verizon

SESSION BORDER CONTROLLER AS A SERVICE +

1. GENERAL

1.1 **Service Definition.** Session Border Controller as a Service (SBCaaS) is a virtual network service that provides Session Border Controller (SBC) services on cloud-based Virtual Machines (VMs) in the Hosted Network Service (HNS) environment. To the extent terms are contained below, such terms will apply to SBCaaS.

1.2 **Standard Service Features.** These service terms include a description of the technical and operational requirements of SBCaaS to be provided by Verizon.

2. SERVICE ELEMENTS

2.1 **Service Sizing.** Customer will choose the maximum number of concurrent calls (CCLs) per Session Border Controller. The CCL sizing range is specified in the table below. Verizon will work with Customer to help Customer identify and select an appropriate number of CLLs per SBC based on Customer's intended use.

Minimum Concurrent Calls (CCLs) Per SBC	25
Maximum Concurrent Calls (CCLs) Per SBC	5000

2.2 **Session Border Controller.** With SBCaaS, Verizon will provide an SBC hosted by Verizon and supported by the HNS platform. The SBC provided to Customer can provide the following features:

Advanced Call Routing Engine	Support for advanced routing features including routing based on SIP username/URL routing, route prioritization including time of day, day of week, call screening and blocking
Basic Call Routing Engine	Call routing based on called and calling party, trunk groups, codec filtering and call route prioritization

Media Services	Border-based media control services such as, Network Address Translation (NAT) and Network Address Port Translation (NAPT) traversal, media anchoring, transcoding, DTMF detection and insertion
Protocol Interworking	SIP/H.323, IPv4-IPv6 Interworking
Quality of Service (QoS)	QoS network and prioritization policies including bandwidth management, Type of Service (ToS) packet marking, and call admission control
Security	Network protection including session aware firewall functionality, Denial of Service (DoS) and Distributed Denial of Service (DDoS) protection, topology hiding, rogue RTP protection, malformed packet protection, media encryption (SRTP) and signaling encryption (IPsec, TLS)
Security for VoIP Traffic	Standards based security services for Real Time Communications (RTC) traffic, e.g., RTP, TLS, etc.
Signaling Services	Support for industry standard signaling protocols, such as SIP, SIP I/T and H.323 in addition to protocol interworking

2.3 **Session Border Controller Deployment and Configuration.** Verizon will create a Customer design document (CDD) based on a written statement of requirements (SOR) agreed to by Customer. Verizon will activate, monitor, and manage the Customer Network as designed in the CDD. If Verizon deems the design to be nonstandard, a separate statement of work will be required.

2.4 **Full Management Service Level.** Verizon will provide management for SBCaaS as follows:

- **Notification.** Verizon provides incident notification for SBCaaS. Verizon will create a trouble ticket and attempt to notify Customer's designated point of contact via e-mail or automated phone message within 15 minutes of Verizon's determination of an SBCaaS failure on the HNS.
- **Managed Services Customer Portal.** The managed services portal, available via the Verizon Enterprise Center (VEC), is an Internet web portal that provides a view of Customer network information 24 hours a day, seven days a week. Customer is limited to 10 user accounts and is responsible for ensuring that all users understand and comply with Verizon's confidentiality requirements. The VEC can be accessed at: www.verizon.com/business/
- **Digital Connect API Gateway.** Verizon will provide access to the Digital Connect API Gateway (https://digitalconnect.verizon.com) (API Gateway) so Customer can develop an application program interface (API) to allow for eBonding to Verizon for services such as incident management or change management.
- **Change Management Activities.** "Standard Change Management" activities shown on the VEC are provided at no additional charge.
- **Monitoring and Management.** Verizon provides proactive monitoring of all SBCs 24 hours a day, seven days a week. Verizon will monitor the SBCs via use of the simple network management protocol (SNMP) and internet control message protocol (ICMP, commonly called a "ping") for status and error conditions (e.g., SNMP trap messages). Management of SBCaaS includes management of applicable SBCaaS software licenses.
- **SBCaaS Patches and Upgrades.** Verizon will provide relevant software patches as provided by the SBC manufacturer from time to time for installation during a scheduled maintenance period. Verizon will provide relevant software upgrades as provided by the SBC manufacturer from time to time at Verizon's initiation or at Customer's request.

verizon

3. SUPPLEMENTAL TERMS

3.1 Verizon Responsibilities

3.1.1 **Demarcation.** Verizon will provide the demarcation of SBCaaS at HNS service edge.

3.2 Customer Responsibilities

3.2.1 **IP Addresses.** Verizon will designate IP addresses for use with SBCaaS. Customer will not use non-approved IP addressing on SBCaaS. Verizon also reserves the right to use border gateway protocol (BGP) routing when SBCaaS terminates Verizon transport.

3.2.2 **Third Party Providers.**

3.2.2.1 **Generally.** Unless otherwise agreed, Customer is responsible for: (a) the selection, compatibility, implementation and onboarding of all components of its unified communications solution provided by a third party provider (TPP); and (b) compliance with any laws and regulations that are applicable in any region or country where a TPP unified communications solution is provisioned by Customer. Verizon is not liable for any of Customer's choices relating to retention periods, access rights or use of any call recordings. Verizon is not responsible for any Customer activity within SBCaaS or any adverse impact that is caused by such activity.

3.2.2.2 **Third Party Unified Communications Providers (TPUC).** Customer must use Verizon-approved TPUC platforms (e.g., MS Teams). Customer must obtain any signed digital certificates required for encrypted connections to the TPUC and manage the TPUC relationship including certificate renewals. Customer is responsible to provide Verizon with original digital certificates and any renewals thereof through the VEC.

3.2.3 **Customer Notifications.** Customer shall report detected SBCaaS failures and provide information to the Verizon Customer Service Center within twenty-four hours.

3.2.4 **Back Up.** Customer is responsible for the adequacy of any duplication or documentation for its electronic files at all times. Neither Verizon nor its designees are responsible or liable for Customer's failure to duplicate or document files or for data or files lost during the performance of SBCaaS.

3.2.5 **Reports.** All copies of any reports, recommendations, documentation, VEC printouts, or other materials in any media form provided to Customer by Verizon will be treated by Customer as Verizon Confidential Information. Customer Confidential Information, if embedded in the above, shall continue to be treated as Customer Confidential Information.

3.2.6 **VEC or API Gateway User Names and Passwords.** Customer must immediately notify Verizon upon learning of any unauthorized use of Customer's login credentials. Customer is responsible for all activities and Charges incurred through the use of the compromised login credentials.

3.2.7 **SIP Trunking Prohibitions.** Customer warrants it is not aware of any prohibition preventing interconnection between Verizon Facilities and their third party provided SIP Trunking provider. Customer also acknowledges that the country from which SBCaaS is provided may differ to the country of the associated SIP Trunking service.

3.2.8 **Restriction on Encryption Functionality in India.** The use of encryption shall be governed by the government policy/rules made under the Information Technology Act, 2000. Customer will not employ bulk encryption equipment in connection with Verizon Facilities in India.

3.2.9 **Restriction on Public Cloud in India.** In India, use of SBC located in a public cloud must be via infrastructure located in India.

3.2.10 **India Compliance.** This clause applies if SBCaaS will be accessed from India. Customer acknowledges compliance with applicable regulations in India with regard to the use of any of unified communications service, associated connectivity or SIP Trunking services is the responsibility of Customer and the provider of those services. Such compliances include requirements as applicable to other service providers (OSPs) in India.

3.2.11 **VoIP Restrictions.** Customer acknowledges that a number of jurisdictions impose restrictions and/or licensing or registration conditions on VoIP transmission over the Verizon Facilities. To the extent such regulations apply, Customer shall comply with those regulations and indemnify, defend, and hold Verizon harmless for any claims arising from Customer's violation of such regulations thereof.

4. **SERVICE LEVEL AGREEMENT.** The SBCaaS service level agreement (SLA) may be found at the following URL: www.verizon.com/business/service_guide/reg/cp-session-border-controller-as-a-service-sla.pdf

5. **FINANCIAL TERMS**

5.1 **Rates and Charges.** Customer will pay the monthly recurring charges (MRCs) for SBCaaS as specified in the applicable Order and at the following URL: www.verizon.com/business/service_guide/reg/applicable_charges_toc.htm and Customer's Service Commitment will be as specified in the applicable Order.

5.1.1 Customer will pay additional MRCs for any optional services or features ordered by Customer as shown in an Order.

5.1.2 Verizon may use various tools and processes to try to identify potential fraudulent use of the Service, however Customer remains solely responsible for protecting against any fraudulent use. Customer is responsible for controlling access to, and the use of its telecommunications equipment and facilities. Fraudulent use indicators include unusual call patterns or call volume variation. If Verizon determines or reasonably believes that there is fraudulent use, Verizon may take immediate action that is reasonably necessary to prevent such use, including suspending the affected Services in accordance with the Service Suspension clause in the Master Terms. Verizon's actions are discretionary and there is no guarantee of prevention or detection of fraud. Customer is responsible for all Charges for the Service, even if incurred as a result of fraudulent or unauthorized use, unless such fraudulent usage results directly from Verizon's gross negligence or intentional misconduct.