SERVICES DESCRIPTION AND TERMS

(Version February 2021)

Table of Contents

About Aryaka Networks, Inc.

Aryaka delivers a fully managed, end-to-end global SD-WAN service for the cloud-first era. Aryaka's technology integrates multi-cloud connectivity, application optimization, security, last-mile management, and visibility into an SLA-driven OPEX-only solution.

These Services Description and Terms apply to Customer's use of Services and, where specified herein, certain third-party products. The Services are only as expressly described in these Services Description and Terms. Capitalized terms used in these Services Descriptions and Terms but not defined below have the meanings in the Aryaka Networks, Inc. Master Subscription Agreement (the "Agreement"). Aryaka has the right to update these Services Descriptions and Terms from time to time without notice. Notwithstanding the foregoing, Aryaka shall ensure that the Services procured by Customer under the Agreement will not materially adversely deviate from what is agreed by the Parties thereon. The most current version of the Services Descriptions and Terms is set forth at: www.aryaka.com/services-terms/.

Definitions

"Activate" ("Activated" and "Activation" as grammatically appropriate) shall mean Aryaka has completed the connectivity of the Services and the Services are ready for use by the Customer regardless of whether Customer is actually utilizing the Services.
"ANAP" means the Aryaka Network Access Point (ANAP), a device that provides bandwidth optimization, SD-WAN capabilities, and application acceleration over a WAN link that is connected to an Aryaka Network point of presence (AN POP or Aryaka POP).

"Aryaka Network" means Aryaka's geographically distributed network of proprietary servers and software.

"Bursting" allows Customer to use bandwidth greater than the Activated bandwidth capacity.

"Last Mile Circuit" means the physical link (wired or wireless) that is used to connect Customer's premise to the closest Aryaka POP. The physical link may be a direct Layer-2 connection or an Internet Circuit.

"NOC" means network operating center.

"Optimized Capacity" means subscribed bandwidth for all the sites per region.

"Order Form" means the ordering document for purchases hereunder, including addenda thereto, that are entered into between the Parties from time to time.

"Oversubscription" means a Customer has a temporary need to go beyond its subscription units as set forth in the Order Form. Units may be bandwidth, sites, Last Mile Management, and/or High Availability ANAPs.

"POP" means point of presence.

"RFS Date" means the date in which a last mile link has been Activated.

"ROW" means rest of the world.

"SD-WAN" means software-defined wide area network.

"Services" means all services provided by Aryaka and any and all Aryaka downloaded materials (including but not limited to Java Applets, soft-ANAP, and browser/User Interface components), user guides, code, user interface passwords, accessories and other documents, that are purchased by Customer or its Affiliates under a fully executed Order Form, including associated offline components as may be further described in an Order Form or as set forth herein. Third party products provided or made available in connection with Services may be subject to third party terms or other additional terms as set forth herein, and as referenced in the Order Form.

Description of Aryaka SmartServices

The description for Aryaka's Services is as set forth below:

Aryaka SmartServices: The Aryaka SmartServices portfolio provides a cloud-first SD-WAN service that combines a global optimized private network, SD-WAN functionality, L3 VPN connectivity, Cloud Connectivity, WAN Optimization capabilities (including compression, Data Deduplication, Application Acceleration proxies) with cloud-based management, security and visibility using the MyAryaka portal.

The Aryaka SmartServices portfolio consists of the following services ("SmartServices"):

1. Aryaka SmartManage ("SmartManage")
2. Aryaka SmartConnect ("SmartConnect")
3. Aryaka SmartOptimize ("SmartOptimize")
4. Aryaka SmartCloud ("SmartCloud")
5. Aryaka SmartSecure ("SmartSecure")
6. Aryaka SmartInsights ("SmartInsights")

Aryaka SmartServices portfolio is available under two pricing models:

- **Standard pricing model**, including all SmartServices and related subscription pricing plans for Global deployment

scenarios only;

- **Enterprise Flex pricing model** additionally includes, besides Global deployment scenarios, Regional deployment scenarios, Elastic Subscription, and Bandwidth Pooling options, as described below.

Global deployment is used for enterprises operating in multiple regions, with traffic traversing the Aryaka core globally. Regional deployment is used for enterprises operating primarily in a single region, as defined by Aryaka, where traffic traversing the Aryaka core stays within the region.

1. **SmartManage** provides the foundational capabilities required to power the SmartServices platform for deployments at enterprise sites, such as branch offices, stores, service centers, and data centers.

a. **SmartManage-SiteLicense** means the basic SmartManage service required to connect enterprise sites. SmartManage-SiteLicense comes in different tiers (Bring Your Own – "BYO", Small, Medium, and Large). The SmartManage-SiteLicense service includes activating, orchestration, always-on monitoring, and 24x7 support by Aryaka's Global NOCs. Optionally, ANAP hardware and shipment thereof are included. Aryaka's ANAP is a hardware appliance that hosts Aryaka's operating system and, of which some hardware models can host certified virtual machines ("VM"). The ANAP is included and is part of Aryaka SmartServices. The capacity and specification of the optional ANAP hardware included with the SmartManage-SiteLicense differs for each tier and are subject to change. The ANAP 1500 or equivalent is provided with the Small Tier; the ANAP 2600 or equivalent with the Medium Tier; the ANAP 3000 or equivalent with the Large Tier. Global and Regional pricing plans are available for each of the above SmartManage- SiteLicense tiers.

b. **SmartManage-ElasticSubscription-Multiplier** means allowing for the on-demand incremental consumption (also called Elastic Subscription) of Aryaka SmartServices already purchased at any time, including but not limited to incremental bandwidth, additional sites, or any other SmartService. The charges related to Elastic Subscription are billed monthly in arrears, with the option to cancel the Elastic Subscription at any time.

Terms of use of SmartManage Services:

(i) Aryaka reserves the right to match the ANAP device type with the Customer subscription and capabilities desired.

(ii) Aryaka reserves the right to determine the POP for connecting a site to its network based on providing optimal service delivery.

2. **SmartConnect** provides the connectivity services, including first, middle, and last mile, to enterprise sites, such as branch offices, stores, service centers, and data centers. SmartConnect leverages Aryaka's global private core to connect

enterprise sites at high performance with a managed SLA. SmartConnect comes with the option to directly connect enterprise sites securely over the internet using Site-2-Site InternetVPN and/or MPLS, including service management. All SmartConnect services require a SmartManage-SiteLicense, as defined in section 1 above.

The Aryaka SmartConnect services consists of the following features:

- InternetVPN
- MPLS
- Private Core Subscribed Bandwidth ("SBW")
- Inter-Region Multiplier
- Bursting
- High Availability ("HA")
- Last Mile Management
- Last Mile Service

a. **SmartConnect-InternetVPN** means the ability for two sites to communicate securely over the Internet using site-2-site VPN and Aryaka HybridWAN technology.

b. **SmartConnect-MPLS** means the ability for a site-to-peer with a Customer Edge MPLS Router.

c. **SmartConnect-PrivateCore-SBW** means the ability for enterprise sites to connect over Aryaka's middle-mile private core. Pricing of subscribing to Aryaka's SmartConnect-PrivateCore-SBW differs per region, as defined by Aryaka in Table 1 below. Enterprise sites are assigned to one specific Region (as defined below) based on the nearest proximity to one of the Aryaka POPs.

Table 1: Aryaka SmartConnect-PrivateCore-SBW regions are defined as:

Aryaka Regions	Different regions of the world
UCM	USA, Canada, Mexico
EUR	Europe (excluding Russia)
IND	India
APJK	Asia (excluding India, Mainland China)
MLCHN	Mainland China
SAF	South-Africa
SAM	South America
ISR	Israel
DUB	Dubai
AUSNZ	Australia and New Zealand

Customers can subscribe to bandwidth on the Aryaka middle-mile private core on a per-site per-Region basis. Subscribed bandwidth is abbreviated as SBW. Aryaka provides "Global" and "Regional" pricing plans for SmartConnect-PrivateCore-SBW. With a Global bandwidth subscription sites can connect from their respective Aryaka Region to any other Region. Regional bandwidth subscriptions allow sites to connect within their respective Aryaka Region only. Global and Regional pricing tiers are available for most Aryaka Regions.

d. **SmartConnect-InterRegion-Multiplier** allows Regional Sites to communicate to sites in Regions other than the Region in which the site resides. Any traffic sent to or from a Regional Site to any site not located in the same region is InterRegion traffic. All InterRegion traffic is metered and billed at the end of the month based on the Inter Region-Multiplier on the Sales Order Form. Without the InterRegion-Multiplier enabled it is not possible for a Regional Site to send to and receive traffic from any site located outside of its region.

e. **SmartConnect-HighAvailability (HA)** provides additional levels of redundancy for enterprise sites consuming SmartServices.
   - **SmartConnect-ANAP-HA** Redundancy is enabled at the ANAP device level for a site. Should the active ANAP fail as described in the SLA, the redundant ANAP will automatically become active and start routing traffic to the designated Aryaka POP. The redundant ANAP is included in this service. SmartConnect-ANAP-HA is available in different tiers: Small, Medium, and Large.
   - **SmartConnect-POP-HA** Redundancy enabled in case of POP failure and traffic is routed to a backup Aryaka POP. SmartConnect- POP-HA includes a redundant ANAP enabling the rerouting to another Aryaka POP in case of POP failure. SmartConnect-ANAP-HA is available in different tiers: Small, Medium, Large.

f. **Bursting-Multiplier** allows Customers to exceed the purchased SmartConnect-PrivateCore-SBW by up to 50% of the SBW per site with an upper limit of 100 Mbps per site. All Bursting usage, exceeding the SBW, is calculated and billed at the end of the month based on the multiplier on the valid Order Form. The calculation for Bursting usage is based on the 99^{th} percentile of the consumed bandwidth. Customers will pay an additional usage fee, as set forth in the Order Form, for the extra bandwidth used.

g. **SmartConnect-LastMileManagement** gives Customers 24x7 proactive Link Monitoring and management of Customer's last-mile links that connect an Enterprise Site to Aryaka Services. Aryaka's Support team proactively works with the Internet Service Providers of Customers to raise and resolve any issues on the Customer's behalf. Last Mile Management is per last-mile link.

h. **SmartConnect-LastMileService** allows a Customer to purchase first- mile and last-mile Internet circuits from Aryaka. SmartConnect-

LastMileService always comes with SmartConnect-LastMileManagement. SmartConnect-LastMileService is always sold separately from all other SmartServices on a separately processed and signed sales order form.

Terms for use for SmartConnect Enterprise Services:

(i) Customer's purchase of the Optimized Capacity will be on a per region basis and can be allocated only among the sites in a particular Region as defined in Table 1 above.

(ii) Site moves, bandwidth reallocation and add-on relocations are limited to no more than one (1) change per site in any given month.

(iii) If Elastic-Multiplier is not included in the Order Form, Customers shall not exceed the purchased aggregate bandwidth, number of site licenses and/or service limits ("Increase") as set forth in the Order Form. If such Increase does occur, Customer will be notified, in writing, and the Parties shall execute an amended Order Form.

(iv) Any billing schedule based on the deployment dates shall be set forth in the Order Form.

3. **SmartOptimize** provides network and application optimization services, respectively Aryaka TurboNet ("TurboNet") and Aryaka TurboApp ("TurboApp"), require a SmartManage-SiteLicense and SmartConnect-PrivateCore-SBW license.
   a. **SmartOptimize- TurboNet** is a set of network optimization protocols, including Aryaka's multi-segment TCP Optimization and LinkAssure as defined below. TCP Optimization improves Quality of Experience ("QoE") for all applications using TCP, including but not limited to the Internet, file sharing, and streaming applications. LinkAssure mitigates packet loss by various techniques such as link aggregation, load balancing, path selection, and error correction algorithms.
   b. **SmartOptimize-TurboApp** consists of WAN Optimization protocols and application acceleration proxies. WAN Optimization includes Aryaka's patented byte-level data deduplication (byte-caching) algorithm, termed Advanced Redundancy Removal ("ARR"). ARR is a unique unanchored technique that is designed to compress and accelerate WAN traffic and improve network throughput. Aryaka's application proxies such as CIFS, SSL significantly enhance the performance of WAN-intolerant applications by intercepting the connections securely and shortening the feedback loop. SmartOptimize-TurboApp is available in different tiers: Small, Medium, and Large. Global and Regional pricing plans are available for SmartOptimize-TurboApp.

Terms of use for SmartOptimize:

i) Optimization and application compression vary by application behavior and deployment scenario.

ii) If ANAP is not deployed, some of the features included in SmartOptimize- TurboApp will not be available.

4. **SmartCloud** enable multi-cloud networking delivered as-a-service. SmartCloud leverages Aryaka's global private core to connect enterprise sites to SaaS and IaaS.

a. **SmartCloud-Azure-VWAN** This service allows Customers to connect to the Azure VWAN Hub from Aryaka's endpoint (ANAP) over the Internet. Aryaka manages connectivity to Azure VWAN Hub. SmartCloud-Azure- VWAN requires a SmartManage-SiteLicense.

b. **SmartCloud-SaaS-APP-License** is a site license required to connect a SaaS application to Aryaka's global private core.

c. **SmartCloud-IaaS-License** is a site license required to connect an IaaS site (i.e., AWS, Azure) to Aryaka's global private core.

d. **SmartCloud-PrivateCore-SBW** provides the ability for IaaS and SaaS sites to connect over Aryaka's middle-mile private core. SmartCloud-PrivateCore-SBW always requires at least one or more of SmartCloud-SaaS-App-License and/or SmartCloud-IaaS-License. Pricing of subscribing to Aryaka's core for these services differs per Region, as defined below by Aryaka. Hosted locations for IaaS and SaaS are assigned to one specific Region, as defined in the Table 2 below.

Table 2: Aryaka's SmartCloud Regions are as defined below:

Aryaka Regions	**Included POPs**
Mainland China	Beijing, Shanghai
Rest of World	Every other region excluding Mainland China

Terms of use for SmartCloud:

i) Pricing for subscription to Aryaka's core for these SmartCloud Services differs per region, as defined by Aryaka and charged as per the agreed rates in Schedule C "Financial Agreements".

ii) Hosted locations for IaaS and SaaS are assigned to one specific region.

5. **SmartSecure** includes all security capabilities offered on the Aryaka platform, including native security capabilities on the ANAP and certain management functions with respect to select third-party firewall services.

a. **SmartSecure-EdgeEssentials** service includes native security capabilities offered on the ANAP, including a stateful firewall (L3/L4), zones, and micro-segmentation. The stateful firewall delivers north-

south access protection. Zones provide site-segmentation to secure east-west branch traffic. Micro-segmentation enforces end-to-end network isolation between different network segments. SmartSecure-EdgeEssentials is available in different tiers: Small, Medium, and Large.

Terms of use for SmartSecure-EdgeEssentials:

i) Tiering of SmartSecure-EdgeEssentials (Small, Medium, Large) is mapped to the SmartConnect Site license sizing.

b. **SmartSecure-CloudSecurity-ANAP-Connector** service allows Customers to connect to select third-party Cloud Secure Internet Gateway solutions licensed by the Customer from its third-party provided (not by or through Aryaka) (such as Zscaler, Palo Alto Prisma, Check Point CloudGuard connect, Symantec) from an ANAP over the Internet. Aryaka monitors and manages connectivity to the respective Cloud Security providers.

Terms of use for SmartSecure-CloudSecurity-Connector:

i) Procurement of Secure Internet Gateway licensing is not included as part of the offering.

c. **SmartSecure-Hosted-VM-Firewall-Service** provides the ability to host select third party virtual firewalls licensed by Customer from its third- party provider (not by or through Aryaka) (a "Customer-Owned Firewall") on an ANAP. In addition to hosting capability, Aryaka provides VM life cycle management consisting of initial Activation, start, stop and deletion of the Firewall virtual machine as part of this offering. Security policy and configuration management of Firewalls, monitoring of threat events, and procurement of the third-party firewall license are outside the scope of the SmartSecure Hosted-VM-Firewall-Service and are the sole responsibility of the Customer. The SmartSecure-Hosted-VM-Firewall- Service is available in different tiers: Compact and Standard.

Terms of use for SmartSecure-Hosted-VM-Firewall-Service:

i) Hosting capabilities of the SmartSecure Hosted VM Firewall Service and the Activation of the SmartSecure Hosted VM Firewall Service are limited to third-party next-generation Firewall vendor solutions and form factors that are approved and qualified by Aryaka ("Approved Hosted Firewalls"). Currently, Approved Hosted Firewalls are the following:

Approved Hosted Firewalls - Compact: Palo Alto Networks VM-50 and Check Point CloudGuard Edge (1 vCPU form factors).

Approved Hosted Firewalls - Standard: Palo Alto Networks VM-100 and Check Point CloudGuard Edge (2 vCPU form factors).

ii) In order to receive the SmartSecure-Hosted VM Firewall Service, Customer must first acquire appropriate license rights with respect to the Customer-Owned Firewall sufficient to allow Aryaka to host the Customer-Owned Firewall and to access the Customer-Owned Firewall as necessary in connection with its Activation of the SmartSecure-Hosted VM Firewall Service (for example, during set-up to ensure traffic flows are acceptable and interface settings are correct) and provide proof to Aryaka of such license rights. Customer must always thereafter maintain such license rights in effect while receiving the SmartSecure-Hosted VM Firewall Service. Customer represents and warrants to Aryaka that Customer has obtained and will maintain such license rights, and Customer agrees to indemnify and hold harmless (without application of any exclusions of damages or exclusions or limitations of liability in the Agreement), and at Aryaka's request defend, Aryaka and its affiliates, successors and assigns (and its and their officers, directors and employees) from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including, without limitation, attorneys' fees and court costs) which arise out of or relate to Customer's failure to have obtained and maintained such license rights. Customer hereby grants to Aryaka and its affiliates the right and license to host the Customer-Owned Firewall and to access the Customer-Owned Firewall in connection with Aryaka's Activation of the SmartSecure-Hosted VM Firewall Service to Customer.

iii) CUSTOMER ACKNOWLEDGES AND AGREES THAT CUSTOMER-OWNED FIREWALLS ARE NOT AN ARYAKA SERVICE OR PRODUCT AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO CUSTOMER-OWNED FIREWALLS.

d. **SmartSecure-Managed-Firewall-Service** is comprised of the operations management described below by Aryaka of select third-party firewalls licensed by Customer from its third-party provider (not by or through Aryaka) (a "Customer-Owned Firewall") hosted on an ANAP or physical firewall appliances. This service is compromised of the following functions with respect to the Customer-Owned Firewall: (i) configuration and change management, (ii) firewall and network access policy rules as determined and approved by the Customer, (iii) software patching, (iv) 24x7 support, and (v) firewall device health monitoring. This service excludes (x) security policy design, formulation, Firewall configuration migration services, managed

Security Operation Center ("SOC") services, and (y) procurement of the Customer Owned Firewall, each of which is the sole responsibility of the Customer.

Terms of use for SmartSecure-Managed-Firewall Service:

i) The Activation of the SmartSecure Managed Firewall Service is limited to third party next-generation Firewall vendor solutions and form factors that are approved and qualified by Aryaka ("Approved Managed Firewalls"). Currently, Approved Managed Firewalls are the following:

Palo Alto Networks

- Compact Firewall: Palo Alto 200 series, 500 series, VM-50
- Standard Firewall: Palo Alto 800 series, VM-100
- Full Size Firewall: Palo Alto 3000 series

Check Point

- Compact Firewall: CloudGuard Edge 1 vCPU
- Standard Firewall: CloudGuard Edge 2 vCPU, SMB 1530, and SMB 1550
- Full Size Firewall: SMB1570, SMB1590

ii) Full Size Managed Firewall is restricted to physical Firewall appliances only.

iii) Security policy design and formulation and managed SOC (Security Operation Center) are not part of the scope of the SmartSecure Managed Firewall Service offering, and Customer is solely responsible for these functions.

iv) Security posture is determined solely by Customer, and Aryaka will only be acting as the implementor of Customer's security policies under direction and authorization by Customer is solely responsible for its security policies.

v) Day 0 Firewall policy formulation or configuration migration from a third- party Firewall is not part of the scope of SmartSecure Managed Firewall Service

vi) In order to receive SmartSecure-Managed-Firewall Services, Customer must first acquire appropriate license rights with respect to the Customer- Owned Firewall sufficient to allow Aryaka to access, manage and otherwise perform SmartSecure-Managed-Firewall-Services with respect to the Customer-Owned Firewall on behalf of the Customer and provide proof to Aryaka of such license rights. Customer must always thereafter maintain such license rights in effect while receiving the SmartSecure-Managed-

Firewall Services. Customer represents and warrants to Aryaka that Customer has obtained and will maintain such license rights, and Customer agrees to indemnify and hold harmless (without application of any exclusions of damages or exclusions or limitations of liability in the Agreement), and at Aryaka's request defend, Aryaka and its affiliates, successors and assigns (and its and their officers, directors and employees) from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including, without limitation, attorneys' fees and court costs) which arise out of or relate to Customer's failure to have obtained and maintained such license rights. Customer hereby grants to Aryaka and its affiliates the right and license to access, manage and otherwise perform SmartSecure-Managed-Firewall-Services with respect to the Customer-Owned Firewall on behalf of the Customer in connection with the Activation of SmartSecure-Managed-Firewall Services.

vii) CUSTOMER ACKNOWLEDGES AND AGREES THAT CUSTOMER-OWNED FIREWALLS ARE NOT AN ARYAKA SERVICE OR PRODUCT AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO CUSTOMER-OWNED FIREWALLS.

e. **SmartSecure-Check Point-Managed-Firewall-Service** is comprised of the same scope of service as provided for the SmartSecure-Managed- Firewall Service (Section 5.d. above) and further includes a subscription license to Customer for the firewall product(s) offered by Check Point Software Technologies Ltd. ("Check Point") and set forth on the applicable Order Form ("Check Point Products").

Terms of use for SmartSecure-Check Point Managed Firewall Service:

i) Check Point Products are Activated through Aryaka solely for use in connection with the SmartSecure-Check Point Managed Firewall Services and are licensed by Check Point to the Customer pursuant to the Check Point End-User License Agreement located at: **https://www.checkpoint.com/support-services/software-license-agreement-limited-hardware-warranty/** (as may be updated from time to time), as provided by Check Point or which accompany the Check Point Products ("Check Point EULA"). By ordering the Check Point Products pursuant to an order, Customer acknowledges that its use of the Check Point Products is subject to the Check Point EULA. Customer further authorizes Aryaka, acting as agent for Customer, to accept the Check Point EULA on behalf of Customer as part of the installation process of the Check Point Products. Customer's license and use of Check Point Products and Check Point's use of personal information that it collects or generates both

in relation to the Check Point website (www.checkpoint.com) and Check Point Products are subject to the terms of Check Point's Privacy Policy located at **https://www.checkpoint.com/privacy/** (as may be updated from time to time). Customer consents to the use of such personal information in accordance with Check Point Privacy Policy.

Customer further acknowledges and agrees:

ii) Any software contained in the Check Point Products is licensed in object code form only. Customer agrees: (a) not to reverse engineer, decompile or disassemble Check Point Products; (b) not to remove any identification or proprietary notices from Check Point Products; (c) except for back-up copies, not to copy Check Point Products or develop any derivative works thereof; (d) not to develop any other products based on Check Point's intellectual property contained in any Check Point Products; and (e) not to develop methods to enable unauthorized parties to use Check Point Products.

iii) Check Point, and its licensors, own and shall retain all right (except those expressly and unambiguously licensed in the Check Point EULA), title and interest in and to the Check Point Products, including all hardware and software incorporated therein, as well as any accompanying documentation, including but not limited to, all intellectual property rights embodied therein.

iv) EXCEPT FOR ANY PRODUCT WARRANTY MADE BY CHECK POINT DIRECTLY TO CUSTOMER PURSUANT TO THE CHECK POINT EULA, CHECK POINT MAKES NO WARRANTIES WITH RESPECT TO ANY PRODUCT, LICENSE OR SERVICE AND DISCLAIMS ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTIES OF NONINFRINGEMENT. CHECK POINT DOES NOT WARRANT THAT THE CHECK POINT PRODUCT(S) WILL MEET ANY REQUIREMENTS OR THAT THE OPERATION OF CHECK POINT PRODUCTS WILL BE UNINTERRUPTED OR ERROR FREE. ARYAKA MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE CHECK POINT PRODUCTS AND EXPRESSLY DISCLAIMS ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING AS SET FORTH ABOVE.

v) EXCEPT TO THE EXTENT EXPRESSLY SET FORTH IN THE CHECK POINT EULA, CHECK POINT WILL HAVE NO LIABILITY ASSOCIATED WITH THE CHECK POINT PRODUCTS. CHECK POINT PRODUCTS ARE NOT AN ARYAKA SERVICE OR PRODUCT AND ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO CHECK POINT PRODUCTS.

vi) By subscribing to the SmartSecure Check Point Managed Firewall service, Customer is agreeing to a 'non-cancellable' Check Point subscription for the applicable Check Point Products valid for the duration specified in the Order Form.

vii) Security posture is determined solely by Customer, and Aryaka will be only acting as the implementor of Customer's security policies under direction and authorization by Customer. Customer is solely responsible for its security policies.

viii) Check Point Products available in connection with the SmartSecure Check Point Managed Firewall belong to (1) NGTP – Next Gen Threat prevention or (2) NGTX – Next Gen Threat Prevention and Sandboxing subscription categories, based on user selection, as such products are described by Check Point in its Product Datasheet.

ix) Customer will have access rights to the Check Point Products Activated in connection with the SmartSecure Check Point Managed Firewall service only when the Aryaka Managed Firewall Service on Check Point is active. Customer's subscription and license to the Check Point Products will not be valid after discontinuation of SmartSecure-Check Point-Managed-Firewall-Services from Aryaka.

f. **SmartSecure-Managed-CloudGuard Connect-Service (cloud service)** is comprised of a similar scope of service as provided for the SmartSecure-Check Point-Managed-Firewall-Service (Section 5.e. above), this Service is however provided as a cloud solution, delivered on the CloudGuard Connect Product (CGC) offered by Check Point Software Technologies Ltd. ("Check Point") and set forth on the applicable Order Form. This Service includes a subscription license (NGTP/NGTX) to Customer for CheckPoint CloudGuard Connect.

Terms of use for SmartSecure-Managed-CloudGuard-Connect-Service:

i) SmartSecure-Check Point-Managed-CloudGuard-Connect-Service is subject to the same terms and conditions and Terms of Use, as in section 5.e. for **SmartSecure-Check Point-Managed-Firewall-Services.**

ii) SmartSecure-Check Point-Managed-CloudGuard-Connect-Service is licensed based on 'Per user' licensing. A user is identified by a unique identity/userid as captured in the Customer's authentication server or identity provider (such as Microsoft Active Directory, LDAP server, etc.) connecting to the Private Access Service during each month.

iii) SmartSecure-Check Point-Managed-CloudGuard-Connect-Service covers only for users connecting into CloudGuard Connect using (a) ANAP at a Smart Connect Site and (b) Remote user coming in through Aryaka Private Access Client.

iv) Upon Activation of the SmartSecure-Check Point-Managed-CloudGuard-Connect-Service, all user licenses purchased by the Customer in the Order Form will be billed from date of Activation of the Service, or Service commencement date, whichever is earlier.

v) At the end of the month, if the number of unique users connected to the SmartSecure-Check Point-Managed-CloudGuard-Connect-Service has exceeded the committed user count, then the additional usage will be invoiced in arrears. Excess users will be billed based on the Burst multiplier as agreed upon in the Order Form.

vi) Each Remote user using the SmartSecure Private Access client to connect into SmartSecure-Check Point-Managed-CloudGuard-Connect shall have no more than three (3) end point devices connecting to such Service.

vii) SmartSecure-Check Point-Managed-CloudGuard-Connect-Service is not available in MainLand China.

g. **SmartSecure-HighAvailability** provides additional levels of redundancy for Enterprise Sites with a hosted and, optionally, a Managed Firewall Service. SmartSecure-HighAvailability, in all cases, requires SmartConnect-ANAP-HA and/or a SmartConnect-POP-HA.

- SmartSecure-HostedVM-FW-HA: provides the ability to enable firewall redundancy at the virtual machine ("VM") level by hosting a redundant firewall on a redundant ANAP. Should the active hosted firewall fail, the redundant firewall on the redundant ANAP will automatically become the active firewall. The SmartSecure-HostedVM-FW is available in different tiers: Compact and Standard.
- SmartSecure-FirewallManage-HA: provides SmartSecure-FirewallManage for a redundant firewall (hosted on an ANAP or a firewall appliance). SmartSecure-FirewallManage is available in different tiers: Compact, Standard, and Fullsize.
- SmartSecure-Check Point-Managed-Firewall-Services-HA: this service is the same as the SmartSecure-FirewallManage-HA , while

including the subscription to a Check Point Product on and subject to the same Terms of Use set forth above with respect to the Check Point Managed Firewall Service.

Terms of use for SmartSecure-HighAvailability offerings for Managed Firewall Service and Check Point Managed Firewall Service:

i) Definition of Compact, Standard and Full-Size Firewall is based on the definitions under SmartSecure Hosted VM Firewall Service and Managed Firewall Service.

ii) **SmartSecure-HighAvailability** offerings will be an optional add-on on top of SmartSecure services defined in Section 5(c), 5(d) and 5(e), and subject to the terms and conditions and Terms of Use of the above respective sections.

iii) SmartSecure-Check Point-Managed-Firewall-Services-HA is subject to the same terms and conditions and Terms of Use, as in section 5(e) for **SmartSecure-Check Point-Managed-Firewall-Services.**

iv) **SmartSecure-HighAvailability requires SmartConnect-ANAP-HA service.**

h. **SmartSecure-VPN Accelerate** provides accelerated connectivity to virtual private networks ("VPN") for remote and mobile users across Aryaka's private core.

- **SmartSecure-VPN Accelerate VPN-License** privately connects a specific VPN concentrator procured by Customer from its third-party provider (not by or through Aryaka) on the Customer premise to Aryaka's global private core (the origin POP). Per VPN concentrator license, a maximum of eight (8) entry-points (the edge POP) are enabled on the Aryaka Private Core.
- **SmartSecure-VPN Accelerate SBW Worldwide** provides a single worldwide bandwidth pool to connect remote and mobile users to the Customer's VPN concentrator using Aryaka's middle-mile private core.

Terms of Use for SmartSecure-VPN Accelerate:

i) For legal compliance purposes, in the case of Mainland China users of SmartSecure-VPN Accelerate, Aryaka requires that the Customer only tunnel corporate internal traffic over SmartSecure-VPN Accelerate, and not use SmartSecure-VPN Accelerate to tunnel Internet traffic to a VPN concentrator located outside of Mainland China.

i. **SmartSecure Private Access** is a managed VPN as a Service offering from Aryaka that provides the Customers with VPN Gateway infrastructure for enabling remote user access to Customer's Private network over Aryaka Private Core. SmartSecure Private Access is delivered as a Managed Service from Aryaka where Aryaka will provide Customers subscribing to the Service with:

- Access to Globally distributed and redundant VPN Gateways (referred to as Private Access Instances) deployed on Aryaka POPs as a Cloud Service.
- Private Access VPN client application (referred to as Private Access Client) provided to the Customer by Aryaka (which will be deployed by the Customer's end users on their devices such as PCs, laptops and mobile phone).
- 24 X 7 health Monitoring of Private Access Instances and technical support for the Private Access Service.
- Configuration and policy management for Private Access Instances.
- Incident management of Private Access Instances.
- Integration into Aryaka SmartConnect and SmartCloud services (subject to SmartConnect / SmartCloud licensing as required to be purchased by the Customer).

The responsibilities below are retained by the Customer:

1. Distribution and installation of Private Access clients.
2. Ensuring no conflicting VPN Apps/Agents are running on the end-user device that is running the Aryaka Private Access Client, as that may result in interoperability issues and connectivity troubles which will be outside the scope of Aryaka support.
3. Level 1 troubleshooting and support for corporate users of Customer based on the documentation and guidance provided by Aryaka to Customer's IT.

Terms of Use for SmartSecure Private Access:

i) SmartSecure Private Access is licensed based on a 'Per user' licensing. A user is identified by a unique identity/userid as captured in the Customer's authentication server or identity provider (such as Microsoft Active Directory, LDAP server, etc.) connecting to the Private Access Service during each month.

ii) SmartSecure Private Access has two offerings: One offering for Mainland China and one offering for ROW which excludes Mainland China. Customer can have access to Mainland China POPs of Private Access only with a Mainland China Private Access subscription.

iii) SmartSecure Private Access ROW license packaging is available as

different tiers based on the size of the user block Customer has opted to commit in for. Per user pricing of SmartSecure Private Access ROW depends on the committed user count as opted in by the Customer as mentioned in the SOF.

iv) Subject to subsection (v) below, Customer will be billed based on the committed user count in the Order Form.

v) All user licenses purchased by the Customer in the Order Form will be billed from date of Activation of the Service or Service commencement date, whichever is earlier.

vi) At the end of the month, if the number of unique users connected to the SmartSecure Private Access Service has exceeded the committed user count, then the additional usage will be invoiced in arrears. Excess users will be billed based on the Burst multiplier as agreed upon in the Order Form.

vii) Each Customer subscribing to Private Access ROW can be provisioned with up to 10 ROW POPs based on the geographical location of the users. Aryaka reserves the right to provision additional POPs to support larger global deployments at no additional cost to Customer.

viii) Each Customer subscribed to Mainland China SmartSecure Private Access can be provisioned with up to 3 Mainland China POPs.

ix) Each end user using the SmartSecure Private Access Service shall have no more than three (3) end point devices connecting to the Service.

x) Aryaka does not provide Internet Breakout (using a VO, Cloud Security Solution or any other such mechanism) from any of the POPs located outside Mainland China for traffic originating in Mainland China.

xi) Aryaka reserves the right to choose the location and number of SmartSecure Private Access POPs that will be reserved for the Customer users to connect to the Service, while every effort will be undertaken by Aryaka to provide the optimal connectivity and experience to end users subject to resource availability on infrastructure side and compliance needs.

xii) Aryaka reserves the right to throttle the bandwidth usage for any remote user if an abusive pattern of consumption is observed on a consistent basis.

xiii) Aryaka reserves the right to decide what capabilities will be added/ modified/removed from the list of supported capabilities and that will be reflected on the product documentation made available to Customers. Notwithstanding the foregoing, Aryaka shall ensure that the Services procured by Customer under the Agreement will not materially adversely deviate from what is agreed by the Parties thereon.

xiv) The SmartSecure Private Access offering is powered by the remote access technology offering from NCP-engineering, Inc. ("NCP"). By installing the SmartSecure Private Access client (powered by NCP), end users are agreeing to the license agreement with NCP (or affiliate) as specified below:

https://www.ncp-e.com/fileadmin/_NCP/pdf/info/NCP_License_Terms_Client_EN.pdf

xv) CUSTOMER ACKNOWLEDGES AND AGREES THAT NCP TECHNOLOGY AND PRODUCT OFFERINGS ARE THIRD PARTY COMPONENTS AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO NCP.

6. SmartInsights Service is delivered via the MyAryaka portal providing visibility into the WAN health, performance, utilization, and entitlements. The MyAryaka portal provides self-servicing options for Service changes and configuration requests and tracking of support tickets.

Description Aryaka SmartCDN (IADS)

In addition to the aforementioned portfolio of SmartServices, Aryaka separately provides an Aryaka SmartCDN service.

Aryaka SmartCDN provides IP Application Delivery-as-a-Service ("IADS") as a usage-based service. IADS is used for accelerating any web or IP-based public applications, such as web servers and VDI farms, over Aryaka's global network using capabilities, such as TCP optimization, caching, and compression with cloud-based management and visibility, when using the MyAryaka portal.

Terms of use of Aryaka SmartCDN Services (IADS):

(i) Aryaka reserves the right to choose the edge POPs and Origin POPs to deliver the Services on its global network.

(ii) Aryaka reserves the right to limit the maximum data transfer rates achieved over the Aryaka Network based on the aggregate commits purchased.

Description of Last Mile Circuits

In addition to the aforementioned Services, Aryaka separately provides Last Mile Circuits.

Last Mile Circuit is the physical link (wired or wireless) that is used to connect Customer's premise to the closest Aryaka POP. The physical link may be a direct

Layer-2 connection or an Internet Circuit. The type of the Last Mile Circuit will be specified in the Order Form.

Terms of use for Last Mile Circuits:

(i) All charges for each Last Mile Circuit Service will commence when each particular circuit is Activated and ready for service, and the ready for service date ("RFS Date") is communicated to You. Such charges shall commence as set forth in the preceding sentence regardless of whether or when other Aryaka Services are Activated.

(ii) Upon completion of the site survey of Your premises, the particular third-party service provider will advise Aryaka if there will be: (a) additional charges for providing service above the charges previously quoted to You. In any such case, Aryaka will propose the associated cost changes to You; (b) "no service available" or equivalent, or if a redesign is required. Aryaka will then undertake to locate an alternate provider for the Last Mile Circuit. Aryaka will propose the alternate Last Mile Circuit together with the associated cost changes to You.

(iii) Customer has the right to reject the proposed charges within five (5) days of receipt of the proposal. If Customer rejects the proposal, then the original order for the Last Mile Circuit will be automatically cancelled with no early termination fees. The proposal will be considered accepted if not so rejected by Customer within the 5-day period.

(iv) All start or completion dates provided at the time of signing the Last Mile Circuit order are advisory and non-binding. The final service activation date will be provided after the third-party service provider has completed the site survey of Customer's premises.

(v) Aryaka will not be responsible for delays in (a) completion of internal wiring, (b) You responding to requests for additional information, or (c) gaining access to Customer's premises to have the service installed.

(vi) All Last Mile Circuit quotes are based on providing connectivity to the Minimum Point Of Entrance (MPOE). All wiring from the MPOE to Customer's facilities or equipment is the responsibility of Customer. Upon written request from Customer, Aryaka will advise whether it has the capability to provide the internal wiring, together with an estimate of the associated extra cost.

(vii) For all Last Mile Circuits, the Mean Time to Repair and the Service Availability Service Level Agreement will, as provided by (or limited by, as the case may be), the particular third-party service provider, depend upon the type of circuit that is ordered.

Description of Link Monitoring

In addition to the aforementioned Services, Aryaka separately provides Link Monitoring.

Link Monitoring means the monitoring by Aryaka of Customer's Last Mile Circuit link to be conducted on a 24x7x365 basis, including reports and support as specified herein. Link Monitoring shall be included with the Last Mile Circuit if and as specified in the Order Form together with a letter of authorization from Customer.

Terms of use for Link Monitoring

Link Monitoring. If Aryaka receives an executed Letter of Authorization (LOA) from Customer, Aryaka will proceed with the following link monitoring services as part of the Last Mile Circuit Management:

(i) Monitor the last mile link 24x7x365 by pinging between Aryaka's POP and the end-user device.

(ii) Pings occur once per second and Aryaka reports average packet loss and latency by the minute.

(iii) Aryaka monitoring team to be alerted when the rolling average for either latency or packet loss exceeds the applicable thresholds set forth in the SLA.

(iv) As specified in the Last Mile Management SLA terms, in the event of an incident where latency or packet loss exceed the applicable thresholds, or the last mile tunnel becomes unavailable, Aryaka will follow up with Customer, Customer's Internet Service Provider (ISP), or both.

(v) In working with each ISP, Aryaka will comply with any incident resolution priority or escalation matrix provided by the ISP.
Aryaka disclaims responsibility for any ISP failing to restore service in accordance with the ISP's SLA. Aryaka is not responsible for procuring ISP links or other non-Aryaka links for You.

Service Usage Calculations

With a few exceptions, for most of the above Services, the service usage calculation for billing purposes is based on the committed subscribed quantity, as stated on the Order Form. This section details the service usage calculation methods for usage-based Services where billing is based on actual usage, and not solely on the committed subscribed quantity.

Service usage calculation for Elastic Subscriptions
Elastic Subscriptions for all Aryaka Services are allowed when the SmartManage-ElasticSubscription-Multiplier option is present on the Order Form and has been elected by the Customer. Any actual Activated quantity of a Service exceeding the subscribed quantity for the Service is defined as Oversubscription usage. The unit price for each unit of oversubscription usage is calculated as the product of the SmartManage-ElasticSubscription-Multiplier and the unit price for the Service, each as set forth in the Order Form.

Service usage calculation for InterRegion Traffic
InterRegion traffic for SmartConnect-PrivateCore-SBW with regional pricing is allowed when the SmartConnect-InterRegion-Multiplier option is present on the Order Form and has been elected by the Customer. InterRegion traffic for a Regional Site is the max of the 99th percentile of the traffic sent to or received from the Regional Site to all other sites that are not in the same Region. InterRegion traffic for a Region is the sum of the InterRegion traffic for all the Regional Sites in that Region. The unit price for InterRegion traffic is calculated as the product of the SmartConnect-InterRegion-Multiplier and the unit price, per the Regional pricing tier, for the Aryaka SmartConnect-PrivateCore-SBW Service, each as set forth in the Order Form.

Service usage calculation for Bursting
Bursting for SmartConnect-PrivateCore-SBW is allowed when the SmartConnect-Bursting-Multiplier option is present on the Order Form and has been elected by the Customer. Bursting is the actual bandwidth usage above the subscribed bandwidth for SmartConnect-PrivateCore-SBW as set forth in the Order Form. Bandwidth Usage for a site is the max of the 99th percentile for the traffic sent or received over Aryaka's private core. For Regional sites, InterRegion traffic is not accounted for in the Bandwidth Usage. For the Enterprise Flex pricing model, Bursting is calculated for each Region by subtracting the aggregate subscribed bandwidth from the aggregate bandwidth usage for all the sites in that Region. For the Standard pricing model, Bursting is calculated for each site by subtracting the subscribed bandwidth from the bandwidth Usage. The unit price for Bursting is calculated as the product of the SmartConnect-Bursting-Multiplier and the unit price for the Aryaka SmartConnect-PrivateCore-SBW service, each as set forth in the Order Form.

Note: For all the above usage-based services, in the case of multiple Order Forms, the unit price and multiplier are determined by the latest Order Form.