



Service Description DDoS Guard Services

Version / Datum

1.0

17.12.2020

Authors

Product Management

Inhaltsverzeichnis

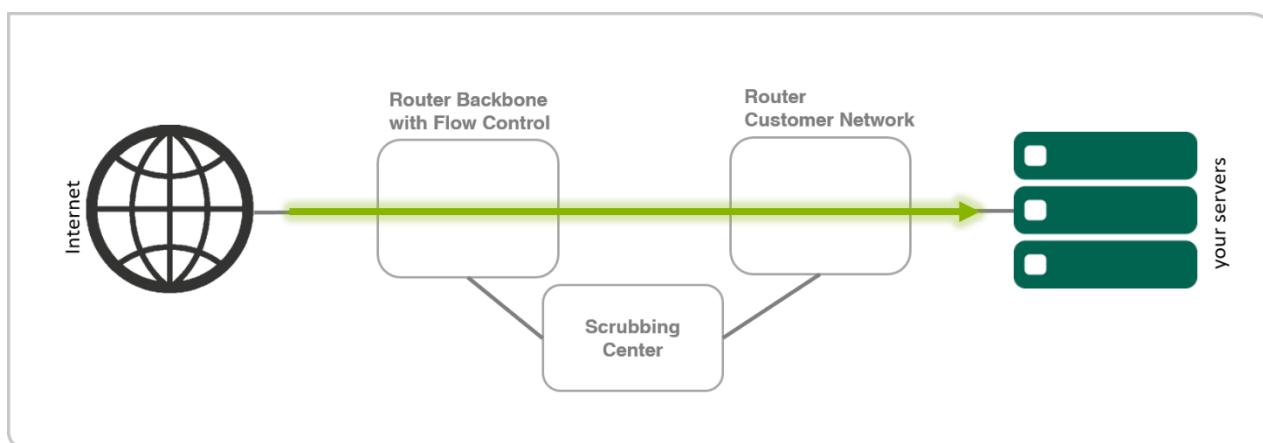
1.	Service description	3
1.1	General flow of DDoS mitigation	5
1.2	Components	6
1.3	Product availability	6
1.3.1	Dedicated Access (standard, extended, premium)	6
1.3.2	Datacenter and Virtual Datacenter Access	7
1.4	Service setup.....	7
1.4.1	DDoS Guard	7
1.4.2	DDoS Guard basic	7
1.4.3	Comparison DDoS Guard DDoS Guard basic	8
1.5	Options	8
1.5.1	DDoS Guard – Protection on Demand	8
1.5.2	DDoS Guard – Always On	8
1.6	Management and controlling portal.....	9
1.6.1	DDoS Guard Customer Dashboard.....	9
2.	Service Level Agreement	13
2.1	Explanation of terms	13
2.2	Customer support	14
2.2.1	Standard channels	14
2.2.2	Support obligations	14
2.2.3	Customer obligations.....	15
2.3	General measures for the security of running operations	15
2.3.1	Physical security through construction, operational, and technical measures:.....	15
2.3.2	Security and availability of internal network infrastructure:	15
2.3.3	Availability of external network connection:	16
2.3.4	Subject of the agreement, scope	16
3.	Service Level	17
3.1	Availability.....	18
3.1.1	Calculation of availability	18
3.1.2	Financial refunds.....	18
3.1.3	Demarcation points	19
3.1.4	Measurement and definition of downtime	19
4.	Customer obligations.....	19
4.1	Warnings	19
4.2	Customer responsibility in the case of a power outage	19
4.3	Canceling services	19
5.	Service management.....	20
5.1	Downtime management.....	20
5.1.1	Reporting of downtime.....	20
5.1.2	Problem-handling procedure.....	20

5.1.3	Support obligations	20
5.2	Amendment procedure.....	21
5.3	Use of subcontractors.....	21
5.4	Escalation process started by the customer	22
5.5	Customer obligations.....	22
5.6	Insurance	23
6.	Legal Terms and Conditions.....	23
6.1	Establishment of the legal relationship.....	23
6.2	Adherence to local laws	23
6.3	Restrictions	23
6.4	Use of personal data	23
6.5	Changes.....	23
6.6	Terms and Conditions	24
7.	Glossary	24

1. Service description

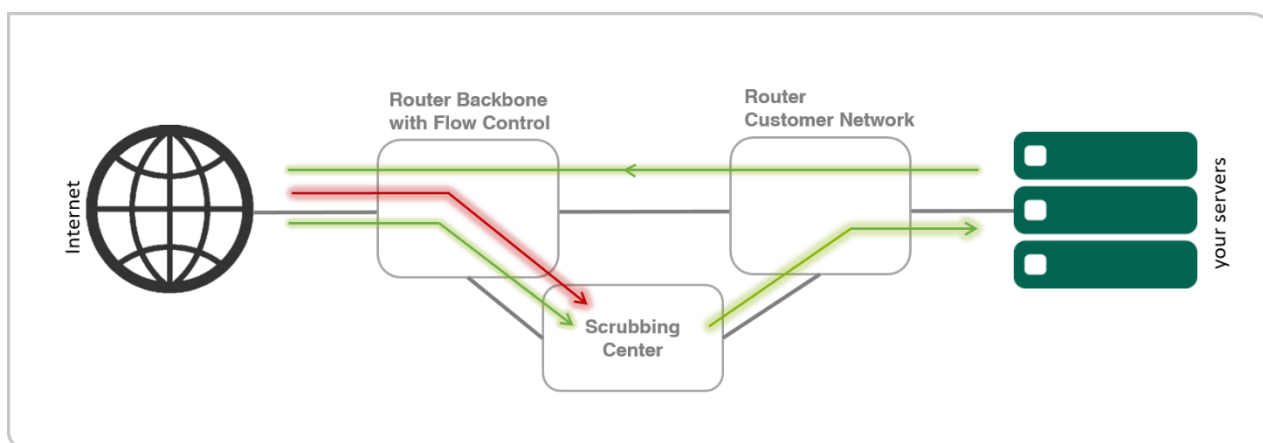
In the past few years, the threat of DDoS attacks has spread throughout a wide range of industries, company sizes, and infrastructures. No one is immune to attacks anymore. Due to the availability of inexpensive bots and reflection attack methods, there is now little difference between industries in the size and scope of the attack.

DDoS Guard is an automated defense solution that protects your network. It protects your infrastructure against volumetric attacks up to 3.5 Tbit/s. All services up to OSI layer 4 are protected. Customers can choose from DDoS Guard and DDoS Guard basic. Options like “Protection on Demand” and “Always On” are available on request and are not part of this service description. For a brief explanation of these options, see section 1.5.



Normal mode – data stream is monitored

DDoS Guard automatically detects attacks (**detection**) and diverts them (**diversion initiation**) to our scrubbing center. In the scrubbing center, the data stream is filtered (**mitigation**), and this clean data stream is routed to the customer network via an NVGRE tunnel. The Green Datacenter (GDC) help desk also promptly contacts the customer to coordinate how to proceed.



Under attack – data stream is filtered

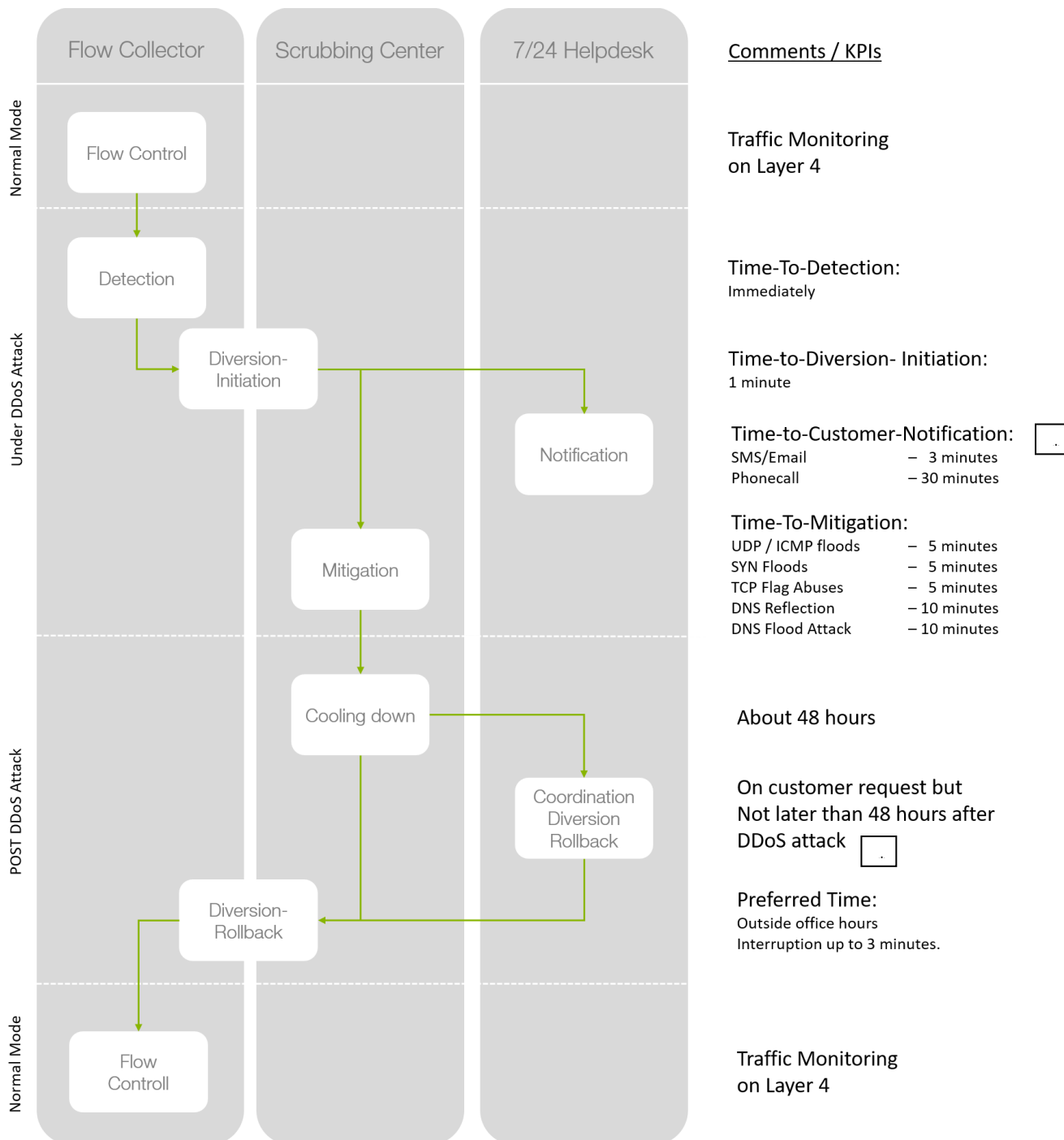
How long a DDoS attack lasts is not relevant. After each attack, the data stream remains in the scrubbing center for several hours, rendering quickly repeated attacks futile. The data stream is only released back into normal operation after the cool-down period and after consultation with the customer. The following conditions are taken into account:

- The scrubbing center does not detect a stream of malicious data packets over a longer period of time of approximately 48 hours (**cool down**).

→ A wave of attacks is rendered futile, decreasing the impact on your business operations.
- Switch back to normal operation takes place during the night or during off-peak hours defined by the customer (**coordination of diversion rollback for DDoS Guard only**).

→ Due to the BGP protocol, it is not possible to fully eliminate short-term interruptions when returning the data stream from the scrubbing center back to normal operation. A coordinated return to normal operation takes this into account (**diversion rollback for DDoS Guard only**).

1.1 General flow of DDoS mitigation



Sequential flow of mitigation of a DDoS attack

* The notification of the customer in case of an attack and the coordinated diversion rollback to normal operation is only done for DDoS Guard, but not for DDoS Guard basic.

1.2 Components

DDoS Guard consists of the following components:

- *Flow collector*

Collects the flow data from all peering points and detects attacks. If an attack is detected, the data traffic of the affected segment is rerouted to the scrubbing center via BGP.

- *Scrubbing center*

Filters the attack data out of the stream and routes the clean data stream to the customer infrastructure.

- *24/7 help desk (not for DDoS Guard basic)*

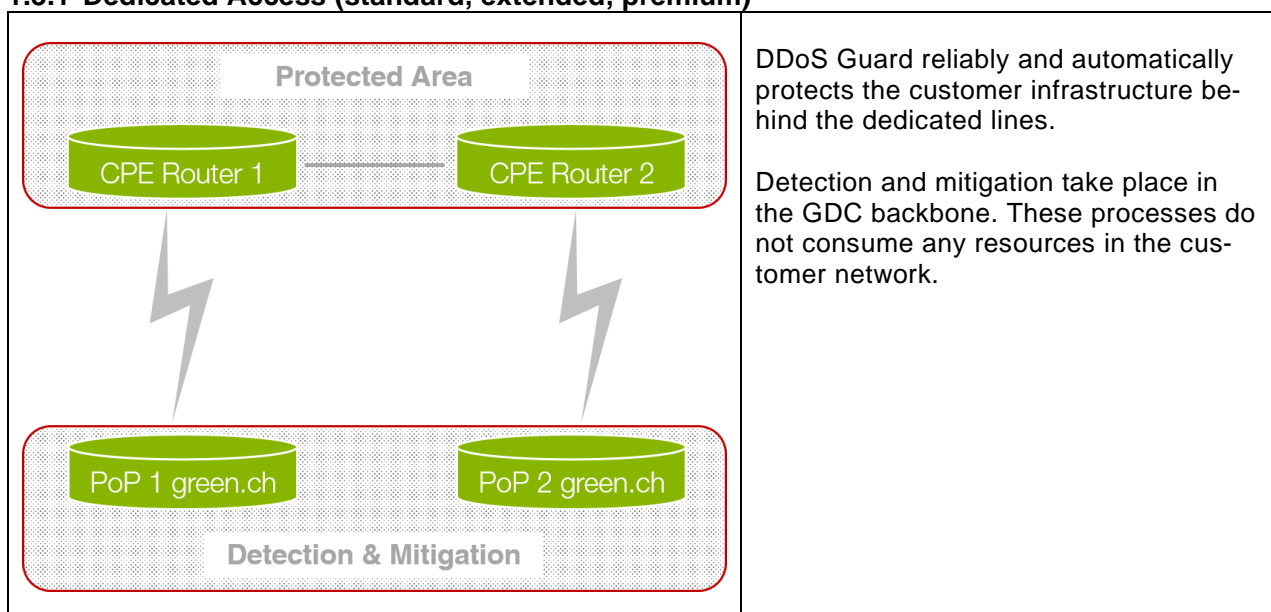
Monitoring and coordination point. In the case of mitigation, the 24/7 help desk contacts the customer with the agreed escalation points and coordinates how to proceed. The following items will be reviewed with the affected areas:

- Reason for mitigation
- Time parameters of the attack (start, duration, etc.)
- Determination of severity
- Consideration and coordination of any necessary additional measures

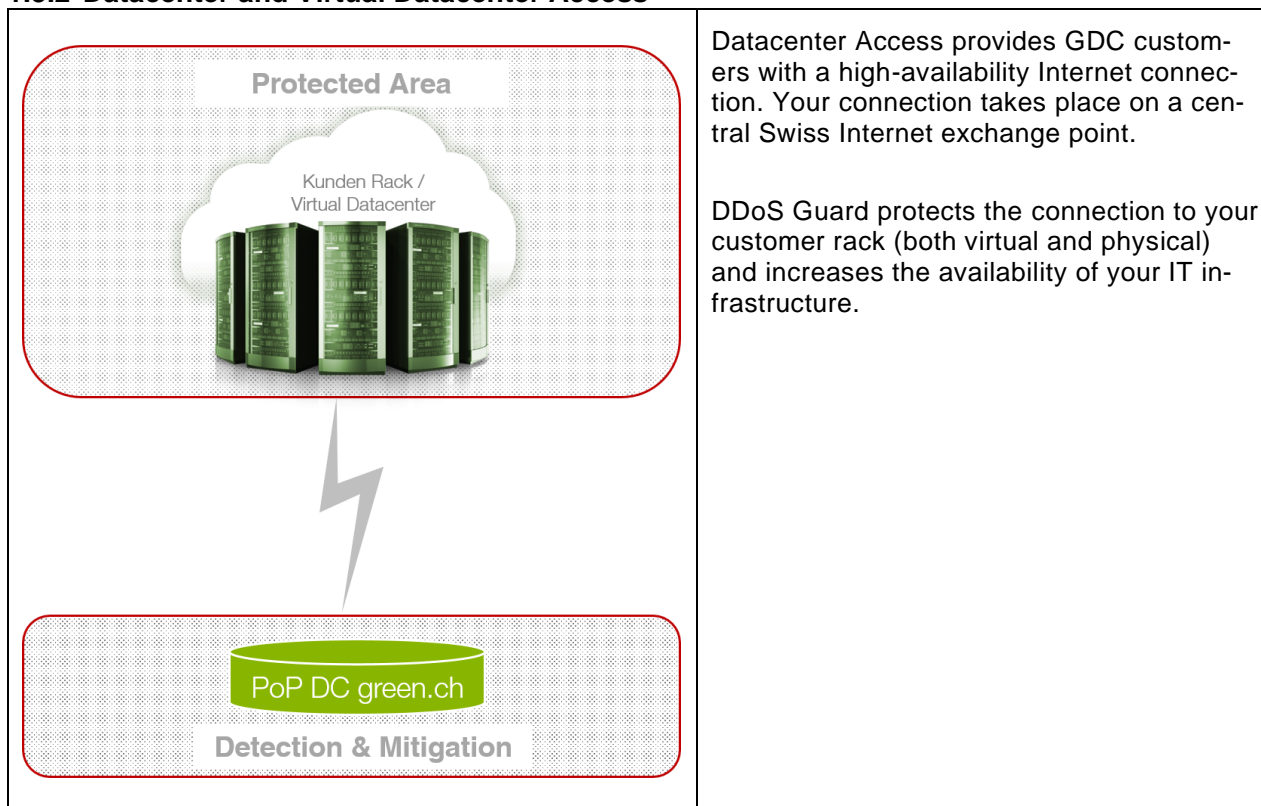
1.3 Product availability

DDoS Guard can be used to defend the following GDC connectivity services against DDoS attacks:

1.3.1 Dedicated Access (standard, extended, premium)



1.3.2 Datacenter and Virtual Datacenter Access



1.4 Service setup

Besides DDoS Guard, GDC is also offering protection for customers with smaller IP-address ranges. DDoS Guard basic uses a very simple setup and is sharing the address range, which is diverted during an attack, with other customers.

1.4.1 DDoS Guard

The objects to be protected are given fixed IP addresses from a predefined range. If the customer has already a IPv4/24 network (256 IP-Addresses) available, it can be used for DDoS Guard.

For smaller networks, the IP address assignments from GDC must be accepted. If the DDoS Guard service is canceled, the associated IP addresses expire. The IP address change is mandatory for all networks.

Independent /24 IPv4 networks (PI networks) are excluded from this regulation.

1.4.2 DDoS Guard basic

DDoS Guard basic includes a GDC defined /28-IP-segment (16 addresses). It is part of a /24 segment which is in shared use with other customers.

The diversion to the scrubbing center on attack is always done for the whole /24 segment – hence, for everybody using this shared network segment. There is no notification of the customer in case of an attack and the rollback to normal operation is done during the early morning hours without coordination with the customers sharing the network segment.

1.4.3 Comparison DDoS Guard DDoS Guard basic

Feature	DDoS Guard	DDoS Guard basic
protected network segment	private /24 segment (256 addresses) or customers already existing /24 PI-segment	/28 segment in a shared /24 segment
larger address segments	optional additional /24 segments or larger	optional larger address segments up to /26 (64 addresses)
Service Desk	365 x 24	Mo to Fr 06:00 to 22:00 h
Attack notification	phone and eMail	none
Rollback after attack	coordinated with customer	automatic, during early morning hours
DDoS Dashboard	yes	none

1.5 Options

Both options are available on demand and for DDoS Guard customers only

1.5.1 DDoS Guard – Protection on Demand

With Protection on Demand, the customer decides when mitigation of an attack should start. The customer is responsible for noticing the attack and escalating it to their provider. There are no automated processes.

1.5.2 DDoS Guard – Always On

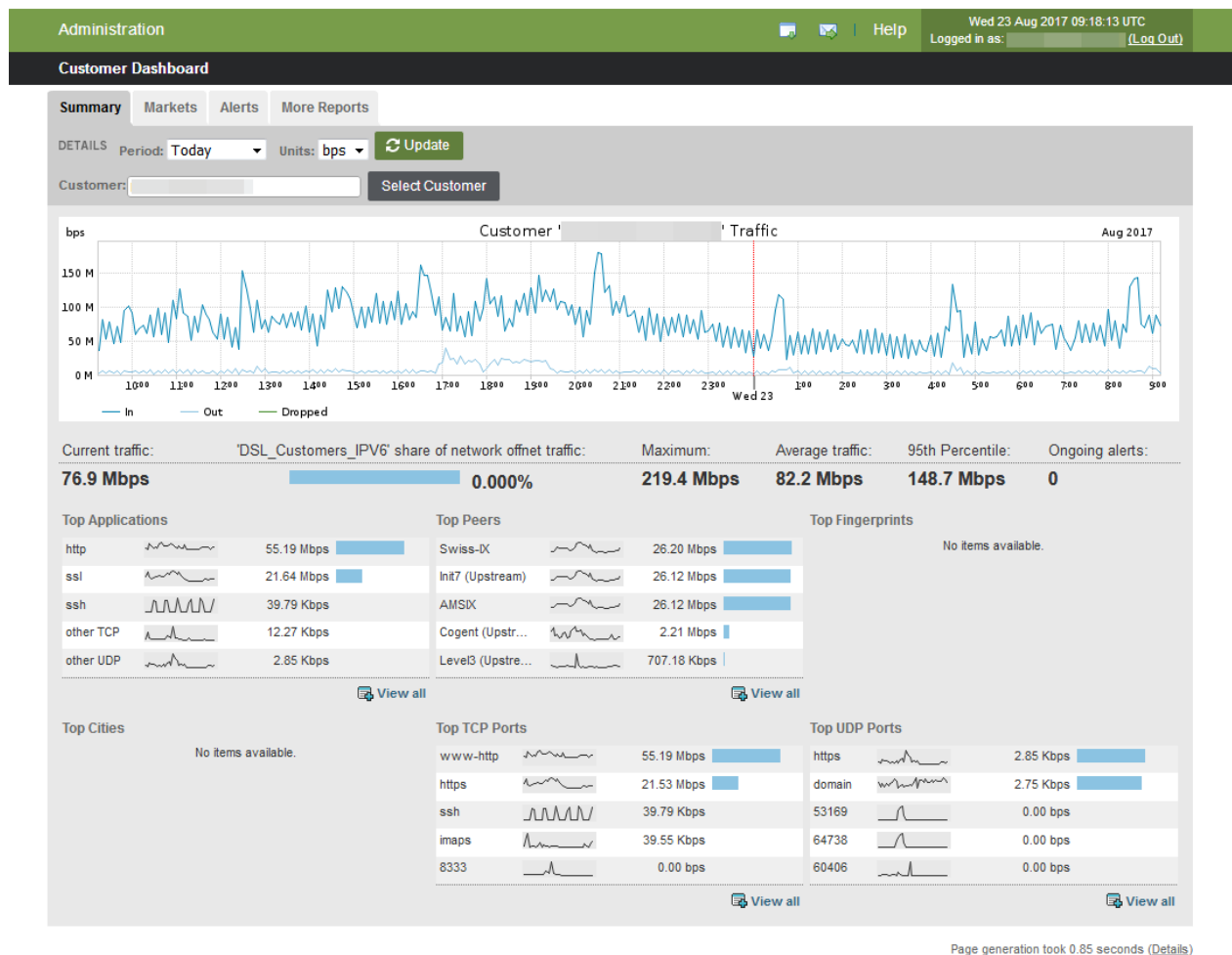
In this case, the data stream is permanently routed to the scrubbing center. Attacks are immediately detected and no time is lost for detection and diversion initiation. And it is not necessary to roll back the data stream into normal operation. The permanent binding of resources for mitigation is reflected in the cost of the service.

1.6 Management and controlling portal

1.6.1 DDoS Guard Customer Dashboard

The DDoS Guard Customer Dashboard allows the customer to monitor his connectivity services. In addition to providing a summary report, alerts are monitored and logged.






green.ch






DDoS Guard Customer Dashboard

The following detailed traffic reports are available to the customer:





BGP 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 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.

Top Talkers



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 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.

Other



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.



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.



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.



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.



Raw Flows

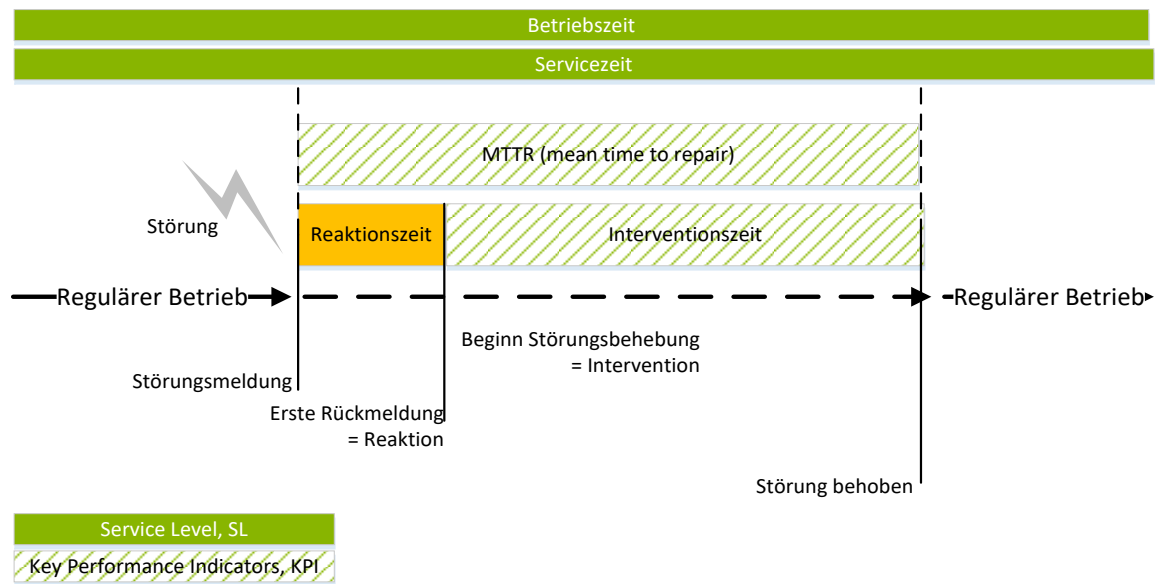
This report shows the last 10 sampled flows through the selected customer.

2. Service Level Agreement

Successful outsourcing of IT services requires a transparent definition of the customer-provider relationship. GDC and the customer define the services to be supplied by GDC (service level) and the customer's obligations in the following Service Level Agreement (SLA).

2.1 Explanation of terms

Service level, SL	Defined, measurable criteria for specific performance levels supplied by GDC
Key performance indicators, KPI	Targeted but not obligatory service measurements
Service hours	The service hours are the times when the contractually agreed services will be provided.
Operating hours	The operating hours are the times when the system is generally available. The planned and announced maintenance windows are not part of the operating hours. The total number of operating hours per year is 8,604 hours, calculated as follows: 1 year 24/7 = 8,760 h – 156 h maintenance window. In the case of redundant architecture, the two redundant devices/systems will be serviced at different times.
Availability	Availability [%] = $100 * ((\text{operating hours} - \text{unplanned downtime during operating hours}) / \text{agreed operating hours})$. Planned maintenance windows are excluded from the agreed operating hours.
Response time	Response time is the maximum amount of time between when a problem occurs or is reported and when problem analysis begins. GDC is committed to maintaining the specified response times and quickly rectifying downtimes and faults. It is not, however, possible to guarantee adherence to the response times in all cases. Exceeding the agreed response times is not subject to penalties nor claims for damages.
Mean time to repair, MTTR	Average time needed for a repair or to restore service
Maintenance windows	For the purposes of this SLA, "planned maintenance" is necessary in order to provide the services or to update the infrastructure. Planned maintenance windows are defined in advance and published at status.green.ch . In addition, the customer will be informed of a planned service interruption for maintenance work at least 48 hours in advance. GDC sends an e-mail to the customer's designated (in writing) technical contact containing information on the planned service interruption and the type of the interruption. If maintenance is required, GDC will attempt to limit it to one of the regular maintenance windows. The maintenance windows are 05.30 to 06.30, CET, on Saturdays, Sundays, and Tuesdays. Should unplanned events or malfunctions occur, GDC has the right to carry out emergency maintenance work at any time and without prior notification. In this case, the maintenance work is published at http://status.green.ch .
Single point of contact, SPOC	The single point of contact (SPOC) is the central contact point for customers and is provided by the Customer Care Center (support hotline +41 330 3535).



General problem-handling process

2.2 Customer support

GDC's highly qualified, multilingual support employees are available to answer your support and administrative questions via phone or via the online ticket system at www.green.ch. Customer phone support is available 24/7 – the Business Support Team is the first contact for all questions, except for questions related to sales. Problems that cannot be solved by the Support Team will be escalated to GDC's responsible technical or business employee.

2.2.1 Standard channels

Support is available for all our services over the standard channels:

Online support: via ticket system (<https://contact.green.ch/>)

Live chat: <https://www.green.ch/>

The GDC website: <https://www.green.ch/support>

As a GDC customer for DDoS Guard, you receive telephone support at +41 44 330 3535 on a 24/7 basis.

2.2.2 Support obligations

- Checking the requester's authorization and the service level
- Starting the downtime management process and the troubleshooting process, which includes:
 - Receipt of the request, opening a trouble ticket, and confirmation

- Prioritization, coordination, and monitoring of the troubleshooting process using internal and external resources
- Informing the customer about measures taken, interim solutions, and the final solution
- Informing the customer about the restoring of server availability
- Analyzing the cause and making recommendations for further action (change management).

2.2.3 Customer obligations

In order to guarantee our high level of service, GDC requires that the customer adhere to the following guidelines:

- The customer supplies all required contact information, including contacts for escalating the delivered services, and ensures that any changes are updated in a timely manner.
- The customer ensures that information on changes to the configuration, interfaces, channels, applications, and systems that is relevant to the provision of joint services is supplied to GDC and kept up to date.
- The customer is responsible for maintaining all of their applications. GDC is not responsible for maintaining customer applications or customer data.
- Only equipment that is in good condition and that poses no danger to persons or property may be installed.
- The customer cannot have write access to equipment managed by GDC.

2.3 General measures for the security of running operations

In its data centers, GDC exclusively provides services with the highest quality and security. Some of the measures used to maintain the security of customer data and the availability of services include:

2.3.1 Physical security through construction, operational, and technical measures:

- Entry control systems
- Video monitoring inside and outside the building
- Smoke, dust, and water detectors
- Fire extinguishing system
- Air conditioning via two separate cooling circuits
- Redundant power feeds from energy providers
- Ring connection to public high-voltage supply
- UPS filter power supply
- High-performance emergency diesel generators
- Redundant supply lines in the building

2.3.2 Security and availability of internal network infrastructure:

- Network segmenting and strict separation of different data streams
- Daily backup of own systems
- Use of firewalls at relevant network nodes
- Network monitoring via an in-house NOC (network operation center)
- Exclusive use of brand-name components

2.3.3 Availability of external network connection:

- Carrier-neutral, redundant data center IP connection

2.3.4 Subject of the agreement, scope

This SLA solely applies to the quote sent with the SLA and the associated signed Service Agreement. Other agreements between GDC and the customer remain unaffected. The SLA only applies to connectivity services and options and is not transferable to other product areas. In the case of conflicting provisions, the provisions in the Service Agreement take precedence over the provisions in the SLA. In all cases, the GDC General Terms and Conditions apply.

3. Service Level

The SLA ensures the customer a defined quality, and if GDC does not provide services included in the guaranteed service level, it entitles the customer to a refund of their monthly charges or a part thereof (hereinafter “service credit for unavailability”).

Service	Value or comment
<u>Guaranteed service level</u>	
DDoS Guard service availability	99.9%
24/7 service management provided by GDC Network Operation Center	DDoS Guard only - invoiced separately
<u>Key performance indicators, KPI</u>	
Response time Time to customer notification	Notification by phone: 30 minutes Notification by SMS/e-mail: 3 minutes → no notification with DDoS Guard basic
DDoS detection Time to detection	Immediate
Rerouting/diverting to scrubbing center Time to diversion initiation	One minute
Typical filter adjustment 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.
Subsequent observation Cool down	48 hours
Coordination of the return to normal operation Coordination of diversion rollback	In consultation with the customer But within 48 hours at the latest → no coordination of rollback for DDoS Guard basic
Return to normal operation Diversion rollback	Overnight or outside office hours The return to normal operation causes an interruption of up to three minutes
Monitoring the data packages Flow control	Up to ISO layer 4
<u>Framework conditions</u>	
Operating hours	365 x 24 (excluding planned and announced maintenance windows)
Service hours	365 x 24 for DDoS Guard Mon to Fri, 06:00 to 22:00 for DDoS Guard basic
Office hours	Mon–Fri, 8.00 to 17.30, CET
Callback	Included
Priority handling	Included
Problem reporting	By phone or contact form at https://contact.green.ch/ , outside office hours only by phone using the provided standby number

3.1 Availability

GDC ensures the following specified availabilities for the services specified in the quote. Failure of part of a redundant system is not considered downtime. If GDC is not able to comply with the aforementioned availability, the customer acknowledges and agrees that the credits agreed to in the SLA represent the sole and exclusive compensation for the customer.

To measure the service level, an in-house monitoring system monitors the availability. GDC uses various technical processes to check the availability of the DDoS services. The customer can also report a problem by opening a service ticket.

3.1.1 Calculation of availability

$\text{Availability} = (\text{operating hours} - \text{downtime}) / \text{operating hours} * 100$

GDC offers credits as soon as service availability falls below the guaranteed threshold. The tables in this document show the credits as a percentage of the base monthly recurring charges (MRC). These credits and compensations are final. Further or other compensation is excluded. No credit will be issued or payment made for any reason or in any scope other than that stated here, including – but not limited to – business losses on the part of the customer due to downtimes.

3.1.2 Financial refunds

If GDC is unable to fulfill contractually agreed obligations, GDC grants the customer a credit of 5% of the monthly subscription fee for each registered hour of downtime – up to a maximum of 50% of the monthly subscription fee for the affected subscription component. Any further claims for damages are explicitly excluded. The customer must submit any claims to GDC by submitting a request at <https://contact.green.ch/>.

No SLA credit will be granted if a service is not available for a specific period of time, if this time or a part of this time is due to one of the following reasons:

- Downtime of equipment on the customer's premises (if it does not belong to GDC), at the customer's location (e.g., due to an electricity outage), or of equipment belonging to one of the customer's providers
- Natural catastrophes, terrorist attacks, or other force majeure events
- Downtime due to magnetic/electromagnetic interference or electrical fields
- Negligence or omission on the part of the customer (or customer employees, representatives or subcontractors), such as:
 - Customer delays in delivering required equipment
 - Failure to grant GDC sufficient access to facilities for testing purposes
 - Failure to grant access to customer premises to allow GDC to fulfill its service obligations
 - Failure to take appropriate countermeasures regarding services as recommended by GDC or preventing GDC from implementing these countermeasures itself
 - Failure to use redundancies as offered in the relevant service level
 - Negligence or intentional malpractice on the part of the customer, including failure of the customer to follow agreed processes
- The customer prevents or delays entry to the cage

- All planned maintenance windows if the customer was informed thereof, and emergency maintenance carried out to prevent future downtime
- Shutting off or interruption of services by GDC after the customer has not paid an invoice within 90 days of the invoice date, or for other sufficient reasons

Customer equipment may not consume more power than the power lines can deliver to each point. Since equipment requires more power in the boot phase, GDC recommends an automatic switch-on delay to prevent overloading during a reboot after a power outage. Overloading for this reason would be considered a design error on the part of the customer and would therefore not be covered by this SLA.

3.1.3 Demarcation points

This SLA applies to GDC DDoS Guard service. All warranties with respect to performance and operability apply solely to GDC-managed equipment that serves as the interface between customer-managed equipment and GDC's providers. These providers include power companies, landlords, and other telecommunications companies.

If the customer manages their own equipment, GDC's area of responsibility ends at the patch panel coming from the patch room or at the endpoint of the carrier service (in-house point of transfer).

3.1.4 Measurement and definition of downtime

Only the downtime (non-availability of a service) that falls under GDC's responsibility is considered. Downtime is defined as follows: Downtime begins when the customer opens a support incident or when GDC itself discovers a problem, and ends when one of GDC's employees indicates that the problem has been solved. There is no other measurement of downtime, and all times used for this calculation are recorded by GDC. Operating times are calculated independently for each service, where the worst value (the longest downtime) is used to calculate the credit for the customer.

4. Customer obligations

4.1 Warnings

It is the responsibility of the customer to open support incidents for all open problems. Creation of an automatic warning on the part of GDC is not a confirmation of a problem. Only a correctly opened ticket can be used to calculate downtimes and credits.

4.2 Customer responsibility in the case of a power outage

After a power outage, it is the customer's responsibility to take the necessary steps to get customer equipment online again.

4.3 Canceling services

When a service is canceled, the customer must return all equipment that GDC provided for the service to GDC within thirty (30) days after the contract ends, without being requested to do so. The equipment must be returned in proper working order. The customer is responsible for all charges and costs

incurred during this process. For a charge, a GDC technician can be commissioned to collect the equipment, send it by post, or choose another method.

- In the following cases, the customer is liable for the cost of replacing hardware:
 - If the equipment is lost or not returned within 30 calendar days after the contract ends
 - If the state of the equipment is such that the GDC cannot use the hardware for another customer; time-related wear is excluded

5. Service management

5.1 Downtime management

5.1.1 Reporting of downtime

GDC informs the customer's technical contact either by phone or e-mail (written notification is sent to the contact in the contact data provided to GDC).

5.1.2 Problem-handling procedure

GDC's philosophy is to provide the customer with the best availability and service quality that is technically and operationally possible. In the case of problems, our main objective is to quickly repair the problem and restore service availability. The benefit to the customer is a limitation of the impact on business operations.

Incidents and downtime related to "reactively" controlled services must be reported by the customer. When downtime is reported, a trouble ticket is opened and analyzed. The service will be restored based on the agreed service level.

Incidents and downtime related to "proactively" controlled services are reported by the monitoring system. The customer will be informed as specified in the agreed service level. If downtime affects the customer's business operations, the customer has to open a trouble ticket over the appropriate channels.

5.1.3 Support obligations

- Determining and checking the authorization of the person who submits the incident and comparing it with the Service Level Agreement between the customer and GDC.
- Starting the incident management process, which includes the following:
 - Receipt of the request, opening a trouble ticket, and confirmation
 - Using internal and external means to prioritize, coordinate, and monitor the troubleshooting process
 - Informing the customer about measures taken, interim solutions, and the final solution
 - Informing the customer about the restoring of server availability
 - Analyzing the cause and making recommendations for further action (change management)

In the case of unexpected delays during troubleshooting that could lead to a violation of the SLA, an internal escalation process will be automatically started. Depending on the type of problem, the first escalation level is either an internal senior employee or sales/subcontractor support. At this point in time, the manager on duty will be involved to ensure that the SLA is adhered to during the escalation process and that the problem is solved in a timely manner.

5.2 Amendment procedure

Changes to the Customer Agreement will be in writing, unless otherwise agreed. Changes that are not in writing are invalid. Unless otherwise agreed, each contracting party will bear the costs associated with management of the agreements.

The contracting parties will check proposed revisions and inform the proposing party in writing whether they agree to the revisions or wish to make any changes – as a rule within two weeks of receipt of the proposed revisions. As a rule, the other party agrees to or refuses the changed proposed amendment or the alternative proposed amendment within a further two weeks.

If one of the parties refuses a submitted proposed revision for a valid reason or if the other party refuses the proposed revision, or does not agree within the stipulated period, the agreed scope of services and conditions remain unchanged.

5.3 Use of subcontractors

GDC mainly provides the agreed services using its own employees and resources. However, GDC is entitled to use third parties or employees of other companies (hereinafter referred to as “subcontractors”) to provide the agreed services.

Only qualified specialists from companies accredited by GDC will be used. The subcontractors must meet the same reliability requirements as GDC itself.

In addition, the following applies whenever subcontractors are used:

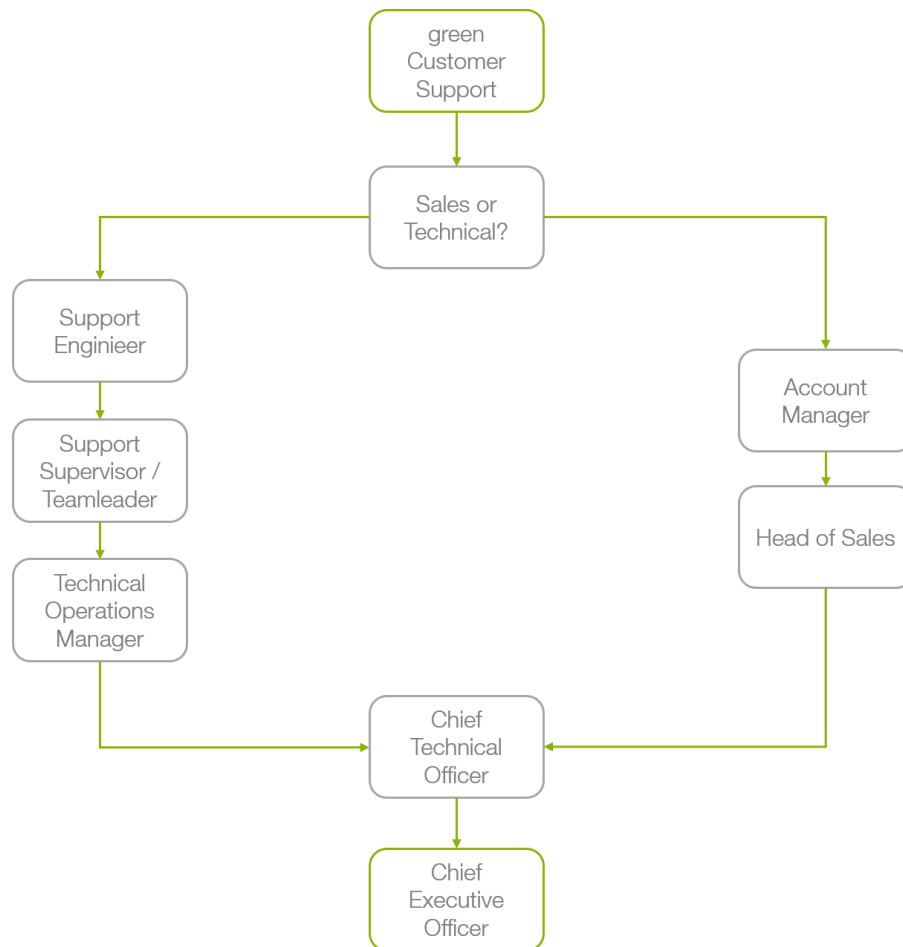
- GDC remains the sole contact for the customer with respect to all services provided by the subcontractor.
- GDC is obliged to ensure that the subcontractor adheres to the obligations contractually agreed with the customer.
- GDC is responsible for selecting, monitoring, and instructing the subcontractor. The use of a subcontractor does not release GDC from its own obligation to perform. Claims arising from simple negligence are excluded.
- GDC must conclude a written agreement with each subcontractor in which the subcontractor's obligations are defined.

The subcontractor's services are performed as GDC services in the name of and on behalf of GDC.

The use of subcontractors with respect to collecting, processing, and using company and personal data is subject to the data protection regulations in accordance with GDC's General Terms and Conditions (GTC). Disclosure of company and personal data, irrespective of the above requirements for using subcontractors, is only allowed when the subcontractor has accepted the data protection regulations in accordance with the GTC. In general, customer personal data can only be disclosed to countries outside Switzerland when the customer has given written permission to do so and the data protection requirements have been met.

5.4 Escalation process started by the customer

If the customer is concerned that the speed or quality of the support or troubleshooting process could seriously jeopardize their business, then the customer can independently trigger the escalation process.



5.5 Customer obligations

- The customer supplies all required contact information, including contacts for escalating the delivered services, and ensures that changes are continually updated.
- The customer supplies GDC with a list of all individuals authorized to access support.
- The customer implements and updates suitable methods for identifying these authorized persons.
- The customer ensures that information about changes to the configuration, interfaces, channels, applications, and systems that is relevant to the provision of joint services is supplied to GDC and kept up to date.
- The customer is responsible for continually maintaining all of their applications. The customer is solely and fully responsible for servicing customer applications and customer data.
- Only equipment that is in good condition and that poses no danger to persons or property may be installed.

- The customer must ensure that GDC has access to the equipment managed by GDC at all times and for whatever reason. If this is not ensured, it is considered a violation of the agreement and can lead to canceling the agreement.
- The customer does not have write rights to equipment managed by GDC. Optional SNMP read rights are available.
- When working together with GDC employees, all activities must be coordinated in advance. This includes the addition of service options such as additional accounts or network changes.
- Every unauthorized attempt on the part of the customer to access GDC equipment, either physically or electronically, is strictly forbidden. This also applies to CPE (customer premise equipment).

5.6 Insurance

GDC systems are insured against the relevant risks. However, neither customer data nor the availability of services that the customer delivers to his own customer base are insured in any way, shape, or form. It is expressly the responsibility of the customer to obtain insurance protection. No compensation beyond the credit percentages explicitly described in this document will be granted for loss of business information or any other consequences of system downtimes.

6. Legal Terms and Conditions

6.1 Establishment of the legal relationship

A legal relationship is established between GDC and the customer when the website order is completed. Measurement of SLA parameters starts on the date the agreement becomes effective.

6.2 Adherence to local laws

The customer ensures that no illegal data traffic will be sent over GDC connections. GDC accepts no liability for such traffic.

6.3 Restrictions

All forms of compensation for GDC services are limited to the scope defined in this document. No credit will be issued or payment made for any reason or to any scope other than that given here, including – but not limited to – business losses on the part of the customer due to downtimes.

6.4 Use of personal data

The customer expressly accepts the GDC data privacy guidelines for using personal data.

See: <https://www.green.ch/en/legal-aspects/data-privacy>

6.5 Changes

GDC reserves the right to change this document as long as the customer is informed in writing before the changes become effective. If the changes have a major impact on the services, the service fee, or

other obligations under this agreement, then the customer may terminate the agreement in writing with a one-month notice period.

6.6 Terms and Conditions

GDC's General Terms and Conditions (Green Datacenter AG General Terms and Conditions) are an integral part of the Customer Agreement. The customer's General Terms and Conditions do not apply. Deviating provisions in customer documents do not apply. Terminations, changes, and additions to this Service Agreement and the Service Level Agreements must be in writing. The written form can only be waived in writing.

If individual provisions of this Service Agreement or the Service Agreements or other Appendices to the Customer Agreement become legally ineffective or infeasible, the contractual parties will replace the ineffective or infeasible provision with an effective and feasible provision which most nearly approximates the intention of the contractual parties at the time of the agreement on the provision in question and complies with the mutual objectives listed in the preamble of this Service Agreement. The newly chosen provision may not affect the relation between the services provided by GDC and the customer.

see: <https://www.green.ch/en/legal-aspects/contract-terms>

7. Glossary

Abbreviation		Explanation of terms
/24	/24 network mask	An IPv4/24 network consists of a maximum of 254 usable IPv4 addresses. Most private LAN networks use a /24 network mask. The network mask is also an indication of the size of an IP network.
/28	/28 network mask	An IPv4/28 network consists of a maximum of 14 usable IPv4 addresses.
BGP	Border gateway protocol	The BGP is the routing protocol used on the Internet to interconnect autonomous systems (AS). These autonomous systems are usually set up by Internet service providers.
Bot/Botnet	Botnet	A botnet is a group of automated malware known as bots. The bots (from robot) run on networked computers whose network connection, local resources, and data can be accessed without the owner's permission.
Cool down	Cool-down phase	Each time a DDoS attack is mitigated, the data traffic remains in the scrubbing center for a defined period of time. Since the data traffic has already been diverted, quickly repeated attacks no longer impact the customer infrastructure.
Coordination of diversion rollback	Coordination of the return to normal operation	After cool down, the data traffic must be returned to normal operation. Since this can cause a short network interruption of up to three minutes, this test is coordinated in advance with the customer.
CPE	Customer premises equipment	Hardware owned by GDC that is installed at a customer location.

DNS	Domain name system	Hierarchical decentralized naming system whose main task is to resolve name resolution requests.
DNS attack	DNS amplification attack	The DNS amplification attack is a denial-of-service attack that misuses the domain name system to divert extremely large data streams to the victim's Internet connection.
DDoS	Distributed denial of service	Attack method to make a service unavailable. Often infrastructures are blocked or overloaded with a large number of requests.
Diversion initiation	Initiation of the diversion	As soon as the flow control detects a DDoS attack, the diversion to the scrubbing center is initiated. The scrubbing center receives information about the network addresses that need to be cleaned and contacts them via the BGP protocol.
Diversion rollback	Rollback of the diversion	When a DDoS attack ends and no further attacks are detected during cool down operation, data traffic is rolled back to normal operation.
Flood	Flood attacks	Attack method in which the target/victim is flooded with random protocol requests (DNS, UDP, etc.) and can therefore no longer respond to normal requests.
Gbit	Gigabit	Data transfer rate. Describes the volume of data that can be transferred via a communications channel within a certain period of time.
GB, MB, TB	Gigabyte, megabyte, terabyte	Size units for storage or memory.
IAAS	Infrastructure as a service	Provision of a virtual IT infrastructure via public or private networks, usually over the Internet. With IaaS, the customer uses servers, storage, network, and the rest of the data center infrastructure as an abstract, virtualized Internet service.
ICMP	Internet control message protocol	Used in computer networks to exchange information and error messages via the Internet protocol version 4 (IPv4). There is a similar protocol for IPv6 that is named ICMPv6.
IP addresses	Internet protocol addresses	Addresses in computer networks that – like the Internet – are based on the Internet protocol. Assigned to devices that are connected to the network, making the networks addressable and accessible.
IPv4	IP protocol version 4	IPv4 was the first version of the Internet protocol that was used worldwide. It forms an important technological basis for the Internet. It was defined in RFC 791 in 1981.
IPv6	IP protocol version 6	Internet protocol version 6 (IPv6), previously also known as Internet protocol next generation (IPng) was declared in 1998 by the Internet Engineering Task Force (IETF) to be a standardized process for transmitting data in packet-switched networks, especially the Internet.
KPI	Key performance indicator	Targeted and usually fulfilled, but not guaranteed service parameter.
LAN	Local area network	A computer network within a limited area consisting of at least two computers.

Mitigation	Damage limitation	In DDoS, mitigation is the filtering of data packages. After mitigation, the clean data traffic is handed over to the customer.
MIPS	Managed IP service	Service provided by GDC to connect you to the Internet using mapped IP addresses.
MRC	Monthly recurring charge	Monthly recurring fee
NAT	Network address translation	A method of remapping one IP address space into another to connect to different networks. They are typically used in routers.
OTC	One-time charge	Non-recurring charge
PA network	Provider-assigned network	The customer is assigned a network by his provider. The customer is loaned the IP addresses. The provider remains the owner of the IP addresses and the network.
PI network	Provider-independent network	PI address space is a block of Internet protocol addresses (IP addresses) assigned by a regional Internet registry (RIR) directly to an end user. The user is not dependent on an Internet service provider for address assignment. PI networks have a prefix length of 24 or greater.
RAM	Random access memory	A type of data storage that is especially used in computers as computer memory, mainly in the form of memory modules.
Scrubbing center	Data cleaning center	When a DDoS attack is detected, the data traffic is diverted to a scrubbing center that removes the malicious data packages.
SLA	Service Level Agreement	Agreement or interface between the customer and service provider for recurring services.
SL	Service level	Guaranteed service parameter; non-fulfillment can lead to penalties.
SSD	Solid state drive	This drive is a fast, purely electronic storage medium.
TCP	Transmission control protocol	This protocol is a reliable, connection-oriented, packet-switched transport protocol in computer networks. It is part of the Internet protocol family, the foundation of the Internet.
Time to...	Time to...	Time by when an action will be executed.
UDP	User datagram protocol	A minimal, connectionless network protocol that belongs to the transport layer of the Internet protocol family.
UPS	Uninterruptible power supply	Used to ensure the power supply to critical electrical elements in the case of disturbances in the electrical grid.
DNS attack	DNS amplification attack	The DNS amplification attack is a denial-of-service attack that misuses the domain name system to divert extremely large data streams to the victim's Internet connection.
VPN	Virtual private network	A closed computer network that extends a private network across a public network.
VDC	Virtual Datacenter	The virtualization of your company in GDC data centers
WAN	Wide Area Network	Computer network that extends over a large geographical area.