Release Notes - Rev. 11.9

Dialogic® BorderNet™ Session Border Controller (SBC)

Release 3.8.1

September 2019

Table of Contents

Copyright and Legal Notice

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see **http://www.dialogic.com/company/terms-of-use.aspx** for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Corporation at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 3300 Boulevard de la Côte-Vertu, Suite 112, Montreal, Quebec, Canada H4R 1P8.

Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.

Dialogic, Dialogic Pro, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, PowerVille, PowerNova, MSaaS, ControlSwitch, I-Gate, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, and NaturalAccess, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Corporation and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 3300 Boulevard de la Côte-Vertu, Suite 112, Montreal, Quebec, Canada H4R 1P8. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Document History

Revision	Release date	Notes
11.9	September 2019	Release 3.8.1 (build 3.8.1-285) – Editorial Release 3.8.0 removed
11.8	September 2019	Release 3.8.1 (build 3.8.1-285)
11.7	September 2019	Release 3.8.1 (build 3.8.1-275)
11.6	August 2019	Release 3.8.1 (build 3.8.1-240) - Update
11.5	August 2019	Release 3.8.1 (build 3.8.1-240)
11.4	August 2019	Release 3.8.1 (build 3.8.1-221) – TLS 1.2 additional Cipher Suite
11.3	August 2019	Release 3.8.1 (build 3.8.1-221)
11.2	July 2019	Release 3.8.1 (build 3.8.1-204)
11.1	June 2019	Release 3.8.1 (build 3.8.1-172)
11.0	June 2019	Release 3.8.1 (build 3.8.1-167)

1. Introduction

1.1 Purpose of this Document

This Release Notes document is for Release 3.8.1 of the Dialogic® BorderNet™ Session Border Controller (SBC).

1.2 Glossary

For the purposes of this document the following abbreviations apply:

Abbreviation	Meaning
AWS	Amazon Web Services
CIS	Center for Internet Security
CTI	Cyber Threat Intelligence
EC2	Elastic Computing Cloud
EMS	Element Management System
EVRC	Enhanced Variable Rate Codec
EVS	Enhanced Voice Services
HA	High Availability
KVM	Kernel-based Virtual Machine
LI	Lawful Interception
LBO	Local Break Out
LDAP	Lightweight Directory Access Protocol
NAS	A Network Access Server
NWL	Network Wide Licensing
OMR	Optimal Media Routing
RADIUS	Remote Authentication Dial-In User Service
SBC	Session Border Controller
SNMP	Simple Network Management Protocol
SR-IOV	Single Root I/O Virtualization
TRF	Transit & Routing Function
VPC	Virtual Private Cloud

1.3 Upgrade Path

Release	Supported Upgrade Path
3.8.0-250 or higher 3.7.6-228	3.8.1-xxx

1.4 Upgrade Notes

- Upgrade is supported only for BorderNet SBCs, which support Centos 7.4 and on.
- For BorderNet SBCs with Centos 7.3, run the Centos 7.3 to Centos 7.4 migration procedure.
- In release 3.8.1, the BorderNet GCC is upgraded to version 9.1 automatically.
- Upgrade from an older release does not install the SBC's hardening (see 2.7) (hardening is installed only through a fresh SBC installation or after re-deployment).
- The two Known Issues: TFS#22211 and TFS#26676 can happen after the upgrade. Please check section 4.1 (SBC Known Issues) for workaround.

- **Notes:**

  1 - NTP synchronization is mandatory for High Availability, Geo Redundancy, and NWL deployments.

1.5 Rollback Notes

- Rollback procedure removes the new GCC version 9.1.

1.6 Contact Us

For a list of Dialogic locations and offices, please visit: **https://www.dialogic.com/contact**

2. New Features

2.1 Geo Redundancy

BorderNet SBC supports geographical high availability on any deployment mode: bare metal, virtualized or cloud.

The traffic flows normally between a peer and an active BorderNet SBC. Upon the active platform's failure, the standby that can reside on a remote network or site, detects the failure. The standby turns to active and sends Re-Invite/Update to the peer, enabling the traffic to flow between the peer and the newly active BorderNet SBC.

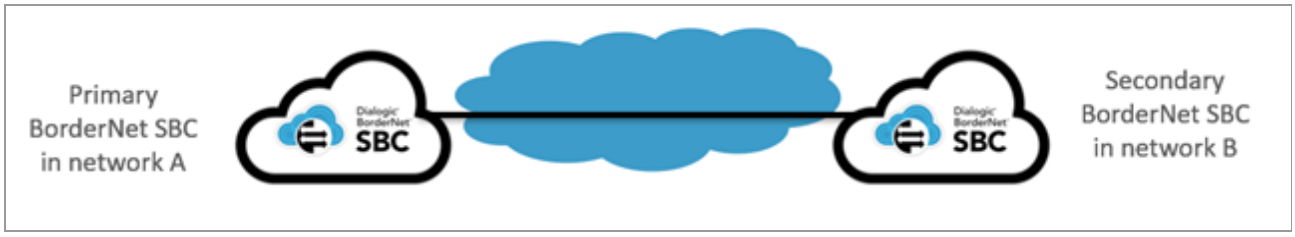

Figure 1: BorderNet in Geo-Redundancy Mode

In this deployment, the BorderNets have the same set of IP addresses (as in the High Availability (HA) mode), and an additional *HA link Gateway IP address*. Since each platform resides on a different network, this address enables the communication between the active and the standby BorderNet SBCs:

- Management IP address
- Utility IP address
- HA link IP address
- HA link Gateway IP address
- Traffic IP addresses

2.2 Network Wide Licensing (NWL)

The Network Wide Licensing (NWL) feature enables a reliable license-sharing solution for a group of BorderNet's on the same network, managed by the Dialogic BorderNet EMS.

The operational flow of the NWL is as follows:

- The original licensing code is provisioned to a license-generating server, to the EMS (license server), and the BorderNet SBC (license client).
- The EMS requests the license-file from the license-generating server, using the provisioned code.
- The server sends back the license-file, which includes the feature list of the BorderNet SBCs.
- The BorderNet SBC retrieves the license file from the EMS.
- The BorderNet checks, using the feature list, the availability of each feature, and in case of features with session quantitative values, it checks their limits' violation, and acts accordingly.

- The BorderNet SBC activates a provisioned timer (RefreshFeatureList) and maintains a keep-alive mechanism towards the EMS.
- Since this feature is a license-sharing solution, each BorderNet is granted with a chunk of sessions (out of the total available sessions), in order to utilize the network capacity.

NWL is agnostic to different deployment modes (hardware, virtualized and cloud), and operating systems (any Linux flavor BorderNet SBC supports).

This feature is managed through the EMS and the BorderNet SBC GUI. For more information, see the BorderNet SBC Provisioning Guide, and BorderNet SBC EMS Users Guide documents.

2.3 LDAP

BorderNet SBC supports the Lightweight Directory Access Protocol (LDAP), in order to allow access to remote resources, regardless to the network location.

Currently BorderNet supports TCP non-secure connection to communicate with the LDAP server, using the default port “389”. TLS/LDAPS secure connection will be supported in future releases.

Customized role attribute is not required, since the role definition is based on group-roles and the user’s association to a role group.

For details on the configuration, see the BorderNet SBC Provisioning Guide document.

2.4 SNMPv3 Trap

The BorderNet SBC uses the Simple Network Management Protocol (SNMP) v3 to send alarm traps to external SNMP managers, in a secured mechanism.

In this release, Get Request is not supported.

For details on the SNMP configuration, see the BorderNet SBC Provisioning Guide document.

2.5 RADIUS User Authentication

Remote Authentication Dial-In User Service (RADIUS) is designed to deliver Authorization, Authentication, and Accounting (AAA) services for dial-up internet. BorderNet SBC uses RADIUS for user authentication and authorization.

For the authentication process, the BoderNet SBC sends the username and the password of the user to the Radius Server. The RADIUS sever confirms and authorizes the user, by providing a privilege (user-groups).

The shared key and the users information and privillages should be agreed and synchronized between the Radius Server, and the BorderNet SBC.

Primary and alternate RADIUS servers use the same synchronized information and the same UDP port. Switching between the primary and alternate RADIUS servers does not require rebuilding the RADIUS message with a new shared secret.

The authentication methods: PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol) are supported in this release.

The Radius authentication parameters are provisioned, using the RADIUS Authentication option in the System drop-down menu (in the BorderNet SBC GUI).Note: Due to TFS#24757, CHAP Authentication Method is not supported and therefore it is removed from GUI.

2.6 Scale In/Out on Amazon

The BorderNet SBC can be scaled out and in (horizontal scaling) according to the system requirements.

- Scale In refers to the process in which a set of servers are removed (brought down), leaving a lower number of servers (or even a single one) in an operational state.
- Scale Out refers to the addition of servers to the existing server or multiple servers. It requires support of a distributed architecture, where the workload is balanced between the different servers. System scalability should be designed, and it is not provided automatically. Scale out is generally more challenging than Scaling In.

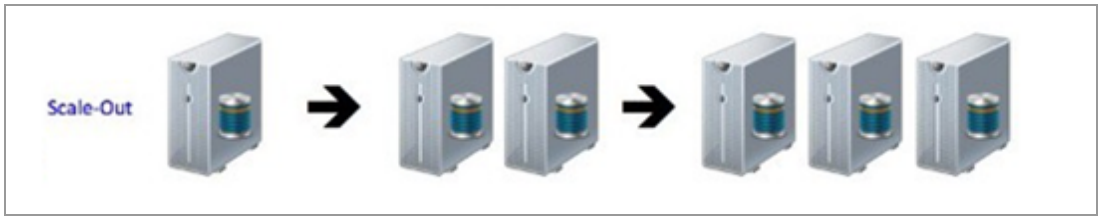

Figure 2: Scale-Out

Scale In/Out on the BorderNet SBC dictates the following restrictions:

- Available only in Amazon (AWS) mode.
- Only the *concurrent sessions* indicator is used as the threshold parameter for scaling decisions.
- Abnormal scenarios, such as cases in which a new instance is not able to become active or is not responsive, are not handled in the current phase.
- Run time configuration is not currently supported, and will be implemented after the full integration of the EMS.
- New instances are not yet configurable. Configuration modification is enabled in a full scale-in state where only the redirect BorderNet is up.
- In the current phase, only the first redirect can be deployed in a High Availability configuration. All new instances are deployed as standalones.

The Scale In and Scale Out actions are directly controlled from the GUI through the Edit Scalability Profile window. For details, see the BorderNet SBC Provisioning Guide document.

2.7 Security & Hardening

The Release 3.8.1 includes the strengthening of the operating system and application according to the Cyber Threat Intelligence (CTI) standard for internet operations.

Based on the Center for Internet Security (CIS) hardening recommendations, to establish a secure configuration posture this process requires the completion of the following tests:

1	Initial Setup	• Filesystem Configuration • Configure Software Updates • Filesystem Integrity Checking • Secure Boot Settings • Additional Process Hardening • Mandatory Access Control • Warning Banners • Ensure updates, patches, and additional security software are installed
2	Services	• INET Services • Special Purpose Services • Service Clients
3	Network Configuration	• Network Parameters (Host Only) • Network Parameters (Host and Router) • IPv6 • TCP Wrappers • Uncommon Network Protocols • Firewall Configuration • Ensure wireless interfaces are disabled
4	Logging and Auditing	• Configure System Accounting (audited) • Configure Logging • Ensure logrotate is configured
5	Access, Authentication and Authorization	• Configure cron • SSH Server Configuration • Configure PAM • User Accounts and Environment • Ensure root login is restricted to system console • Ensure access to the su command is restricted
6	System Maintenance	• System File Permissions • User and Group Settings

2.8 EVS and EVRC

Release 3.8.1 supports the Enhanced Voice Services (EVS) and the Enhanced Variable Rate Codec (EVRC) codecs and the transcoding operations associated with these codecs.

- EVS is a wideband speech audio coding standard, offering up to 20 kHz audio bandwidth and robustness to delay, jitter, and packet loss due to its channel-aware coding and improved packet loss concealment.
- EVRC is a speech codec used in CDMA networks. It was developed to replace the QCELP vocoder, which used more bandwidth on the carrier's network. So EVRC's primary goal is to offer the mobile carriers with capacity without increasing the bandwidth or the wireless spectrum. EVRC uses RCELP technology, which improves speech quality using lower bit rates.

2.9 EMS New XML Configuration

The EMS manages multiple BorderNet SBCs, and if present, the provisioning is performed only through the EMS.

Release 3.8.1 applies some modifications for a generalized configuration-synchronization between the BorderNet SBCs and the EMS.

The following parameters use a BorderNet-specific provisioning which prevents a general provisioning:

- Port Allocation parameter in media profile provisioning uses a BorderNet-specific VLAN name.
- Advanced Policy and Sip-Rec Peer parameters in service profile provisioning use BorderNet-specific interface/peers.

In order to generalize the media profile and service profile configurations at the EMS level, the Port allocation, the Advanced Policy, and Sip-Rec Peer should be removed from the media and service profiles settings, and then added at the Peer & Interface level.

Upgrade Procedure handles the data migration of the service profile to the Interface/Peer.

2.10 EMS Provisioning

In release 3.8.1 the following BorderNet SBC status values have been added to the EMS:

- InSync: The EMS and BorderNet SBC’s configurations are synchronized.
- Not InSync: The EMS and BorderNet SBC’s configurations are not synchronized. The EMS has failed to reach the BorderNet SBC.
- SyncInProgress: The BorderNet SBC is being synchronized.
- New Device: A new BorderNet SBC, with no content, has been added to the EMS.
- Unmanageable: Old version (older than 3.8.0) in BorderNet SBC does not allow the full configuration.
- Corrupted: The BorderNet SBC has experienced one of the following:
    - Added to the EMS with its own initial data
    - Is out of synchronization with the EMS because of a configuration issue
    - Upgraded from a not EMS-supported version to a supported one.

The provisioning of the following profiles are enabled on the EMS:

- Media Profile
- Service Profile
- Security Profile
- Parameter Profile
- SRTP Profile
- Number Translation Profile
- Criteria Set Data
- Directory Lookups
- Time Band Profile
- Global Variable Profile
- SIP Profiler
- ISUP Profiler

2.11 Denial of Service Protection for Access Public Interface

The current denial of service protection is limited to a specific peer/s associated to SIP interface.

This limitation caused severe security breach concerning the Access Public SIP interface, serving multiple end-clients. When one of the clients attacked the SIP interface, the other clients' services, attached to the same SIP interface, were effected.

The new implementation protects against the INVITE and REGISTER flooding attacks, addresses only the un-configured peers, which are connected to an Access Public SIP interface.

Both scenarios affect the black list by preventing the source IP packets to reach the signaling stack.

Once a client's specific IP address is blocked, other clients with different IP addresses, communicating with the same Access Public SIP interface, are granted with regular service.

For details on provisioning, see the Provisioning Guide document.

2.12 TLS 1.2 additional Cipher Suite

The Cipher suites: DHE_RSA_WITH_AES_128_CBC_SHA, and RSA_WITH_AES_128_CBC_SHA_256 for the TLS 1.2 support are added to the following BorderNet SBC's current cipher suites:

- RSA_WITH_AES_256_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_128_MD5
- RSA_WITH_NULL_SHA
- RSA_WITH_NULL_MD5

For details on provisioning, see the Provisioning Guide document.

3. Resolved Issues

3.1 Build 3.8.1-285

The following table lists all the resolved problems for Build 3.8.1–285

	Defect	Issue	Fix Description
1	26195	Mirroring Cores on Standby SBC	When context id or other channel allocation fails in standby, then transcoding allocation is inserted to the map and deleted without removing its entry from the map. This scenario is handled gracefully by removing the entry from the transcoding map when Transcoding Allocation is deleted.
2	26253	BorderNet crashes with error "RVSIP_CALL_LEG_STATE", when receiving incoming INVITE with P-Charging Vector in specific format.	When handling the Incoming Leg State modification in case of mTopologyTransp = false, the mp Peer Data was NULL. To fix this problem, mpPeerData's value is checked first. This correction has been added also when topology transparency is enabled.
3	26568	SIPGW Cores Periodically	When there are 3 or more dialogs created and 503 is received from the egress, in a race condition, a new dialog, creating 18x was being processed even after receiving 503. The scenario has been handled by ensuring no dialog creation can occur after receiving any negative final response for INVITE.
4	26651	Transcoding: Resource leakage on both Active and Standby for a forked dialog that needed transcoding.	The way that transcoding context was released has been fixed.

3.2 Build 3.8.1-275

The following table lists all the resolved problems for Build 3.8.1–275

	Defect	Issue	Fix Description
1	23563	BorderNet changes the codec's payload type in a transcoded call on receiving a new SDP in Re-Invite. The sip client rejects the Re-Invite with the changed payload as this is not as per standard.	Changed to work according to standard and not change the payload type for a specific codec during the call.
2	25173	The '+' sign translated to 'space' on BN username & password	User name cannot contain '+' sign. Name with a '+' sign is rejected now.

	Defect	Issue	Fix Description
3	25854	Duplicate Record Route Header Removed	For every outgoing message there was logic added earlier to avoid duplicate routes as sometimes the SCS was indenting the egress destination and adding a route even though it's a loose routed call. This for an egress leg with record routes is causing an issue as reported. Fix - Not invoking logic to remove duplicate routes when egress leg sends record routes.
4	26037	BorderNet crashes when receiving 200 OK with SDP IMAGE inactive	Fixed the crash in case of inactive Image in SDP answer
5	26215	vSBC crashes in RealTimeThreadsKeepAlive	Calling session's functionality on the CacheManager Thread caused a deadlock. Moved some session call to be invoked on MidLayer Thread instead of CacheManager Thread.
6	26243	RTP destination port not updated after receiving UPDATE. SBC is not sending RTP to the correct media port after UPDATE comes before the session is established. Ingress leg there is not reliable, and egress is reliable.	Pinholes were not modified. Update SDP used for pinhole modification.
7	26253	Bordernet crash with error "RVSIP_CALL_LEG_STATE". While receiving incoming INVITE with P-Charging Vector in specific format Bordernet Crashed	In HandleIncomingLegStateChange in case mTopologyTransp = false the mpPeerData was NULL. Check mpPeerData if NULL.
8	26271	Domain name passing in Req-uri instead of IP in Host part in case of surrogate registration	update the ReqUri in case of access-public
9	26447	LI: The Li Cache is not getting mirrored in standby platform	Fix – mirrored the LI cache
10	26448	LI: The get target request is giving single X2/X3 details	Implementation added
11	26449	SBC Rejecting Calls with 503 Peer Disabled	Fixed the scenario and now with either rate limit or configuration change, KA status is correctly updated in the association.

3.3 Build 3.8.1-240

The following table lists all the resolved problems for Build 3.8.1–240

	Defect	Issue	Fix Description
1	23294	Allow configuring ISUP content-type version in SIP-I messages as SPIROU.	Current Profiler didn't have the capability to iterate through the different SIP bodies and extract content type header. Added logic to modify content type in multiple SIP message bodies.

	Defect	Issue	Fix Description
2	23864	Softbank Merge: SIP Profiler <DropSipMessages> cannot delete the 2nd 18x. (Addition of appparam: StopRelayOf18xAfterOfferAnswer)	A new control for dropping 2nd 18x without SDP introduced. Profiler is not approached.
3	24749	ENUM routing query caused the SCS to crash and switchover.	For ENUM the timeout thread was deleting the ongoing resolution that stack was in progress. Thus, causing memory corruption and eventual crash. Fixed by handling the process timeout only on resolved and timeout DNS ENUM queries.
4	25395	SIP Capture (pcap) file is corrupted after manual switchover.	Close the last captured file after the switchover.
5	25404	SIP Capture was not deleted because the script name was changed.	Change the script file name at the SBC Install.
6	25569	SCS crashed due to TCP traffic.	NULL pointer – Fixed

3.4 Build 3.8.1-221

The following table lists all the resolved problems for Build 3.8.1–221

	Defect	Issue	Fix Description
1	16697	REFER message not handled by SBC when 200 OK contact has IP which is not the Peer IP	The message may be sent to a different ip-port if it exists in the contact header. the ACL was not opened for the desired ip-port in the route header in the refer message. Issue fixed by rechecking before sending the message whether it should be sent to another ip-port and if so, open the ACL for that specific ip-port and then close them.
2	22059	SBC does not forward 200 OK to UPDATE(2nd) during call setup if the UPDATE(2nd) is received in 5 seconds after the 1st UPDATE	The issue seems to be due to more than 1 transaction active on egress side. Stack's transaction DELETE call back is being received after the 2nd UPDATE, that resets the outstanding transaction. Now the delete transaction call backs checks the correct transaction in progress before resetting.
3	23730	BorderNet - /opt/bnet/scripts/delete_transcoding_logs.sh tries to remove logs from a nonexistent directory "/archive/logger/output"	fixed the script to remove only if the logs are existing in the directory.
4	25132	Error 505 response on specific report. Statistics -> Peer Statistics -> Outgoing Sessions -> Hourly -> Data -> Check Peak	fixed type (extra comma)
5	25144	Supported: replaces option tag is dropped from forwarded messages	Handling of replaces in case of forward was added.

	Defect	Issue	Fix Description
6	25288	Core: RVSIP_CALL_LEG_STATE_ when INVITE is received with Max-Forwards: 0 or 1 SCS process crashed.	GetPeerData() return NULL so wee access to null address. check GetPeerData() before accessing to the address.
7	25326	SIP Profile doesn't invoked when Trunk Authentication feature is in use	profiler not set - Fixed

3.5 Build 3.8.1-204

The following table lists all the resolved problems for Build 3.8.1–204

	Defect	Issue	Fix Description
1	25105	Setting MaxAllowedCallDuration to 0 does not disable the call duration timer.	Added fix to disable timer when the value is set to 0.
2	25156	From header of the Invite messages after the Refer Message does not contain the original ANI of the call.	Dynamic handling modified the from header. Remove the modification in case of dynamic handling.
3	25157	Handling of parameter "isup-oli" in the INVITE message after a Refer message is not the same for Local and Dynamic Refer.	Dynamic handling modified the from header. To make both dynamic and local handling behavior consistent have removed the dynamic handling modification of from header.
4	25179	NWL with EMS is failing with "could not connect to license server" when SYSMANAGER user is DISABLED or password is changed.	Use internal user instead and stop using SYSMANAGER user.
5	23789	"Refer message handling” of Dynamic and Local. UUI not consistent and incorrect on the Invites after the Refer message.	Dynamic and local behavior made consistent to contain similar headers. As UUI parameter is received in Refer-To header it will be constructed as header in the INVITE generated towards Transfer-Target as per RFC.
6	24981	SIP capture does not capture TCP traffic correctly resulting with an unreadable capture file	The TCP header not handle correctly, so the Wireshark couldn't decode it. 1. All the sip capture will be over transport UDP. 2. The message size didn't include the SDP size, so update the size accordingly.
7	25012	External DNS causing Page unresponsive errors.	The java queries the DNS-server for localhost, however if DNS is down, the page refresh takes time. Name Service order changed. Fix it in sbcinfra rpm.
8	25198	BorderNet SipGateway Core RVSIP_METHOD_CANCEL / RVSIP_TRANSPORT_BS_ACTION_UNDEFINED	Access to NULL pointer. Check the pointer before accessing.
9	25239	Option Keep Alive minimum time changed from 30sec to 2sec	The range for Option Keep alive is now 0 or between 2-900 where 0 is disable. It is not recommended to use KA time less then 30 sec.

	Defect	Issue	Fix Description
10	23997	HKT Merge: SUBSCRIBE from Huawei Softswitch was rejected by BN-SBC due to the cause of “Route not found”	added support for SUBSCRIBE message from Access-Local side.
11	23998	HKT Merge: UPDATE (after 183) from Huawei Softswitch was rejected with 415 (media type unsupported). Call Scenario: Egress is reliable, ingress not. Egress sent 183 with SDP and SBC replied with PRACK, offer answer closed on egress. SBC send 183 to ingress but its non-reliable and hence offer answer is in opened state so new offer coming in UPDATE was rejected with 415.	After the fix UPDATE is responded locally with 200 OK.
12	25124	HKT Merge: BN did not forward large message size of NOTIFY to Ingress Side.	Change was made to allow large message size for Notify messages.
13	25241	HKT Merge: BN should add SDP in outgoing INVITE when incoming INVITE is without SDP.	Added Support for Slow start calls. New parameter interduce and needs to be configured in AppParam.xml AlwaysGenerateINVITEWithSDP <BooleanParameter name="AlwaysGenerateINVITEWithSDP" value="true" type="boolean" OperatorEditable="true"/>
14	25243	HKT Merge: Flexible media feature is not working, BN drops SDP.	Issue came up because flexible media needs media out of the box and transcoding needs the media to be terminated on the box. It’s a feature interaction issue. So currently making flexible media off when transcoding is configured.
15	25244	HKT Merge: Asymmetric registration is not working in 3.8.1-500.	New parameter interduce and needs to be configured in AppParam.xml for enabling Asymmetric REGISTER in case of non-NAT. <BooleanParameter name="LocalRegisterResponseBeforeExpire" value="true" type="boolean" OperatorEditable="true"/>
16	25245	HKT Merge: In App Server to PBX Calls BN should add called number in request URI of INVITE in place of pilot number	Add support for pilot number registration in Access. New parameter “Pilot Name” was added in Access-Public interface. if parameter kept empty it work as it work before without pilot registration. In Access-Local to Access-Public call if configured Pilot Name is equal to “userpart” of incoming INVITE R-URI, SBC change the “userpart” of outgoing INVITE R-URI to be same as To Header.
17	25246	HKT Merge: IP overlap is not allowed in case of Access interface.	SBC configuration was changed to allow IP overlap in case of Access Interface. Same IP is not allowed.
18		3.7.0-208 fix merge into 3.8.1	Merge the fix for TFS#24287 and TFS#24987

3.6 Build 3.8.1-172

The following table lists all the resolved problems for Build 3.8.1–172

	Defect	Issue	Fix Description
1	24986	SBC Hardening: IPSEC, IPv6 and SCTP Calls are not working after hardening on 3.8.1-167	It is observed that SBC hardening on 3.8.1-167 block/remove the support of IPv6 and SCTP. update the hardening rpm to support it and provide new images for fresh install.

3.7 Build 3.8.1-167

The following table lists all the resolved problems for Build 3.8.1–167

	Defect	Issue	Fix Description
1	15647	BorderNet Media Inactivity Call disconnection Alarm's Reported FDN show Epoch time	Time format in inactive media alarm was converted from Unix/Epoch time format to human readable format.
2	19261	Profiler Not Working on SUBSCRIBE message for changing the Contact Header IP and Port	Add support for outgoing side profiler execution on SUBSCRIBE message.
3	20220	SIP and RTP interface separation are not working on AWS - local IP not converted to Public IP	Resolve the issue when different PAT is set for media and signaling, and Public IP is associate to the VLAN IP.
4	22217	REST API isn't being updated with user modification after establishing a successful REST API message	Restart REST API service when user is being deleted and reject login if user is found to be not enabled.
5	22382	In Access scenario after 302 redirect new INVITE is generated with original R-URI and not using URI from Contact header in 302	Issue fixed by taken the URI from the contact header of 302 message and insert it into the new R-URI generated INVITE.
6	22418	SBC GUI "System" - "Change Password" item is not available when login user does not have SYSTEM_ADMIN role	change privileges and update onclick operation to change password (instead of users)
7	22419	SNMP Trap Community Name (AppParam TrapCommunityName) cannot include non-alphabet letters (other than A-Za-z) when attempt to edit from GUI.	The App-Param for “Community Name” has been removed and now the settings is a parameter in the SNMP trap manager configuration screen for SNMPv1/V2
8	22443	SNMP community name in BorderNet cannot be changed	A new 'Community' parameter introduced under add SNMP manager, as a text/string input. It should be visible and configurable if 'SNMP Version' parameter is set to either 1 or 2c.
9	22527	Search in NT profile will not find the profile unless you add the prefix NT_ but it isn’t case sensitive	Add support for search by partial word. Search is case sensitive.
10	22528	Cannot double click an entry in directory set to change, but you can in NT Profile.	Changed the existing behavior. Double click to an entry in directory and criteria set is supported now.
11	22573	Nalpeiron - Some session got stuck on server as allocated causing BN to be blocked from increasing traffic	The new License mechanism that was implemented with BorderNet EMS resolved the issue.

	Defect	Issue	Fix Description
12	22576	Number of OPTIONS keepalive destinations is limited to 5 for one Peer FQDN, when multiple SRV records returned by external DNS	Modified the MAX Records and max Elements in Single DNS List value from 5 to 30.
13	22587	SIPREC: BN doesn't send 200OK to ingress in case SRS is not reachable	New REQ, Release call on SRS failure Yes\No. Added configuration parameter to the SIP-Rec configuration. · If "Release call (CS) on SRS failure" = yes, then the CS call shall be released. · If "Release call (CS) on SRS failure" = no, then the CS shall not be released. the call shall continue regularly without interruption. · Default shall be set to "No", so the call will continue and there will be no calls dropped. If the call is released due to "Release call (CS) on SRS failure" = yes, then a final response shall be sent to the peer.
14	22799	New user created in 3.8.0-xx cannot access REST API GUI	Users needed to be reloaded, so restart REST API service in case user is being added or deleted.
15	22808	Core- RealTimeThreadsKeepAlive	Apply SIP stack patch that fix the deadlock. The fix was in the “attachServerCancelOrPrackToServerInvite” function.
16	22880	Trunk-Authentication - cannot put "+" sign in the "Auth Username" field	Add support for “+” sign in the “auth username” on Trunk-Authentication
17	22896	BorderNet FMS unable to reopen TCP socket after timeout from SMTP server what causes FMS not to send alarm mails.	When an alarm that needs to be sent via email arrives, FMS tries to send it. If socket is found to be closed, the FMS reopens it and resend the same alarm.
18	22918	Lack of Topology hiding on “maddr” in Contact header	Resolved by removed the “maddr” from Contact header.
19	22991	BorderNet - if transcoding enabled and receives an SDP with many telephone-event rates, it answers with topmost header and no according to selected codec rate	Choose telephone event according to selected codec clock rate.
20	23186	Adding SBC Name in the Dashboard	User need to clearly see the host name which is currently active. Added active host name to the GUI upper pane.
21	23187	Add Directory tables names to table edit page.	Correctly set the title with edited set name for Criteria Set and Directory lookup.
22	23193	Alerting when other user (With Provisioning privilege) is already logged in	Added an alert message to the upper pane when non read only users are logged in.
23	23212	BN - drops SDP answer with single m line and port 0 (UPDATE message)	media line with m=0 is deliberately treated as unexpected and hence call processing stops. Ensured that for UPDATE method m=0 line is processed, and call continues further.

	Defect	Issue	Fix Description
24	23235	SDP version not getting incremented for re-invite because of which calls are failing	SBC could not differentiate the SDP as same session id and version id to the egress SDP was received from transfer-target Added fix to increment SDP session id in case the SDP is received from transfer target
25	23239	OPTIONS: SBC should answer OPTIONS locally, if req-uri is missing port but the actual IP parameters are valid and match a valid SIP interface on the BN	Made code changes with respect to the IP:Port validation in the OPTIONS request message If request-uri is pointing to BN's interface on which OPTIONS is received, It should be replied with 200 OK.
26	23254	Access-Call: Request-URI of new INVITE created by BN does not use the username received in 302 contact.	Issue fixed by taken the URI from the contact header of 302 message and insert it into the new R-URI generated INVITE.
27	23258	Registration Cache Data Load Error in BNSBC GUI	Having & in the display name makes the xml invalid so before writing them into the file - remove & and + from display name.
28	23680	BN- INFO transaction stuck when receive INFO requests from both ingress and egress	Check transaction state changed event and reply 491 if needed.
29	23697	Unable to load Trial License	Fixed wrong NIC's name
30	24936	Merge all 3.8.0 fixes to 3.8.1 release	bug parity is as following: 3.8.1-160 <== 3.8.0-250 <== 3.7.6-228

4. Known Issues

4.1 SBC Known Issues

Defect	Description	Workaround
20955	WebRTC: Only Chrome browser supported.	Use only Chrome Browser
20991	WebRTC: High Availability not supported.	
22151	PostgreSQL: When viewing large NT profile from GUI with 1,000,000 records, 505 error is displayed, and Java CPU reaches 950%.	Do not view from GUI profile with more than 100,000 records. Error message appear in GUI.
24757	RADIUS Authentication - login failed with Authentication Method = CHAP	Option removed from BorderNet configuration.
22211	After upgrading platform on first login "Repository is Busy" error appears on login page.	
24747	Geo redundancy (AWS) - GUI is accessible by management IPs of both ACTIVE and Stand by in same time.	

4.2 SBC EMS Known Issues

Defect	Description	Workaround
24937	Bordernet Upgrade from EMS GUI sometimes stuck, and status displayed only on first BN on List.	SBC upgrade should be done from SBC UI
24522	EMS Upgrade: Need to activate again license after upgrade from 3.8.0-238 to 3.8.1-X	After upgrade EMS from 3.8.0 to 3.8.1 need to activate again EMS License on Tools->License
24557	Failed synchronize appears in report on update criteria set and directory lookup while synchronize finished successfully on SBC.	Ignore the wrong report message.
24843	Synchronize failed when action include add/delete number translation	
24943	After deploy HA SBC the provisioning status became "unmanageable" since Postgres is failed on "Active"	Manually start the Postgres service from command
	LDAP configuration is deleted after upgrade	Reconfigure the LDAP – new LDAP implementation
	Analytic IP address is deleted from EMS configuration after upgrade	Reconfigure the Analytic IP address

END OF DOCUMENT