Service Description

Managed Security

Version	Datum	Autoren
1.0	31.05.2021	Product Management Green

moving. forward. together.

Inhaltsverzeichnis

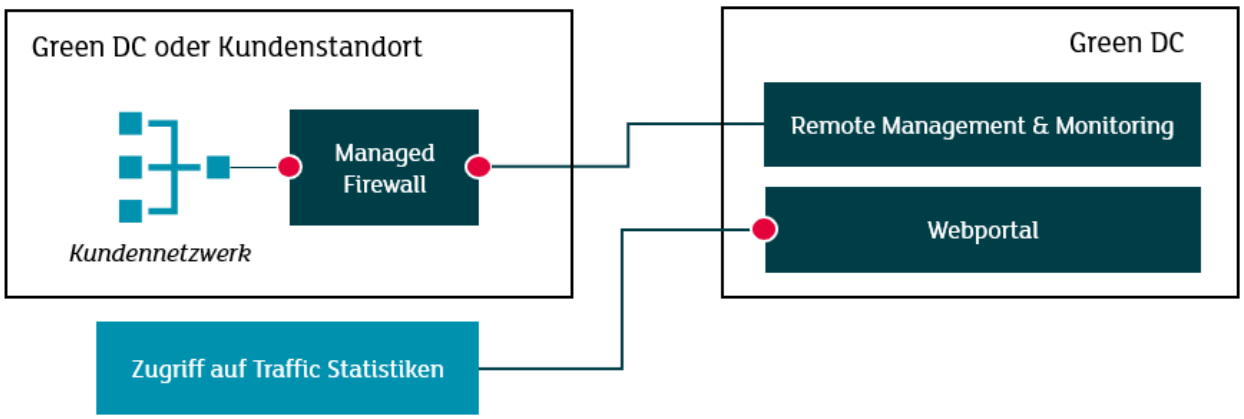
1. Service Ausprägungen

Managed Security ist ein Firewall-Service von Green, der die folgenden Komponenten umfasst: Bereitstellung einer physischen Firewall am Kundenstandort oder im Green Datacenter, Remote-Management der Firewall und Überwachung der Verfügbarkeit durch das Network Operation Center von Green, Software-Aktualisierungen nach Bedarf, Bereitstellung von Auswertungen in Form von Traffic Statistiken via Webportal.

Der Service bietet Stateful Packet Inspection, Deep Packet Inspection, eine grosse Auswahl an Anwendungsproxies (HTTP, HTTPS, SMTP, FTP, DNS, POP3), NAT und VPN Funktionalitäten. Optional sind weitere Security Pakete (Multifaktor-Authentisierung für VPN, Basic Security und Total Security) verfügbar.

1.1 Service Access Punkt

Der Service Access Punkt befindet sich auf den Interfaces der Firewall am Kundenstandort oder im Green Datacenter bzw. auf dem Webportal.



Der Managed Security Service ist ebenfalls redundant mit einer Cluster Firewall und zwei separaten Internet Anbindungen verfügbar. Die Cluster Firewall kann im Active-Active oder Active-Passive Modus betrieben werden.

1.2 Verantwortlichkeiten

Bereitstellung des Service

- Green ist verantwortlich für die Installation der Firewall vor Ort. Die Einbindung in das Kundennetzwerk erfolgt im Regelfall als in-Line-Konfiguration.
- Der Kunde gewährt Green bzw. dem Subunternehmer Zutritt zum Standort für die Installation der Endgeräte und die Inbetriebnahme des Service.
- Der Kunde stellt eine funktionsfähige, permanente Internetanbindung zur Verfügung, so das Green jederzeit auf die Firewalls zugreifen kann. Green empfiehlt die Nutzung einer dedizierten Leitung (Dedicated Access). Pro Firewall wird eine statische und aus dem Internet direkt erreichbare IP Adresse benötigt.
- Der Kunde liefert Green alle notwendigen Informationen zur Erstellung eines Firewall Regelsets, um die ein- und ausgehenden Datenströme zu schützen.

Betrieb des Service

- Der Kunde muss die korrekte Stromversorgung am Kundenstandort sicherstellen (AC Eingangsspannung 230 V, AC Eingangsfrequenz 50 Hz, Max. AC Eingangsstrom 2A). Die Verantwortung für Ausfallszeiten aufgrund eines Stromausfalls beim Kunden vor Ort wird explizit ausgeschlossen.
- Der Kunde muss die korrekte Umgebungsbedingungen am Standort sicherstellen (Betriebstemperatur 0° bis 40°C, Betriebsfeuchtigkeit 10 bis 85%, nicht kondensierend, Raumluft weitgehend staubfrei).
- Der Kunde muss die Firewall vor Zugriffen durch unbefugte Dritte schützen. Der physische Zugang zur Firewall darf nur autorisierten Betriebskräften möglich sein.
- Green stellt dem Kunden Supportleistungen zur Behebung von Störungen zur Verfügung.
- Der Kunde, sofern er eine Störung feststellt, meldet diese an Green über die unter Abschnitt 3 genannten Kanäle. Im Falle einer notwendigen Störungsbehebung beteiligt sich der Kunde aktiv und im Rahmen seiner Möglichkeiten bei der Fehleranalyse. Für die Kommunikation von Störungen an die Anwender ist der Kunde verantwortlich.
- Der Kunde muss Green einen kompetenten Ansprechpartner nennen, der für den Kunden verbindlich Entscheidungen treffen kann
- Der Kunde muss Störungen in nachvollziehbarer und detaillierter Form unter Angabe aller für die Ursachenerkennung und -Analyse zweckdienlichen Informationen schriftlich melden.
- Der Kunde muss auf Anfrage von Green einen Protokoll-Trace von seinem Router zur Verfügung stellen, um die Funktionsfähigkeit der Interfaces nachzuweisen.
- Der Kunde muss Mitarbeitern der Green Zugang zu seinen Betriebsräumen gewähren, soweit dies für Störungseingrenzung oder –Beseitigung erforderlich ist.
- Green überwacht die bereitgestellte Firewall durch das Network Operation Center (NOC) an 365 Tagen im Jahr (24x7) auf ihre Verfügbarkeit.
- Green installiert die, vom Hersteller der verwendeten Firewall zur Verfügung gestellten, Software Updates und Patches in einem zeitnahen Wartungsfenster (siehe unter Punkt 2.1). Bei Cluster-Firewalls wird der Update ohne Unterbruch durchgeführt.
- Anpassungen der Initialkonfiguration, wie zum Beispiel der Änderung von Firewall Regeln, werden nach Prüfung durch das NOC zu Geschäftszeiten ausgeführt. Konfigurationsänderungen ausserhalb der Geschäftszeiten werden gesondert zu den üblichen Stundensätzen verrechnet.
- Green stellt dem Kunden über ein Webportal Traffic Statistiken und Logfiles der eingesetzten Firewalls zur Verfügung. Eine Analyse bzw. Interpretation der Logfiles durch Green ist kostenpflichtig.

Beendigung des Service

- Der Kunde muss innerhalb von 30 Tagen nach Vertragsende sämtliche Ausstattung, die von Green zu Erbringung des Services zur Verfügung gestellt wurde, unaufgefordert und in ordnungsgemässem Zustand 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: a. Falls die Firewall verloren gegangen ist oder nicht innerhalb von 30 Kalendertagen nach Vertragsende zurückgegeben wird. b. Falls die Firewall nicht mehr funktionstüchtig ist.

1.3 Service Parameter

Es gelten die Service Parameter in der folgenden Tabelle.

Ausprägungen	XS	S	M	L
Empfohlene Nutzerzahl	5	20	60	150
Verfügbarkeit ohne Redundanz	99.5%	99.5%	99.5%	99.5%
Verfügbarkeit mit Redundanz	-	99.9%	99.9%	99.9%
VLANs	10	50	100	200
Gleichzeitige Verbindungen	100'000	500'000	2'000'000	3'300'000
Neue Verbindungen pro Sek.	8'500	18'000	40'000	51'000
Mobile VPN	10	30	75	150
Zweigstellen VPNs	10	30	50	100
Schnittstellen 10/100/1000	5	5	8	8
Option Basic Security	✓	✓	✓	✓
Option Total Security	✓	✓	✓	✓
Option MFA für VPN	✓	✓	✓	✓

Weitere Konfigurationen für höhere Bandbreiten sind auf Anfrage verfügbar.

1.3.1 Option Mobile VPN mit Multi-Faktor Authentisierung (MFA)

VPN Verbindungen können mittels Multi-Faktor Authentisierung über eine Mobile Applikation gesichert werden. In der Mobile Applikation stehen drei verschiedene Authentisierungsverfahren zur Verfügung:

- Push Meldung
- One-Time Passwort
- QR Code

Benutzer für den MFA Service können entweder ans NOC per Ticket gemeldet werden oder über ein Active Directory oder LDAP synchronisiert werden.

1.3.2 Option Basic Security

Die Option Basic Security bietet die folgenden Funktionalitäten:

Intrusion Prevention Service (IPS): Dieser Dienst überwacht mithilfe laufend aktualisierter Signaturen den Datenverkehr in allen gängigen Protokollen und bietet Echtzeit-Schutz vor Netzwerkbedrohungen.

Application Control: Mit diesem Feature können Sie den Zugriff auf Anwendungen in Abhängigkeit von Abteilung, Position im Unternehmen und Tageszeit gewähren, verweigern oder einschränken. Anschließend verfolgen Sie in Echtzeit, was von wem aufgerufen wurde.

Web Blocker: Blockiert bösartige Websites automatisch; durch Einsatz granularer Content-Filter-Tools können unangemessene Inhalte blockiert und die Produktivität gesteigert werden.

Spam Blocker: Spam-Erkennung in Echtzeit - so schnell und effektiv, dass er täglich bis zu vier Milliarden Nachrichten überprüfen kann

Gateway Antivirus: Laufend aktualisierte Signaturen identifizieren und blockieren bekannte Spyware, Viren, Trojaner und mehr – einschließlich neuer Varianten bekannter Viren.

Reputation Enabled Defense (RED): Ein cloudbasierter Reputations-Suchdienst, der Benutzer vor bösartigen Websites und Botnets schützt und dabei den Overhead bei der Webverarbeitung erheblich verbessert.

Network Discovery: Es wird eine visuelle Topologie sämtlicher Knoten in Ihrem Netzwerk generiert. So können Sie umgehend riskante Bereiche erkennen.

1.3.3 Option Total Security

Die Option Total Security enthält alle Funktionalitäten der Basic Security Option wie oben beschrieben.

Zusätzlich bietet Total Security die folgenden Funktionalitäten:

APT Blocker – Erweiterter Schutz vor Schadsoftware: Durch Einsatz einer prämierten Sandbox der nächsten Generation werden selbst raffinierteste Attacken erkannt und gestoppt, einschließlich Ransomware und Zero-Day-Angriffen.

Threat Detection and Response (TDR): Setzen Sie Sicherheitsereignisse im Netzwerk und am Endpunkt in Bedrohungsanalysen in Beziehung. Dadurch können potenzielle Angriffe noch früher erkannt, priorisiert und bewertet werden. Sofortmaßnahmen zur Abwehr erfolgen ohne Verzögerung.

DNSWatch: Verringert Infektionen durch Schadsoftware, indem bösartige DNS-Anforderungen blockiert und Benutzer zu Informationen umgeleitet werden, die ihnen Best Practices in puncto Sicherheit vermitteln und betonen, wie wichtig deren Einhaltung ist.

Access Portal: Bietet einen zentralen Zugangspunkt für in der Cloud gehostete Anwendungen und einen sicheren, clientlosen Zugriff auf interne Ressourcen über RDP und SSH.

IntelligentAV: Ist eine signaturlose Anti-Malware-Lösung, die künstliche Intelligenz zur automatischen Erkennung von Schadsoftware einsetzt. Durch Nutzung umfassender statistischer Analysen kann aktuelle und Zero-Day-Schadsoftware in Sekundenschnelle klassifiziert werden. *(Nicht verfügbar für Managed Security XS)*

2. Service Level Agreement

Der Service-Verfügbarkeit ist pro Service definiert und in der jeweiligen Tabelle ersichtlich. Alle in diesem Dokument beschriebenen Services werden durch das Green NOC betrieben und durch den Green Kundendienst supportet.

2.1 Betriebs- und Supportzeiten

Die Betriebszeiten und Supportzeiten sowie die Störnugsannahmezeiten sind in der folgenden Tabelle definiert.

Service Level und Zielwerte	Standard Support	Business Support (24x7)
Betriebszeit	Mo-So 00.00-24.00	Mo-So 00.00-24.00
Wartungsfenster	So 02.00-06.00 Mo 20.00-22.00 oder gemäss vorheriger Ankündigung	So 02.00-06.00 Mo 20.00-22.00 oder gemäss vorheriger Ankündigung
Supportzeit	Mo-Fr 08.00-17.30 ausgenommen an gesetzlichen Feiertagen	Mo-So 00.00-24.00
Störungsannahme	Mo-So 00.00-24.00	Mo-So 00.00-24.00

Support-Tickets können über die folgenden Kanäle eröffnet werden:

- MyGreen Portal: my.greendatacenter.ch
- Per Telefon unter +41 44 330 35 35 während den Kundensupportzeiten
- Formular auf der Webseite: https://www.green.ch/de/kontaktformular

2.2 SLA Verstösse und Gutschriftenregelungen

Kann Green die definierte Verfügbarkeit nicht einhalten, so erkennt der Kunde an und stimmt zu, dass die hier vereinbarten Gutschriften die einzige und ausschliessliche Entschädigung für den Kunden darstellen. Eine Gutschrift wird gewährt, sobald die Serviceverfügbarkeit unterhalb der garantierten Schwellwerte liegt und der Kunde dies mit einem Support-Ticket meldet. Der Ausfall eines Teils eines redundanten Systems wird nicht als Ausfallzeit betrachtet. Nur ein korrekt eröffnetes Ticket kann für die Berechnung von Ausfallzeiten und Gutschriften herangezogen werden.

Die nachfolgende Tabelle zeigt die Gutschriften (pro Jahr) 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. Die Gutschrift bezieht sich jeweils ausschliesslich auf den von der Störung betroffenen Service.

Erreichte Verfügbarkeit ohne Redundanz	Erreichte Verfügbarkeit mit Redundanz	Gutschrift
≥ 99.9%	≥ 99.5%	keine Gutschrift
≥ 99.8%	≥ 99.95%	10% des MRC
≥ 99.7%	≥ 99.9%	20% des MRC
≥ 99.5%	≥ 99.8%	30% des MRC
weniger als 99.5%	Weniger als 99.8%	40% des MRC

Der Kunde hat seine Ansprüche bei Green mittels einer Anfrage unter https://contact.green.ch/ geltend zu machen.

Es wird keine SLA-Gutschrift gewährt, wenn der Service Ausfall oder Unterbruch insgesamt oder zum Teil durch eine der folgenden Ursachen bedingt ist:

1) ein Ausfall von Ausstattung in den Räumlichkeiten des Kunden (falls diese nicht im Besitz von Green ist), des Kundenstandortes (etwa durch Stromausfall) oder von Ausstattung eines Lieferanten des Kunden
2) im Fall von Naturkatastrophen, Terrorangriffen oder anderen Force Majeure-Ereignissen
3) ein Ausfall aufgrund von magnetischen / elektromagnetischen Interferenzen oder elektrischen Feldern
4) jede fahrlässige Handlung oder Unterlassung des Kunden (oder von Mitarbeitenden, Vertretern oder Subunternehmern des Kunden), u.a.:
    a) Verzögerungen bei der Lieferung notwendiger Ausstattung durch den Kunden
    b) Versäumnis, Green zwecks Tests ausreichend Zugang zu den Einrichtungen zu gewähren
    c) Versäumnis, den Zugang zu den Räumlichkeiten des Kunden zu gewähren um es Green zu ermöglichen, ihren Verpflichtungen hinsichtlich des Services nachzukommen
    d) Versäumnis, entsprechende Gegenmassnahmen hinsichtlich des Services zu ergreifen, wie von Green empfohlen, oder Hinderung der Anbieterin, diese selbst durchzuführen
    e) Versäumnis, Redundanzen zu nutzen, wie sie vom Service Level geboten werden
    f) Fahrlässigkeit des Kunden oder absichtliches Fehlverhalten, darunter auch das Versäumnis des Kunden, vereinbarte Verfahren zu befolgen
5) wenn der Kunde den Zugang zum Cage verhindert oder verzögert
6) alle geplanten Wartungszeiträume, wenn der Kunde darüber informiert wurde, und Notfallwartungen, die dazu dienen, künftige Ausfallzeiten zu verhindern

Abschaltung oder Aussetzung des Services durch Green, nachdem der Kunde nicht innerhalb von 90 Tagen ab Rechnungsstellungsdatum bezahlt hat, oder wegen anderer hinreichender Gründe.

3. Rechtliche Bestimmungen

3.1 Zustandekommen des Rechtsverhältnisses

Mit dem Abschluss der Bestellung (bei Erhalt einer unterzeichneten Offerte) kommt zwischen Green und dem Kunden ein Rechtsverhältnis zustande. Die Messung der SLA-Parameter erfolgt ab bestätigter Serviceübergabe.

3.2 Einhaltung der örtlichen Gesetze

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

3.3 Beschränkungen

Alle Entschädigungen für Green 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.

3.4 Verwendung von persönlichen Daten

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

3.5 AGB

Die allgemeinen Geschäftsbedingungen der Anbieterin (Allgemeine Geschäftsbedingungen von Green https://www.green.ch/de/rechtliches/agb) 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. 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.

4. Definitionen

Begriff	Definition
Service Level	festgelegte und messbare Kriterien für die Erbringung einer bestimmten Leistungsqualität durch Green
Service Parameter	angestrebte aber nicht verpflichtende Servicemesswerte
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‘712 Stunden und berechnet sich wie folgt: 1 Jahr 24/7 = 8‘760 h – 48 h Wartungsfenster. Bei redundanter Architektur werden die beiden redundanten Geräte/Einrichtungen zu unterschiedlichen Zeitpunkten gewartet
Supportzeit	Die Zeit in welcher der Kunde einen Kundendienstmitarbeiter oder im Fall von 24x7 Support einen Techniker im Pikettdienst erreichen kann.
Verfügbarkeit	Verfügbarkeit [%] = 100 * ((Betriebszeit - geplante Ausfälle innerhalb der Betriebszeit) / vereinbarte Betriebszeit). Die vereinbarte Betriebszeit enthält nicht die Zeitfenster für geplante Wartungsfenster. Die Verfügbarkeit wird von Green auf der Rechenzentrumsinfrastruktur gewährleistet. Dies beinhaltet folgende Ebenen: Gebäude mit Versorgungsinfrastruktur und Netzwerk. Um die hohen Verfügbarkeit auf der Verbindung zu erreichen, sind auf Endkundenseite die Lösungen ebenfalls entsprechend hochverfügbar zu designen.
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 angekündigt, sofern mehrere Kunden betroffen sind. Kunden werden zudem mindestens 10 Arbeitstage vor dem geplanten Serviceunterbruch infolge Wartungsarbeiten informiert. Green informiert die vom Kunden schriftlich mitgeteilte technische Kontaktstelle per E-Mail über die geplante Serviceunterbrechung und die Art dieses Unterbruchs. Diese Mitteilung ist für alle von diesem Dokument verfolgten Zwecke gültig, unabhängig davon, dass es dem Kunden und/oder seinen Vertretern nicht möglich war, aus irgendeinem Grund diese Mitteilung zu erhalten, so auch aufgrund von E-Mail Systemproblemen oder -ausfällen oder fehlerhaften Kontaktinformationen des Kunden oder weiteren Gründen.
Notfall-Wartungsfenster	Notfall-Wartungsfenster werden mindestens 48 Stunden im Voraus angekündigt und auf status.green.ch aufgeschaltet, sofern mehrere Kunden davon betroffen sind.
Service Access Punkt	Der Service Access Punkt ist der vertraglich vereinbarte Punkt, an dem ein Service dem Kunden bereitgestellt und überwacht wird, und an dem die erbrachten Service Level ausgewiesen werden.