starten, was Folgendes umfasst:
    - Erhalt der Anfrage, Eröffnung eines Trouble-Tickets und Bestätigung
    - Priorisierung, Koordination und Überwachung des Fehlerbehebungsprozess mit internen und externen Mitteln
    - Information an den Kunden über die ergriffenen Massnahmen, Zwischenlösungen und die Lösung
    - Information an den Kunden über die Wiederherstellung der Serververfügbarkeit

- Analyse der Grundursache und Empfehlungen für das weitere Vorgehen (Änderungsverwaltung)

2.2.3 Pflichten des Kunden

Um unseren hohen Service zu gewährleisten fordert GDC die Einhaltung der folgenden Richtlinien:

- Der Kunde liefert alle erforderlichen Kontaktangaben, einschliesslich Kontakte für die Eskalation aller erbrachten Dienstleistungen, und stellt sicher, dass sie im Falle von Änderungen rechtzeitig aktualisiert werden.
- Der Kunde stellt sicher, dass die Informationen zu Änderungen an der Konfiguration, an Schnittstellen, Kanälen, Applikationen und Systemen, die für die Erbringung von Joint Services relevant sind, an GDC geliefert und jederzeit auf dem neuesten Stand gehalten werden.
- Der Kunde ist für die Instandhaltung aller Kundenapplikationen verantwortlich. GDC ist nicht für die Wartung der Kundenapplikationen oder Kundendaten verantwortlich.
- Es darf nur Equipment installiert werden, welches in einwandfreiem Zustand ist und keine Gefahr für Personen und Objekte darstellt.
- Der Kunde darf nicht über einen Schreibzugriff auf Managed Geräte von GDC verfügen. Allerdings ist SNMP-Lesezugriff optional erhältlich.

2.3 Allgemeine Massnahmen zur Sicherheit des laufenden Betriebs

GDC erbringt in seinen Datencentern ausschliesslich Dienstleistungen höchster Qualität und Sicherheit. Die Sicherheit der Kundendaten und die Verfügbarkeit der Dienstleistungen werden unter anderem durch folgende Massnahmen sichergestellt:

2.3.1 Physische Sicherheit durch bauliche, betriebliche und technische Massnahmen:

- Zugangskontrollsysteme
- Videoüberwachung vor und im Gebäude
- Rauch-, Staub- und Wassermelder
- Brandbekämpfungsanlage
- Klimatisierung über zwei getrennte Kühlkreisläufe
- redundante Stromzuführung durch Energieversorger
- Ringförmige Anbindung an das öffentliche Starkstromnetz
- Durch USV gefilterte Stromversorgung
- Leistungsstarke Notstrom-Dieselgeneratoren
- Doppelte Ausführung der Versorgungsleitungen im Gebäude

2.3.2 Sicherheit und Verfügbarkeit der internen Netzwerkinfrastruktur:

- Segmentierung der Netzwerke und strikte Trennung der unterschiedlichen Datenströme
- Tägliches Backup der eigenen Systeme
- Einsatz von Firewalls an relevanten Netzwerkpunkten
- Netzwerküberwachung durch hauseigenes NOC („Network Operation Center“)
- Ausschliessliche Verwendung von Markenkomponenten

2.3.3 Verfügbarkeit der externen Netzwerkanbindung:

- Carrier-neutrale und redundante IP-Anbindung des Datencenters

2.3.4 Vertragsgegenstand, Geltungsbereich

Dieses SLA gilt nur für das mit dem SLA versendeten Angebot und dem hieraus geschlossenen Leistungsvertrag. Sonstige Verträge zwischen GDC und dem Kunden bleiben hiervon unberührt. Das SLA ist nur auf die Connectivity Lösungen und seine Optionen, nicht aber auf andere Produktbereiche übertragbar. Im Falle widersprüchlicher Regelungen haben die Vereinbarungen im entsprechenden Leistungsvertrag Vorrang vor den Bestimmungen des SLAs. Daneben gelten die jeweils gültigen Allgemeinen Geschäftsbedingungen von GDC.

3. Service Level

Das SLA ermöglicht dem Kunden eine definierte Qualität und berechtigt bei seitens GDC nicht erbrachten Leistungen der garantierten Service Level zur Rückerstattung ihrer monatlichen Gebühren oder eines Teils hiervon (nachfolgend «Service Gutschrift bei Nicht Verfügbarkeit» genannt).

Leistung	Wert oder Bemerkung
Garantiertes Service Level	
Verfügbarkeit DDoS Guard Service	99.9 %
Service-Management 24x7 durch Network Operation Center von GDC	Nur bei DDos Guard – wird separat verrechnet
Key Performance Indicator, KPI	
Reaktionszeit Time-To-Customer-Notification	Telefonische Benachrichtigung: 30 Minuten SMS / Email Benachrichtigung: 3 Minuten → keine Benachrichtigung bei DDoS Guard basic
DDoS Erkennung Time-To-Detection	Sofort
Umleitung zu Scrubbing Center Time-To-Diversion-Initiation	1 Minute
Übliche Justierung des Filters Typical Time-to-Mitigation	UDP / ICMP floods – 5 min SYN Floods – 5 min TCP Flag Abuses – 5 min DNS Reflection – 10 min DNS Flood Attack – 10 min
Nachträgliche Beobachtung Cooling Down	48 Stunden
Koordination Rückführung Normalbetrieb Coordination Diversion Rollback	Nach Absprache mit Kunden Jedoch spätestens nach 48 Stunden → Keine Koordination der Rückführung bei DDoS Guard basic
Rückführung in Normalbetrieb Diversion-Rollback	Nachts oder ausserhalb der Bürozeiten Rückführung provoziert einen Unterbruch von bis zu 3 Minuten
Monitoring der Datenpakete Flow Control	Bis ISO Layer 4

Rahmenbedingungen	
Betriebszeit	365 x24 (abzüglich geplanter und angekündigter Wartungs-fenster)
Servicezeit	365 x 24 bei DDoS Guard , Mo bis Fr 06:00 bis 22:00 bei DDoS Guard basic
Bürozeiten	Mo–Fr 08.00–17.30 Uhr
Rückruf	Inklusive
Prioritätsbearbeitung	Inklusive
Störungsmeldung	Per Telefon oder Kontaktformular unter https://contact.green.ch/, ausserhalb der Bürozeiten ausschliesslich per Telefon auf +41 44 330 3535

3.1 Verfügbarkeit

GDC ermöglicht die im Folgenden jeweils genannten Verfügbarkeiten der in der Offerte erwähnten Services. Der Ausfall eines Teils eines redundanten Systems wird nicht als Ausfallzeit betrachtet. Kann GDC die vorerwähnte Verfügbarkeit nicht einhalten, so erkennt der Kunde an und stimmt zu, dass die in den SLA vereinbarten Gutschriften die einzige und ausschliessliche Entschädigung für den Kunden darstellen.

Zur Messung des Service Levels wird die Verfügbarkeit durch eigene Monitoring-Systeme überwacht. GDC überprüft die Verfügbarkeit des DDoS Services mithilfe unterschiedlicher technischer Verfahren. Alternativ kann eine Störung durch den Kunden gemeldet werden, indem er ein Service-Ticket eröffnet.

3.1.1 Berechnung der Verfügbarkeit

Verfügbarkeit=(Betriebszeit-Ausfallzeit)/Betriebszeit*100
GDC bietet Gutschriften, sobald die Serviceverfügbarkeit unterhalb der garantierten Schwellwerte liegt. Die Tabellen in diesem Dokument zeigen die Gutschriften als Prozentsatz der Basis der monatlich wiederkehrenden Gebühren (MRC). Diese Gutschriften und Entschädigungen verstehen sich als abschliessend. Weitere oder andere Entschädigungen sind ausgeschlossen. Keine Gutschrift oder Zahlung erfolgt aus anderen Gründen oder in anderem Umfang als in dem hier angegebenen, einschliesslich – aber nicht beschränkt darauf – Geschäftsverluste auf Seiten des Kunden aufgrund von Ausfallzeiten.

3.2 Finanzielle Rückerstattung

Sofern GDC seine vertraglichen Verpflichtungen nicht nachkommen kann, gewährt GDC dem Kunden für jede registrierte Ausfallstunde eine Gutschrift von 5 % bis zu einem Maximum von 50% der monatlichen Gebühren für die betroffenen Leistungsteile. Weitergehende Schadenersatzansprüche werden explizit wegbedungen. Der Kunde hat seine Ansprüche bei GDC mittels einer Anfrage unter https://contact.green.ch/ geltend zu machen.

Keine SLA-Gutschrift wird gewährt, wenn ein Service für einen bestimmten Zeitraum nicht verfügbar ist, sofern dies insgesamt oder zum Teil durch eine der folgenden Ursachen bedingt ist:

- ein Ausfall von Ausstattung in den Räumlichkeiten des Kunden (falls diese nicht im Besitz von GDC), des Kundenstandortes (etwa durch Stromausfall) oder von Ausstattung eines Lieferanten des Kunden;
- Naturkatastrophen, Terrorangriffe oder andere Force Majeure-Ereignisse;

- ein Ausfall aufgrund von magnetischen / elektromagnetischen Interferenzen oder elektrischen Feldern;
- jede fahrlässige Handlung oder Unterlassung des Kunden (oder von Mitarbeitenden, Vertretern oder Subunternehmern des Kunden), u.a.:
  - Verzögerungen bei der Lieferung notwendiger Ausstattung durch den Kunden;
  - Versäumnis, GDC zwecks Tests ausreichend Zugang zu den Einrichtungen zu gewähren;
  - Versäumnis, den Zugang zu den Räumlichkeiten des Kunden zu gewähren um es GDC zu ermöglichen, ihren Verpflichtungen hinsichtlich des Services nachzukommen;
  - Versäumnis, entsprechende Gegenmassnahmen hinsichtlich des fehlerhaften Services zu ergreifen, wie von GDC empfohlen, oder Hinderung der Anbieterin, diese selbst durchzuführen; oder
  - Versäumnis, Redundanzen zu nutzen, wie sie vom Service Level geboten werden.
  - Fahrlässigkeit des Kunden oder absichtliches Fehlverhalten, darunter auch das Versäumnis des Kunden, vereinbarte Verfahren zu befolgen;
- wenn der Kunde den Zugang zum Cage verhindert oder verzögert;
- alle geplanten Wartungszeiträume, wenn der Kunde darüber informiert wurde, und Notfallwartungen, die dazu dienen, künftige Ausfallzeiten zu verhindern; oder
- Abschaltung oder Aussetzung des Services durch GDC, nachdem der Kunde nicht innerhalb von 90 Tagen ab Rechnungsstellungsdatum bezahlt hat, oder wegen anderer hinreichender Gründe.

Schliesslich darf die Kundenausstattung nicht mehr Strom verbrauchen, als die Stromleitungen an jedem Punkt gemäss Servicebeschreibung liefern können. Da Geräte in der Bootphase mehr Strom benötigen, empfiehlt die Anbieterin eine automatische Einschaltverzögerung, um eine Überlastung während des Wiederhochfahrens nach einem Stromausfall zu verhindern. Eine solche Überlastung würde als Designfehler seitens des Kunden betrachtet werden und wäre daher nicht durch dieses SLA abgedeckt.

3.2.1 Demarkationspunkte

Dieses SLA bezieht sich auf DDoS Guard Service von GDC. Alle hier gegebenen Zusicherungen bezüglich Performance oder Betriebsbereitschaft gelten nur für die von GDC verwaltete Ausstattung zwischen der vom Kunden verwalteten Ausstattung und den eigenen Providern von GDC. Zu diesen Providern zählen u.a. der Stromversorger, die Vermieter, sowie andere Telekommunikationsunternehmen. Falls der Kunde seine eigene Ausstattung verwaltet, endet der Verantwortungsbereich von GDC an den Patch-Panels vom Patch-Raum kommend oder am Endpunkt des Carrierservice (Übergabepunkt im Haus).

3.2.2 Messung und Definition der Ausfallzeit

Ausfallzeit (bzw. nicht-Verfügbarkeit des Services) wird nur insofern berücksichtigt wie sie von GDC zu verantworten ist.
Ausfallzeit ist wie folgt definiert: Sie beginnt zu dem Zeitpunkt, an dem der Kunde die Supportanfrage eröffnet oder GDC selber einen Fehler feststellt und endet, wenn ein Mitarbeiter der Anbieterin die Lösung des Problems anzeigt. Es gilt keine andere Messung der Ausfallzeit, und alle Zeiten, die für diese Berechnung verwendet werden, sind die von GDC aufgezeichneten. Betriebsdauerberechnungen werden unabhängig für jeden Service durchgeführt, wobei der schlechteste Wert (die längste Ausfallzeit) verwendet wird, um die Gutschrift für den Kunden zu berechnen.

4. Pflichten des Kunden

4.1 Warnmeldungen

Es obliegt dem Kunden, für alle offenen Probleme Support-Anfragen zu eröffnen. Das Erzeugen einer automatischen Warnmeldung durch GDC beinhaltet keine Bestätigung eines Problems. Nur ein korrekt eröffnetes Ticket kann für die Berechnung von Ausfallzeiten und Gutschriften herangezogen werden.

4.2 Kundenbeteiligung nach einem Stromausfall

Nach einem Stromausfall obliegt es dem Kunden, alle notwendigen Schritte zu unternehmen, um seine Ausstattung wieder online zu bringen.

4.3 Kündigung von Services

Bei Kündigung eines Services muss der Kunde innerhalb von 30 Tagen nach Vertragsende sämtliche Ausstattung die von GDC zu Erbringung des Services zur Verfügung gestellt wurde, unaufgefordert und in ordnungsgemässem Zustand an GDC zurückgeben. Der Kunde ist verantwortlich für alle Gebühren und Kosten, die im Zusammenhang mit dieser Rückübertragung verbunden sind. Der Kunde kann auch einen Techniker der Anbieterin kostenpflichtig beauftragen, die Ausstattung abzuholen, per Post zu verschicken oder sich ggfs. für eine andere Option entscheiden.

- In den folgenden Fällen ist der Kunde schadenersatzpflichtig für die Kosten von Ersatzhardware:
  - Falls die Ausstattung verloren gegangen ist oder nicht innerhalb von 30 Kalendertagen nach Vertragsende zurückgegeben wird.
  - Falls die Ausstattung in solch einem Zustand ist, dass die Anbieterin die Hardware nicht mehr für andere Klienten verwenden kann; eine zeitbedingte Abnutzung bleibt vorbehalten.

5. Service Management

5.1 Störfallmanagement

5.1.1 Ausfallmeldung

GDC informiert den technischen Ansprechpartner des Kunden entweder per Telefon oder E-Mail (bei einer schriftlichen Meldung an die Kontaktdaten, die an GDC mitgeteilt wurden).

5.1.2 Ablauf Störfall

Die Philosophie von GDC ist, dem Kunden eine technisch und betrieblich bestmögliche Verfügbarkeit und Servicequalität zu erbringen. Bei Störungen ist unser Hauptziel die schnelle Bearbeitung und Wiederherstellung der Service-Verfügbarkeit. Der Vorteil für den Kunden ist die Begrenzung des Einflusses auf seine Geschäftstätigkeit.
Störfälle und Ausfälle bezüglich “reaktiv” gesteuerten Services müssen vom Kunden gemeldet werden. Nach der Meldung des Ausfalls wird ein Trouble Ticket eröffnet und analysiert. Der Service wird anhand des vereinbarten Service Level wiederhergestellt.

Störfälle und Ausfälle auf “proaktiv” gesteuerten Services werden vom Überwachungssystem gemeldet. Der Kunde wird nach Massgabe des vereinbarten Service Level informiert. Wenn sich der Ausfall auf die Geschäftstätigkeit des Kunden auswirkt, hat der Kunde über die entsprechenden Kanäle ein Trouble Ticket zu eröffnen.

5.1.3 Pflichten des Supports

- Die Berechtigung der Person, welche die Anfrage einreicht, feststellen und prüfen und mit dem Service Level Agreement zwischen dem Kunden und der Anbieterin vergleichen.
- Den Störfallmanagement-Prozess zu starten, was folgendes umfasst:
    - Erhalt der Anfrage, Eröffnung eines Trouble Tickets und Bestätigung.
    - Den Fehlerbehebungsprozess mit internen und externen Mitteln priorisieren, koordinieren und überwachen.
    - Den Kunden über die ergriffenen Massnahmen, Zwischenlösungen und die Lösung informieren.
    - Den Kunden über die Wiederherstellung der Serververfügbarkeit informieren.
    - Analyse der Grundursache und Empfehlungen für das weitere Vorgehen (Änderungsverwaltung).

Im Fall von unerwarteten Verzögerungen bei der Fehlerbehebung, die zu einer Verletzung des SLA führen, wird automatisch eine interne Eskalation gestartet. Je nach Art des Problems sind entweder interne Senior-Mitarbeitende oder der Vertriebs-/Subunternehmer-Support die erste Eskalations-Ebene. Zu diesem Zeitpunkt wird der diensthabende Manager involviert, um sicherzustellen, dass das SLA während des Eskalationsprozesses eingehalten und das Problem rechtzeitig gelöst wird.

5.2 Änderungsverfahren

Änderungen der Kunden-Vereinbarung werden schriftlich vereinbart, soweit nichts Abweichendes vereinbart ist. Änderungen, die nicht in Schriftform vorliegen, sind ungültig. Die im Zusammenhang mit dem Vertragsmanagement entstehenden Kosten werden mangels besonderer Abrede von jeder Vertragspartei selbst getragen.
Die Vertragsparteien prüfen Änderungsangebote und teilen der ersuchenden Partei ihre Zustimmung oder eventuelle Änderungswünsche in der Regel innerhalb von zwei weiteren Wochen nach Vorlage des Änderungsangebots schriftlich mit. Die ersuchte Partei stimmt in der Regel innerhalb von weiteren zwei Wochen nach Vorlage des überarbeiteten Änderungsangebots diesem oder dem alternativen Änderungsangebot zu oder lehnt dieses ab.
Lehnt eine Partei die Abgabe eines Änderungsangebotes begründet ab oder nimmt die andere Partei das Änderungsangebot nicht oder nicht innerhalb der Bindefrist an, so bleiben die vereinbarten Leistungsumfänge und Konditionen unverändert bestehen.

5.3 Einsatz von Subunternehmern

GDC erbringt die vertraglichen Leistungen grundsätzlich mit eigenen Mitarbeitenden und Mitteln. Sie ist aber bei der Erbringung der vertraglichen Leistungen zum Einsatz von Dritten und/oder Mitarbeitenden dritter Unternehmen (nachfolgend "Subunternehmer") berechtigt.

Es kommen dabei nur von GDC akkreditierte Unternehmen und deren ausgebildete Fachleute zum Einsatz. Die Subunternehmer erfüllen hinsichtlich Verlässlichkeit dieselben Anforderungen wie die Anbieterin selbst.

Darüber hinaus gilt für den Einsatz von Subunternehmern was folgt:

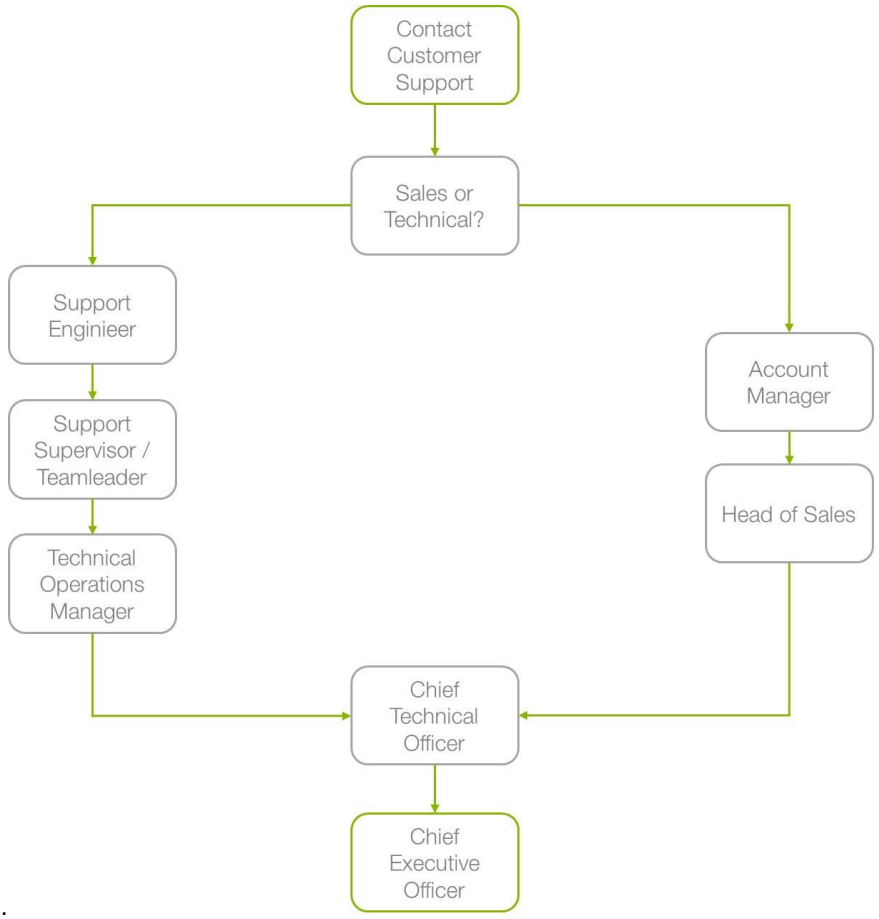
- GDC bleibt ausschliessliche Ansprechpartnerin des Kunden im Hinblick auf alle Leistungen, die der Subunternehmer erbringt.
- GDC ist verpflichtet, dafür zu sorgen, dass der Subunternehmer sich an die vertraglichen Verpflichtungen hält, die den Kunden betreffen.
- GDC bleibt für die Auswahl, Überwachung und Instruktion des Subunternehmers verantwortlich und ist durch den Einsatz des Subunternehmers nicht von der eigenen Leistungspflicht entbunden. Ansprüche aus leichter Fahrlässigkeit sind hingegen ausgeschlossen.
- GDC hat mit jedem Subunternehmer einen schriftlichen Vertrag abzuschliessen, in dem die Pflichten des Subunternehmers festgelegt sind.

Die Leistungen des Subunternehmers werden im Namen und Auftrag sowie als Leistungen von GDC erbracht.

Der Einsatz von Subunternehmern bei der Erhebung, Verarbeitung und Nutzung von unternehmens- und personenbezogenen Daten unterliegt darüber hinaus den datenschutzrechtlichen Bestimmungen gemäss den allgemeinen Geschäftsbedingungen, AGB von GDC. Die Weitergabe von unternehmens- und personenbezogenen Daten ist unabhängig von obigen Voraussetzungen zur Einschaltung von Subunternehmern erst zulässig, wenn der Subunternehmer die datenschutzrechtliche Vereinbarung gemäss AGB akzeptiert hat. Allgemein gilt, dass personenbezogene Daten auf Kundenseite von der Anbieterin und ihren Subunternehmern nur dann in Länder ausserhalb der Schweiz gebracht werden dürfen, wenn der Kunde schriftlich zugestimmt hat und die datenschutzrechtlichen Voraussetzungen hierzu geschaffen sind.

5.4 Vom Kunden in Gang gesetzte Eskalation

Befürchtet der Kunde, dass entweder die Geschwindigkeit oder die Qualität des Supports / des Fehlerbehebungsprozesses sein Geschäft ernsthaft gefährden könnte, hat der Kunde die Möglichkeit selbständig eine Eskalation auszulösen.



5.5 Pflichten des Kunden

- Der Kunde liefert alle erforderlichen Kontaktangaben, einschliesslich Kontakte für die Eskalation für alle erbrachten Dienstleistungen, und stellt sicher, dass sie im Falle von Änderungen laufend aktualisiert werden.
- Der Kunde liefert und aktualisiert für GDC eine Liste aller Personen, die einen Anspruch auf einen Zugang zum Support haben.
- Der Kunde implementiert und aktualisiert geeignete Mittel für die Identifizierung dieser berechtigten Personen.
- Der Kunde stellt sicher, dass die Informationen zu Änderungen an der Konfiguration, an Schnittstellen, Kanälen, Applikationen und Systemen, die für die Erbringung von Joint-Services relevant sind, der Anbieterin geliefert und jederzeit aktuell sind.
- Der Kunde ist für die ständige Instandhaltung aller Kundenapplikationen verantwortlich. Die Wartung der Kundenapplikationen oder Kundendaten obliegt ausschliesslich in der Verantwortung des Kunden.
- Es darf nur Equipment installiert werden, welches in einwandfreiem Zustand ist und keine Gefahr für Personen und Sachen darstellt.
- Der Kunde hat sicherzustellen, dass GDC jederzeit und aus jedem Grund auf die von GDC verwaltete Gerätschaft Zugang hat. Falls dies nicht sichergestellt wird, bedeutet dies eine Verletzung der Vereinbarung und kann zu einer Vertragsauflösung führen.
- Der Kunden hat keine Schreibrechte auf die von GDC verwalteten Geräte. Es ist jedoch ein SNMP Leserecht optional erhältlich.

- Bei der Zusammenarbeit mit GDC Mitarbeitern müssen alle Aktivitäten im Voraus koordiniert werden. Dies beinhaltet den Zusatz von Serviceoptionen wie zum Beispiel zusätzliche Konten oder Netzwerkänderungen.
- Jeder nicht autorisierte Versuch eines Kunden, auf die Gerätschaft von GDC zuzugreifen ist strikt verboten, sei dies in physischer Art oder in elektronischer. Dies beinhaltet auch CPE (Customer Premise Equipment).

5.6 Versicherung

GDC Systeme sind gegen entsprechende Risiken versichert. Jedoch werden weder Kundendaten noch die Verfügbarkeit der Services, geliefert vom Kunden zum eigenen Kundenstamm, in irgendeiner Weise versichert. Es ist die ausdrückliche Verantwortung des Kunden, Versicherungsschutz zu erhalten. Für Verluste von Geschäftsinformationen oder andere Auswirkungen von Systemausfällen wird kein Schadenersatz gewährt, der über die in diesem Dokument explizit beschriebenen Gutschrift-Prozentsätze hinausgeht.

6. Rechtliche Bestimmungen

6.1 Zustandekommen des Rechtsverhältnisses

Mit dem Abschluss der Bestellung auf der Website kommt zwischen GDC und dem Kunden ein Rechtsverhältnis zustande. Die Messung der SLA-Parameter erfolgt ab Vertragsstartdatum.

6.2 Einhaltung der örtlichen Gesetze

Der Kunde stellt sicher, dass kein illegaler Datenverkehr über GDC Verbindungen gesendet wird. GDC übernimmt dafür keine Haftung.

6.3 Beschränkungen

Alle Entschädigungen für GDC Services sind auf den in diesem Dokument angegebenen Umfang begrenzt. Keine Gutschrift oder Zahlung erfolgt aus anderen Gründen oder in anderem Umfang als in dem hier angegebenen, einschliesslich – aber nicht beschränkt darauf – Geschäftsverluste seitens des Kunden aufgrund von Ausfallzeiten.

6.4 Verwendung von persönlichen Daten

Kunden akzeptieren ausdrücklich die von GDC erlassenen Richtlinien zur Verwendung persönlicher Daten.
Siehe dazu: https://www.green.ch/de/rechtliches/datenschutz

6.5 Änderungen

GDC behält sich das Recht vor, dieses Dokument zuweilen abzuändern, sofern der Kunde entsprechend schriftlich informiert wird, bevor die Änderungen in Kraft treten. Wenn die Änderungen eine wesentliche Auswirkung auf die Services, die Servicegebühr oder auf andere Pflichten aus diesem Vertrag haben, kann der Kunde diesen Vertrag jederzeit unter Einhaltung der monatlichen Kündigungsfrist schriftlich auflösen.

6.6 AGB

Die allgemeinen Geschäftsbedingungen der Anbieterin (Allgemeine Geschäftsbedingungen GDC AG) sind integraler Bestandteil der Kunden-Vereinbarung. Allgemeine Geschäftsbedingungen des Kunden finden keine Anwendung. Anderslautende Regelungen in den Unterlagen des Kunden sind nicht anwendbar. Kündigungen, Änderungen und Ergänzungen der Service-Vereinbarung und der Leistungsverträge bedürfen der Schriftform. Auf die Schriftform kann nur schriftlich verzichtet werden.
Sollten einzelne Regelungen dieser Service-Vereinbarung oder der Leistungsverträge oder anderer Anhänge zur Kunden-Vereinbarung sich als rechtsunwirksam oder nicht durchführbar erweisen, so tritt an die Stelle der unwirksamen oder undurchführbaren Regelung eine wirksame oder durchführbare, die dem bei Vereinbarung der jeweiligen Regelung vorhandenen Willen der Vertragsparteien am nächsten kommt sowie den in der Präambel dieser Service-Vereinbarung aufgeführten gemeinsamen Zielen entspricht. Die neugewählte Regelung darf keine Beeinträchtigung des Verhältnisses zwischen der Leistung der Anbieterin und des Kunden zur Folge haben.
Siehe dazu: https://www.green.ch/de/rechtliches/agb

7. Glossar

Abkürzung		Begriffserklärung
/24	/24 Netzmaske	Ein IPv4 /24 Netzwerk besteht aus maximal 254 nutzbaren IPv4 Adressen. Vor allem im privaten Bereich sind die LAN Netzwerke mit einer /24 Netzmaske weit verbreitet. Die Netzmaske kann man auch als Größenangabe eines IP-Netzes verstehen.
/28	/28 Netzmaske	Ein IPv4 /28 Netzwerk besteht aus maximal 14 nutzbaren IPv4 Adressen.
BGP	Border Gateway Protocol	Das BGP ist das im Internet eingesetzte Routing-protokoll und verbindet autonome Systeme (AS) miteinander. Diese autonomen Systeme werden in der Regel von Internetdienstanbietern gebildet.
Bot / Botnet	Botnetz	Ein Botnet oder Botnetz ist eine Gruppe automatisierter Schadprogramme, sogenannter Bots. Die Bots (von englisch: robot „Roboter“) laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen, ohne Einverständnis des Eigentümers, zur Verfügung stehen.
cooling down	Abkühlungsphase	Nach jeder Mitigation einer DDoS Attacke verbleibt der Datenverkehr über einen definierten Zeitraum im Scrubbing Center. Da der Datenverkehr bereits umgeleitet ist, haben kurz aufeinanderfolgende Attacken keinen weiteren Impact mehr für die Kundeninfrastruktur.
Coordination Diversion Rollback	Koordinierung der Übergabe in Normalbetrieb	Nach dem Cooling Down muss der Datenverkehr wieder den Normalbetrieb übergeben werden. Da diese Übergabe einen kurzen Unterbruch von bis zu 3 Minuten auf dem Netzwerk verursacht, wird diese Umstellung im Vorfeld mit dem Kunden koordiniert.
CPE	Customer Premises Equipment	Hardware im Besitz von GDC, dass in einer Kundenlokation aufgestellt wird.
DNS	Domain Name System	Verzeichnisdienst in IP-basierten Netzen; seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung.
DNS Attack	DNS Amplification Attack	Die DNS Amplification Attack (deutsch: DNS-Verstärkungsangriff) ist ein Denial-of-Service-Angriff, bei dem unter Missbrauch des Domain Name Systems extrem große Datenströme auf den Internetanschluss des Opfers gelenkt werden.
Diversion-Initiation	Einleitung der Umleitung	Sobald die Flow Control eine DDoS Attacke erkennt, wird die Umleitung zum Scrubbing Center eingeleitet. Das Scrubbing Center erhält die Informationen über die zu reinigenden Netzwerk Adressen und zieht diese über das BGP Protokoll an.
Diversion-Rollback	Rückbau der Umleitung	Ist eine DDoS Attacke zu Ende und im cooling down Betrieb sind keine weiteren Attacken mehr fest zu stellen, wird der Datenverkehr wieder in den Normalbetrieb zurück geleitet.
Flood	Flood (Flut) Attacke	Angriffstechnik bei der das Ziel/Opfer mit willkürlichen Protokoll-Anfragen (DNS,UDP etc.) überflutet wird und somit auf reguläre Anfragen nicht mehr antworten kann.

Gbit	Gigabit	Datenübertragungsrate. Bezeichnet die digitale Datenmenge, die innerhalb einer Zeiteinheit über einen Übertragungskanal übertragen wird.
GB, MB, TB	Giga Byte, Mega Byte, Terra Byte	Grössenangabe für Speicherplatz oder Arbeitsspeicher
IAAS	Infrastructure as a Service	Bereitstellung von virtualisierter IT-Infrastruktur über öffentliche oder private Netzwerke, meist über das Internet. Beim IaaS nutzt ein Kunde Server, Storage, Netzwerk und die übrige Rechenzentrumsinfrastruktur als abstrakten, virtualisierten Dienst über das Internet.
ICMP	Internet Control Message Protocol	Dient in Rechnernetzwerken dem Austausch von Informations- und Fehlermeldungen über das Internet-Protokoll in der Version 4 (IPv4). Für IPv6 existiert ein ähnliches Protokoll mit dem Namen ICMPv6.
IP-Adresse	Internetprotokoll- Adresse	Adresse in Computernetzen, die – wie das Internet – auf dem Internetprotokoll basiert. Sie wird Geräten zugewiesen, die an das Netz angebunden sind, und macht die Geräte so adressierbar und damit erreichbar.
IPv4	IP Protokoll Version 4	IPv4 war die erste Version des Internet Protokolls, welche weltweit verbreitet und eingesetzt wurde, und bildet eine wichtige technische Grundlage des Internets. Es wurde in RFC 791 im Jahr 1981 definiert.
IPv6	IP Protokoll Version 6	Das Internet Protocol Version 6 (IPv6), früher auch Internet Protocol next Generation (IPng) genannt, ist ein von der Internet Engineering Task Force (IETF) seit 1998 standardisiertes Verfahren zur Übertragung von Daten in paketvermittelnden Rechnernetzen, insbesondere dem Internet.
KPI	Key Performance Indicator	Angestrebte und üblicherweise erfüllte, aber nicht garantierte Service Parameter
LAN	Local Area Network	Aus mindestens zwei Rechnern bestehendes Rechennetz, das sich über einen begrenzten Raum erstreckt
Mitigation	Entschärfung/Schadensminderung	Bei DDoS wird mit Mitigation die Filterung der Datenpakete beschrieben. Nach der Mitigation wird der saubere Datenverkehr dem Kunden übergeben.
MIPS	Managed IP Service	Dienstleistung, mit welcher Sie von GDC mit fixen IP-Adressen an das Internet angebunden werden
MRC	Monthly Reccuring Charge	Monatlich wiederkehrende Gebühr
NAT	Network Address Translation	Sammelbegriff in Rechnernetzen für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden. Daher kommen sie typischerweise auf Routern zum Einsatz.
OTC	One Time Charge	Einmalgebühr
PA Network	Provider Assigned Network	Der Kunde erhält von seinem Provider ein Netzwerk zur Verfügung gestellt. Die IP Adressen werden dem Kunden verliehen. Der Besitzer der IP Adressen bzw. des Netzwerks ist nach wie vor der Provider.
PI Network	Provider independent Network	PI-Adressräume sind Blöcke von Internet-Protokoll-Adressen (IP Adressen), die von einer Regional Internet Registry (RIR) direkt an einen Endnutzer vergeben werden, ohne noch von einem Internetdienstanbieter für die Adressvergabe

		abhängig zu sein. PI Netzwerke haben eine Präfixlänge von 24 oder grösser.
RAM	Random Access Memory	Informationsspeicher, der besonders bei Computern als Arbeitsspeicher Verwendung findet, meist in Form von Speichermodulen
Scrubbing Center	Datenwaschstrasse	Wird eine DDoS Attacke erkannt, wird der Datenverkehr über ein Scrubbing Center Umgeleitet, welches die bösartigen Datenpakete entfernt.
SLA	Service Level Agreement	Vereinbarung bzw. die Schnittstelle zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen
SL	Service Level	Garantierte Service Parameter, bei Nicht-erfüllung können Vertragsstraffen zur Anwendung kommen
SSD	Solid State Drive	Diese Festplatte ist ein schnelles, rein elektronisches Speichermedium.
TCP	Transmission Control Protocol	Das Protokoll ist ein zuverlässiges, verbindungsorientiertes, paketvermitteltes Transportprotokoll in Computernetzwerken. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets.
Time-To-…	Zeit bis…	Zeitangabe, bis wann eine Aktion durchgeführt wird.
UDP	User Datagram Protocol	Ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört.
USV	Unterbrechungsfreie Stromversorgung	Wird eingesetzt, um bei Störungen im Stromnetz die Versorgung kritischer elektrischer Lasten sicherzustellen
VPN	Virtual Private Network	Ein geschlossenes Rechnernetz, das auf einer öffentlichen Netzwerkinfrastruktur aufgebaut ist
VDC	Virtuelles Datencenter	Die Virtualisierung Ihres Unternehmens in den Datencentern von GDC
WAN	Wide Area Network	Rechnernetz, das sich über einen sehr grossen geografischen Bereich erstreckt