Release Notes - Rev. 11.0

Dialogic® BorderNet™ Session Border Controller (SBC)

Release 3.8.1

June 2019

Table of Contents

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
11.0	June 2019	Release 3.8.1 (build 3.8.1-150)
10.4	March 2019	Release 3.8.0 (build 3.8.0-238) - update resolved bugs
10.3	March 2019	Release 3.8.0 (build 3.8.0-238)
10.2	February 2019	Release 3.8.0 (build 3.8.0-197)
10.1	December 2018	Release 3.8.0 (build 3.8.0-153) - update bugs parity
10.0	December 2018	Release 3.8.0 (build 3.8.0-153)

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). It also contains the release notes of Release 3.8.0.

1.2 Glossary

For the purposes of this document the following abbreviations apply:

Abbreviation	Meaning
AWS	Amazon Web Services
EC2	Elastic Computing Cloud
EMS	Element Management System
KVM	Kernel-based Virtual Machine
LI	Lawful Interception
LBO	Local Break Out
OMR	Optimal Media Routing
SBC	Session Border Controller
SR-IOV	Single Root I/O Virtualization
TRF	Transit & Routing Function
VPC	Virtual Private Cloud

1.3 Contact Us

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

2. Release Notes 3.8.1

2.1 Overview

This document provides the **Release Notes 3.8.1** for the Dialogic BorderNet SBC, covering the following topics:

- Upgrade Path
- New Features
- Resolved Issues

Notes:

1 - NTP synchronization is mandatory for High Availability BorderNet SBC deployments.

2.2 Upgrade Path

Release	Supported Upgrade Path
3.8.0-241 3.7.6-228	3.8.1-xxx

2.3 Upgrade Notes

Upgrade is supported only from BorderNet 3.7.6 with Centos 7.4.

BorderNets with Centos 7.3 should run the migration procedure from Centos 7.3 to Centos 7.4.

BorderNet EMS upgrade from 3.7.6 to 3.8.0 release is supported only from command line and not from GUI.

2.4 New Features

2.4.1 Geo Redundancy

Geo-Redundancy enables the deployment of the BorderNet SBC in High Availability mode where each platform/instance (primary and secondary) is located on two different networks or sites.

Figure 1: BorderNet in Geo-Redundancy Mode

In this deployment mode, each BorderNet SBC has its own set of IP addresses which can be on a totally different network:

- **Management IP address**: Each platform has its own management IP address as opposed to normal HA deployment mode where the management IP addresses are shared between primary and secondary
- **Utility IP address**
- **HA link IP address**
- **HA link Gateway IP address**: since each platform can be placed on a different network, the BorderNet SBC needs a Gateway IP address to be able to reach its partner platform
- **Traffic IP addresses**: Each platform will have its own sets of traffic IP addresses as opposed to normal HA deployment mode where traffic IP addresses are shared between primary and secondary

Geo-Redundancy can be implemented on bare metal deployment, virtualized deployment or cloud deployment.

In the diagram below, in a Geo-Redundancy configuration, during normal operation, traffic runs from Peer A to the active platform/instance and vice-versa.

If the active platform/instance fails, the standby platform/instance senses the failure and there is no keep-alive response from the active platform via the HA link.

The standby platform declares the mated pair as failed and assumes the active role by sending a re-invite to Peer A, displaying its IP address so that Peer A starts sending traffic to that platform/instance instead.

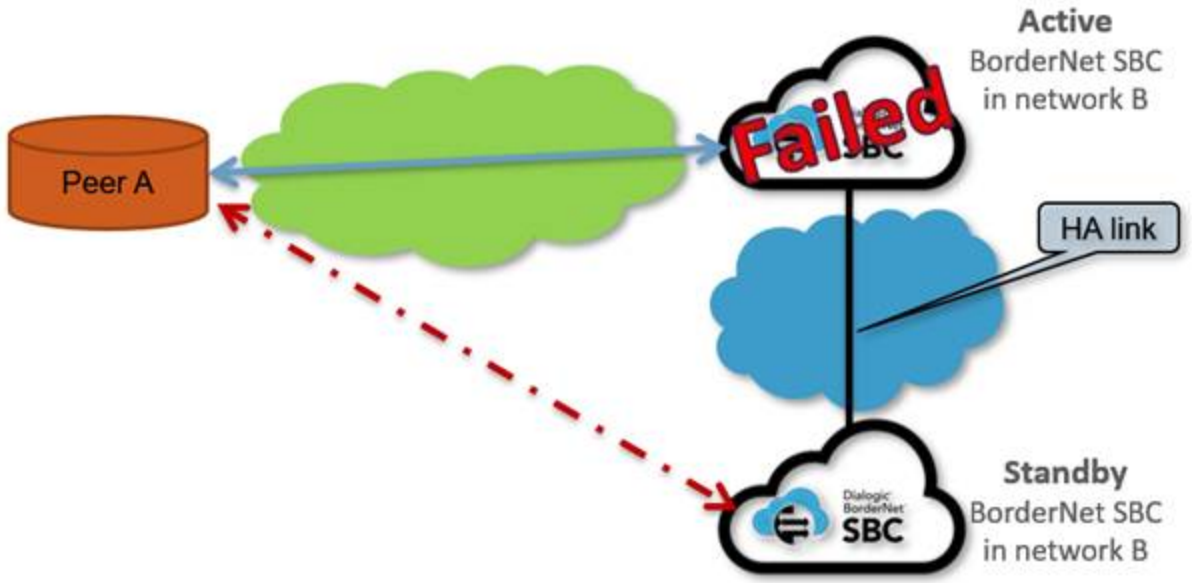


Figure 2: Geo-Redundancy Scenario

2.4.2 Network Wide Licensing (NWL)

The BorderNet SBC provides reliable licensing management.

There are three modes of licensing:

- Regular standalone licensing using a local license file on the BN.
- Licensing of a single BN through a Nalpeiron server which is used for license retrieval and then the BN builds a local file. There is no on-going license enforcement through Nalpeiron. License refresh is triggered manually.
- EMS-based network licensing. The initial license is retrieved from the Nalpeiron server using a DLGC interface and then the EMS builds a local file. There is no on-going license enforcement through Nalpeiron and only periodic usage updates are sent for statistical purposes. License refresh is triggered manually.

BorderNet has adopted a cloud-based **Network Wide Licensing (NWL)** solution, based on the following logical components, as shown in the figure below:

- **Licensing Client** - Installed on every BorderNet SBC.
- **Licensing Server** - Installed on the cloud.

NWL facilitates license sharing of multiple BorderNets which reside on the same network.

Licenses can be dynamically granted to distributed BorderNets based on their momentary load. If some are not loaded, others can utilize the unused license capacity. NWL implementation previously used Nalpeiron as the NWL server.

The **Nalpeiron Software Licensing (NSL)** framework is a cloud-based software licensing entitlement, analytics and management solution.

The use of the Nalpeiron server has given rise to some reliability issues. To overcome this a new NWL mechanism has been implemented, which will be based on the Dialogic BorderNet EMS as an NWL server. The Nalpeiron is still used as the license generator, but after the initial license retrieval it is not addressed anymore by the EMS or by the BorderNet.

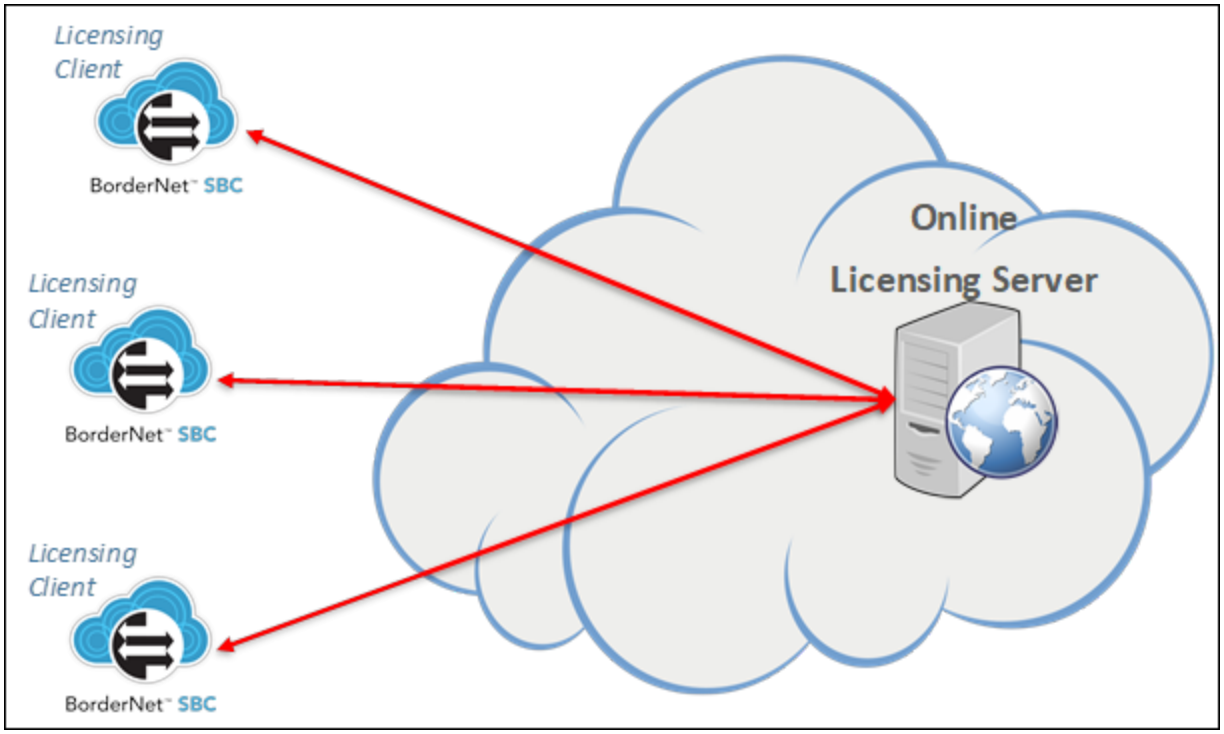


Figure 3: BorderNet SBC's Network Wide Licensing Architecture

The solution is agnostic to the deployment type (hardware, virtualized and cloud), and to the operating system (any Linux flavor supported by the BorderNet SBC).

When the NWL is activated:

- A code is created in the Licensing server per BorderNet SBC (or a group of BorderNet SBCs), together with the relevant feature list, and is provisioned in the EMS.
- The code is sent to each BorderNet SBC. The BorderNet SBC creates its own feature list.
- After the initialization, the BorderNet SBC (the licensing client) sends the **GetLicenseInfo** message and the license code to the Licensing server.
- The **GetLicenseInfo** message's response is sent back together with the feature list. Upon receiving the response, the BorderNet SBC populates the feature list and activates a timer using the **RefreshFeatureList** timer's value (see **Provisioning**).
- Upon the timer's expiration, the client periodically sends the **UpdateLicenseInfo** request and resets the timer each time.
- The **UpdateLicenseInfo** response contains the full list of features.
- For the **Yes/No** licenses, the feature list value is checked, and the relevant action is taken accordingly, and for the **Quantitative** licenses, the feature's value is incremented per session, and is checked. If the value is larger than the value in the feature list, the session is rejected.
- The updates and steps that follow the update are provided periodically.

In the case of EMS-based NWL, the EMS creates a non-reproducible license and uses it locally. It then sends periodic usage reports as accumulated values only and not per BorderNet. This is illustrated in the figure below.

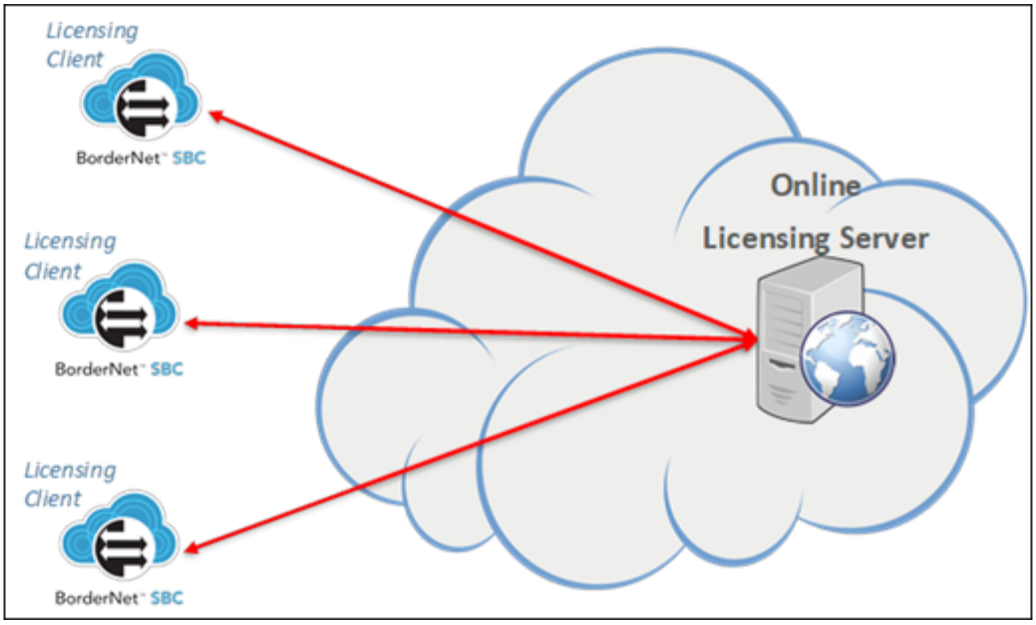


Figure 4: EMS-Based Network Wide Licensing

EMS to BorderNet communication is based on the current **RESTfull API** mechanism and all licensing messages are encrypted and authorized.

Message types include the following:

- **EMSGetLicense** - BorderNet to EMS: request for a new initial license, or a request for updating the existing license, if the license has been changed. If this request fails it is reattempted every 60 seconds.
- **EMSGetLicenseResponse** - EMS to BorderNet: list of full licenses and features.
- **EMSUpdate** - BorderNet to EMS: periodic updates on the amount of sessions and features used and requested. Used to both request and inform on current sessions usage.
- **EMSUpdateResponse** - EMS to BorderNet: The amount of sessions approved per each feature.

Network Wide Licensing configuration can be implemented directly from the BorderNet screen as shown here below.

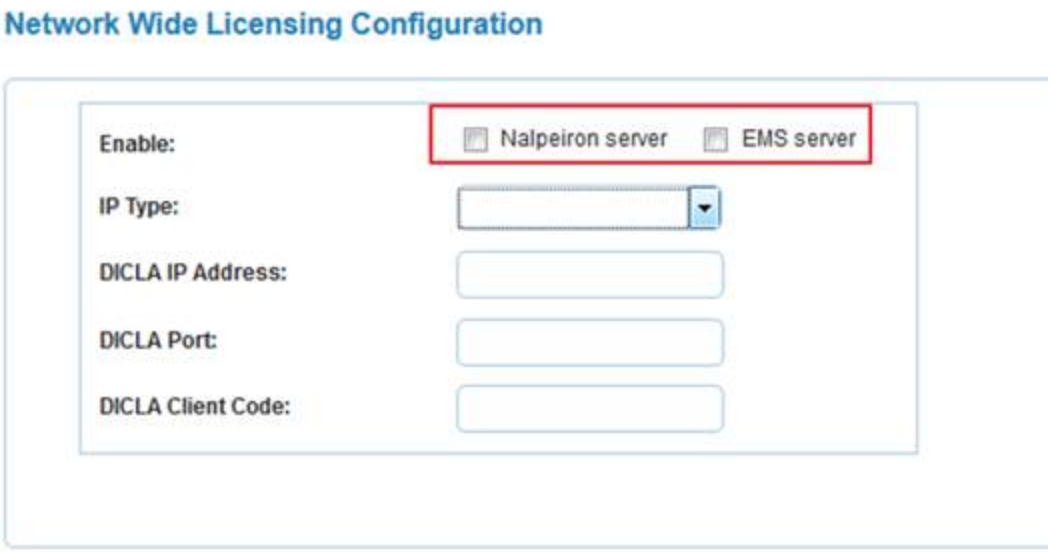


Figure 5: NWL Configuration in BorderNet

2.4.3 LDAP Configuration

Lightweight Directory Access Protocol (LDAP) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

LDAP allows you to search for an individual on the network without knowing where they're located.

BorderNet supports a TLS/LDAPS secure connection and the default port for the secure LDAP is 636. Certificates received from the LDAP server are automatically accepted by BorderNet and EMS. No customized role attribute is required as role definition is performed based on role groups and the user's association to a role group.

In BorderNet the group names match the pre-defined roles available on the BorderNet. In order to support different privileges options for different BorderNets, the customer can define groups with the BorderNet pre-defined roles prefixed with a string. For example: IL_SYSTEM_ADMIN and US_SYSTEM_ADMIN. The BorderNet has an optional prefix parameter (example: prefix=IL, prefix=US)

In the EMS new roles are created with new names, so the customer can either create a new group or use an existing one. There is no need for a group prefix. The EMS roles can be customized and there is a single EMS on a network.

The Authentication process works as follows:

- Search the user.
- If a 'member of' attribute is available, this attribute lists all the groups this user belongs to. (No need to search for groups, they are already listed).
- If a 'member of' attribute does not exist, search all the groups to find the ones containing this user.
- Use the list of groups as a list of roles.
- The group list can contain other group names in the tree, so it will ignore any unknown role name.
- Order of authentication - local users, LDAP, RADIUS.
- The required parameters are shown in the table below.

• **Parameter Name**	• **Description**	• **Mandatory**	• **Optional Values**	•
• Enable	• Enable/disable LDAP configuration. • Type: checkbox.		• Checked/unchecked	•
• **Connection**				

• Parameter Name	• Description	• Mandatory	• Optional Values	•
• LDAP Server IP	• IP address of LDAP server	• Yes	• IPv4 address	•
• LDAP Server Port	• TCP port number of the LDAP server	• Yes	• 0-65535	•
• Use TLS	• Enable secure connection using LDAP over TLS • (usually over port 636) • Type: checkbox.		• Checked/unchecked	•
• Admin DN	• A user with privilege to access the LDAP server directory. Full path required.	• No	• String. • Example:CN=Administrator,CN=Users • DC=dialogic,DC=com	•
• Admin password	• Password of Admin user. • Should be hidden. • (user should see '*' signs)	• No	• String	•
• **Users**				

• **Parameter Name**	• **Description**	• **Mandatory**	• **Optional Values**	•
• Users base DN	• Search scope to look for users (search starting with this point/under this branch)	• Yes	• String • CN=Users,DC=dialogic,DC=com	•
• User identification attribute	• Attribute type to uniquely identify a user. • This is the attribute that will be used as the login identifier. • Usually 'uid'. For AD it will be sAMAccountName	• Yes	• String	•
• **Groups**				
• Group membership attribute	• Attribute of a user entry listing all the groups this user is associated with.	• No	• String	•
• Groups base DN	• Search scope to look for groups containing the user (search starting with this point/ under this branch)	• Yes	• String • Example:CN=Guests,DC=dialogic,DC=com	•

• Parameter Name	• Description	• Mandatory	• Optional Values	•
• Group identification attribute	• Attribute type to uniquely identify a group (a group search filter). • This is the attribute that will be used as the group name which is mapped to an access level role.	• Yes	• String • Example: CN	•
• Only on BorderNet. • Group name prefix	• String placed before the 'group identification' and removed by the BorderNet. • Used for flexible provisioning of several groups with several prefixes on the LDAP server.	• No	• String	•

2.4.4 SNMPv3 Support

The BorderNet SBC uses **Simple Network Management Protocol (SNMP**) for sending alarm traps to external SNMP managers, and also for remote SNMP managers to retrieve limited information from the BorderNet via GET requests.

In Release 3.8.1 SBC support **SNMPv3**, which enables each SNMP packet to be both authenticated and encrypted in a secure way.

SNMPv3 requires an application to know the identifier (snmpEngineID) of the remote SNMP protocol engine in order to retrieve or manipulate objects maintained on the remote SNMP entity. The EngineID is also one of the inputs used for key derivation of the authentication and privacy keys.

In order to learn the snmpEngineID of a remote SNMP protocol engine, a discovery mechanism is used.

For SNMPv3 traps there is no discovery process. Traps are also not acknowledged.

The authoritative SNMP engine for a trap packet is the sending SNMP agent. Since the generator of the message and the authoritative engine are one and the same, there is no need for the SNMPv3 discovery process. All the information is already inside the single trap message.

As mentioned, SNMPv3 traps use the engineID of the local application sending the trap rather than the engineID of the remote application (like in a GET request). This means that you have to create users in your remote user database (the SNMP trap server) for every engineID you wish to send traps from. Some servers allow all EngineIDs and identify the traps by their user-name.

2.4.5 RADIUS Autentication

Remote Authentication Dial-In User Service (RADIUS), was originally designed to deliver AAA services for dial-up internet. As such, most of its parameters are network access oriented and are aimed to supply different networking properties for the user accessing the network services. Typical parameters include service type, protocol type, IP address to assign the user (static or dynamic), access list to apply, or a static route to install in the NAS routing table.

A **Network Access Server (NAS)** operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.

The RADIUS server response includes a list of attribute-value pairs that describe the parameters to be used for a session.

As part of its authentication capabilities, the RADIUS protocol is widely used for user authentication which is not necessarily related to network access. On top of the regular PAP/CHAP password authentication, it can also support a variety of other user authentication protocols like EAP-TTLS, EAP-TLS and PEAP.

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and the RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.

RADIUS uses UDP as the transport layer, and therefore it implements reliability options on the application (RADIUS) level. If no response is returned within a predetermined length of time, the request is re-sent a number of times. The client can also forward requests to an alternate server or servers in the event that the primary server is down or unreachable.

RADIUS message types include the following:

- **Access-Request** - This is the first message sent from the client to the server, asking permission to access the network. It contains user and network information for authentication and authorization. An Access-Request can include multiple attributes, each containing some information regarding the requested service.
- **Access-Accept** - Sent from the server to the client, granting permission to access the network. An Access-Accept message can provide specific configuration information for the client, such as IP address, QoS profile, user authorization or any other attribute needed.
- **Access-Reject** - Sent from the server to the client, denying permission to access the network. Can include reject cause and a message to the user.
- **Access-Challenge** - Sent by the server to issue a challenge to which the user must respond. The client then re-submits its original Access-Request with the extra information required by the Access-Challenge.

2.4.6 Scale In/Out on Amazon

The BorderNet SBC can be scaled out and in (horizontal scaling) according to 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. Scalability can be architected into the system, so it is not automatic and is generally more challenging than Scaling Up.

Figure 6: Scale-Out

The following limitations refer to the scope for Scale In/Out on the BorderNet SBC:

- Only Amazon (AWS) is supported.
- Only a concurrent sessions indicator is used as a threshold parameter for scaling decisions.
- Abnormal scenarios, such as a new instance which is not able to become active or is not responsive, are not handled in the current phase.
- Changing configuration at runtime is not part of the current phase. This will be implemented after the full integration of EMS.
- New instances are not yet configured. A change of configuration will be done only 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 will be deployed as standalones.

The **Scale In** and **Scale Out** actions are directly controlled from the GUI through the **Edit Scalability Profile** window.

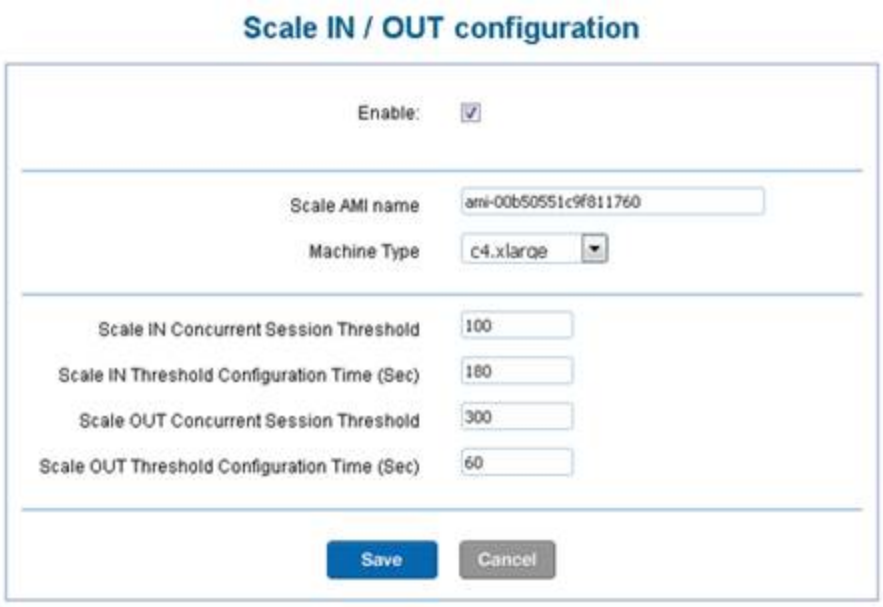


Figure 7: Editing Scale In/Out Parameters

2.4.7 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 operation. This includes a list of tests to complete in order to establish a secure configuration posture, as per the **Center for Internet Security (CIS)** hardening recommendations.

The list of tests includes all the following areas:

1 Initial Setup

1.1 Filesystem Configuration

1.2 Configure Software Updates

1.3 Filesystem Integrity Checking

1.4 Secure Boot Settings

1.5 Additional Process Hardening

1.6 Mandatory Access Control

1.7 Warning Banners

1.8 Ensure updates, patches, and additional security software are installed

2 Services

2.1 INET Services

2.2 Special Purpose Services

2.3 Service Clients

3 Network Configuration

3.1 Network Parameters (Host Only)

3.2 Network Parameters (Host and Router)

3.3 IPv6

3.4 TCP Wrappers

3.5 Uncommon Network Protocols

3.6 Firewall Configuration

3.7 Ensure wireless interfaces are disabled

4 Logging and Auditing

4.1 Configure System Accounting (audited)

4.2 Configure Logging

4.3 Ensure logrotate is configured

5 Access, Authentication and Authorization

5.1 Configure cron

5.2 SSH Server Configuration

5.3 Configure PAM

5.4 User Accounts and Environment

5.5 Ensure root login is restricted to system console

5.6 Ensure access to the su command is restricted

6 System Maintenance

6.1 System File Permissions

6.2 User and Group Settings

2.4.8 EVS and EVRC

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

- **EVS** is a super wideband speech audio coding standard. It offers up to 20 kHz audio bandwidth and has high robustness to delay jitter and packet losses due to its channel aware coding and improved packet loss concealment.
- **EVRC** is a speech codec used in CDMA networks. It was developed in 1995 to replace the QCELP vocoder which used more bandwidth on the carrier's network, so EVRC's primary goal was to offer the mobile carriers more capacity on their networks while not increasing the amount of bandwidth or wireless spectrum needed. EVRC uses RCELP technology, which Qualcomm claims improves speech quality with lower bit rates.

2.4.9 New XML Configurations for EMS

Release 3.8.1 includes some changes in BorderNet to accommodate the new EMS.

The EMS manages multiple BorderNets. With EMS in place, configurations are performed on BorderNet through EMS only.

Configurations such as media profile and service profile are created and pushed to all the managed BorderNets, so that the configuration of a specific BorderNet on the EMS will be always in sync with the configuration on a specific BorderNet.

The exact same media profiles are configured on all BorderNets, but one of the parameters of the media profile is Port Allocation. It uses a VLAN name which is specific to the BorderNet.

Similarly for service profiles, there are other parameters such as Advanced Policy and Sip-Rec Peer, which refer to certain interface/peers of the specific BorderNet.

These BorderNet specific configurations block the user from generalizing the media profile and service profile configurations at the EMS level. The way to deal with this problem is to remove port allocation configuration from teh media profile setting, to remove advance policy and Sip-Rec peer configurations from the service profile setting and then re-add these configurations at the Peer & Interface level.

2.4.10 EMS Provisioning

Release 3.8.1 adds a more comprehensive provisioning facility to the EMS.

Possible provisioning statuses for the BorderNets are defined as follows:

- ¨ **InSync** - where all the EMS configuration appears in the BorderNet.
- **Not InSync** - where the BorderNet went out of synchronization with the EMS because of an operation that was performed and consequentially the EMS has failed to reach the BorderNet.
- **SyncInProgress** - during the synchronization process.
- **New Device** - where there is a new BorderNet with no content.
- **Unmanageable** - where there is a BorderNet version older than 3.8.0 which doesn't have the necessary parameters to configure it.
- **Corrupted** - where the BorderNet has experienced one of the following:
  - has been added to the EMS with own data initially
  - went out of synchronization with the EMS because of a configuration issue
  - has been upgraded to a version supported by the EMS from a version that did not support it

The user can now perform provisioning on all the following profiles:

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

2.5 Resolved Issues on Build 3.8.1-150

The following table lists all the resolved problems for Build 3.8.1-150

	Defect	Issue	Fix Description
	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.
	16697	REFER message not handled by SBC when 200 OK contact has IP which is not the Peer IP	The ACL was not opened for the desired IP-Port. 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 it.
	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.
	20220	SIP and RTP interface separation are not working on AWS - local IP not converted to Public IP	
	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.
	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.
	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)
	22419	SNMP Trap Community Name (AppParam TrapCommunityName) cannot include non-alphabet letters (other than A-Za-z) when attempt to edit from GUI.	Change application parameters module to accept also numbers and some special characters for string values.
	Defect	Issue	Fix Description
	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.

	Defect	Issue	Fix Description
	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.
	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.
	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.
	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.
	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.
	22808	Core-RealTimeThreadsKeepAlive	Apply SIP stack patch that fix the deadlock. The fix was in the "attachServerCancelOrPrackToServerInvite" function.
	22880	Trunk-Authentication - cannot put "+" sign in the "Auth Username" field	Add support for "+" sign in the "auth username" on Trunk-Authentication
	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.
	22918	Lack of Topology hiding on "maddr" in Contact header	Resolved by removed the "maddr" from Contact header.
	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.
	Defect	**Issue**	**Fix Description**
	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.
	23187	Add Directory tables names to table edit page.	Correctly set the title with edited set name for Criteria Set and Directory lookup.

	Defect	Issue	Fix Description
	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.
	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. No change for INVITE/RE-INVITE.
	23235	SDP version not getting incremented for re-invite because of which calls are failing	
	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	
	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.
	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.
	23680	BN- INFO transaction stuck when receive INFO requests from both ingress and egress	Check transaction state changed event and reply 491 if needed.
	23697	Unable to load Trial License	Fixed wrong NIC's name

2.6 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.
22182	Rollback - During rollback process from 3.8.0 to 3.7.6 active calls are dropped.	
23238	Mirroring issue observed for transcoding calls during upgrade from 3.8.0-197 to 3.8.0-238	

3. Release Notes 3.8.0

3.1 Overview

This document provides the **Release Notes 3.8.0** for the Dialogic BorderNet SBC, covering the following topics:

- Upgrade Path
- New Features
- Resolved Issues

> **Notes:**
>
> 1 - NTP synchronization is mandatory for High Availability BorderNet SBC deployments.

3.2 Upgrade Path

Release	Supported Upgrade Path
3.7.6-228	3.8.0-xxx

3.3 Upgrade Notes

- Upgrade is supported only from BorderNet 3.7.6 with **Centos 7.4.**
- BorderNets with Centos 7.3 should run the migration procedure from Centos 7.3 to Centos 7.4.
- New GCC 8.2 must be installed before the upgrade (see 2.5.9).
- BorderNet EMS upgrade from 3.7.6 to 3.8.0 release is supported only from command line and not from GUI.

3.4 Rollback Notes

During the Rollback process from 3.8.0 to 3.7.6 active calls are dropped (**TFS 22182**).

3.5 New Features

3.5.1 Diameter Rx Interface

The **Diameter Rx** reference point is used for policy control of sessions on the **IP Connectivity Access Network (IP-CAN**) and is operated between the **P-CSCF (Proxy-Call Session Control Function)** and the **PCRF (Policy and Charging Rule Function)**. The **PCRF** provides network control regarding service data flow detection, gating (blocking or allowing packets), QoS control and flow-based charging towards the **PCEF (Policy and Charging Enforcement Function**).

When the **Policy and Charging Control (PCC)** is used in the network the **P-CSCF** sends information obtained from a SIP/SDP session setup signaling to the PCRF via the **Rx reference point.**

This information enables the PCRF to form authorized IP QoS data (e.g. maximum bandwidth and QoS class) and charging rules that will be delivered to the access gateway via the **Gx reference point**.

The **P-CSCF** is tasked to send policy information to the **PCRF** about every SIP message that includes an SDP payload. This ensures that the **PCRF** passes the proper information to perform policy and charging control for all possible IMS session setup scenarios.

Similarly, the **PCRF** utilizes the **Rx reference point** to send notifications of bearer events to the **P-CSCF**. For passing the information, the **P-CSCF** and **PCRF** use a **Diameter protocol** as defined in **3GPP TS 29.214.**

The **Diameter Rx** interface therefore relies mainly on the following standards:

- **IETF rfc6733** - Diameter Base Protocol
- **IETF rfc7155** - Diameter Network Access Server Application
- **3GPP 29.214** - Policy and Charging Control over Rx reference point

The **Diameter Rx** properties use the existing Diameter profile configuration screen, which is available for **Rf & Ro**.

An **Rx** interface activation checkbox is available in the SIP interface configuration screen.

The Rx uses message types as defined in **RFC6733 Diameter Base Protocol**, with the addition of the **AAR (Authentication Authorization Request**) message type defined in **RFC7155 Diameter NASREQ**.

The license for **Diameter Rx** is per Diameter feature. The entire feature is either enabled or disabled regardless of the number of concurrent sessions using it.

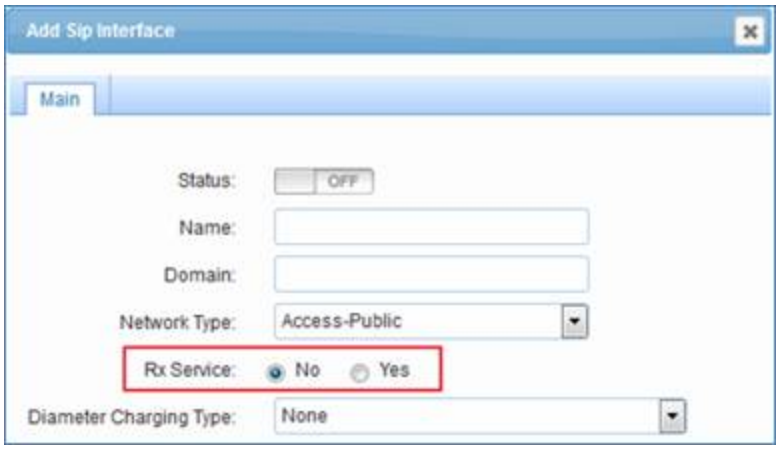
NOTES:

- **Rx** Diameter connections to the **PCRF** shall be independent of the **Ro** and **Rf** Diameter connections used for the **OCS/OCF** and the **CDF** accordingly.
- **Rx** user validation shall be enabled only for the **Access-Public** interface type.
- **Rx** validation shall be performed only if the **Rx Interface** parameter is set on the **SIP interface** configuration screen. Otherwise no **Rx** handling is required.
- **Rx** messages are sent by the BorderNet to the Diameter server (**PCRF**) only when the BorderNet receives a SIP message with SDP.
- **Rx** authorization process shall be performed before the call is routed, and before any **Rf** or **Ro** messages are sent.

The **Diameter Rx** interface:

- is not dependent on Rf/Ro.
- is applied only on **Access Public** interfaces.
- sends an Rx message only when the BorderNet receives or sends a SIP message with SDP.

- is handled per offer/answer, regardless of the message carrying it.



3.5.2 Diameter Ro/Rf on Interface Level

In the previous BorderNet release, **Diameter Ro/Rf** was supported only on the Peer level.

In the 3.8.0 release Diameter Ro/Rf is supported on both the Peer and Interface Levels.

As with all parameters & profiles which are configured in both the Interface & Peer screens:

- If a user configures both, then the Peer configuration overrides the Interface configuration.
- If only the Interface is configured, it is inherited to all associated Peers.
- If only the Peer is configured, it is allowed only for the configured Peer.

3.5.3 WebRTC Support (Controlled Introduction)

WebRTC introduces the possibility of making interfaces available in a standardized way within the browser.

WebRTC works only on the Access Public interface type and there is also a WebRTC Gateway between the WebRTC and SIP.

The total WebRTC effort consists of two major parts, each consisting of multiple documents:

- **IETF** protocol specification - describes the different network protocols to be supported when implementing WebRTC.
- World Wide Web Consortium (**W3C**) JavaScript API specification - describes a set of APIs, embedded in the client browser, which enable a JavaScript code using it to establish a real time connection between browsers.

WebRTC call setup has been designed to focus on controlling the media plane, leaving signaling plane behavior up to the application as much as possible. The rationale is that different applications may prefer to use different protocols, such as the existing SIP call signaling protocol, or something custom to the particular application, perhaps for a new use case.

In this approach, the key information that needs to be exchanged is the multimedia session description, which specifies the necessary transport and media configuration information necessary to establish the media plane.

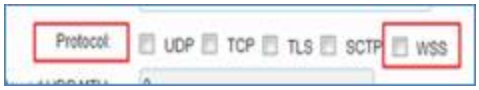
The BorderNet deployment will obviously use SIP as the signaling protocol, sent as SIP over WebSocket.

BorderNet supports the secured **WebSocket** protocol (**WSS**), for connecting with Peers.

The **WSS** is a WebSocket protocol on top of a TLS connection. When selecting WSS from the Interface configuration screen, then TLS and SRTP profile will appear as well.

Protocols implemented for **WebRTC** support include the following:

- WebSocket Secured (WSS)
- ICE-Lite
- STUN connectivity checks
- DTLS-SRTP
- RTCP-Mux
- RTCP-Based Feedback (RTP/AVPF)
  - Audio+Video
  - Transparent transfer of SDP attributes and RTCP packets



3.5.4 Rerouting

Rerouting a session means trying a new destination when the session initialization attempt towards an existing server fails. BorderNet retries all existing Egress servers when there is a failure, except for 486. To enable operators to control this behavior and provide alternate actions like REJECT, SKIP_CARRIER, REDIRECT or CONTINUE, rerouting is used.

The following session rerouting options are available:

Treatment	Functionality
Reject	Rejects the call and stops attempting further routes. An optional cause value can also be set
SKIP Carrier	SKIPs the carrier associated to the current Egress point and jumps to the next
Continue Next Route	Continues to attempt the next route identified earlier
Redirect	Ability to drop existing routes and reanalyze new routes
LNP	Dips to an External server for LNP
External Routes	Dips to an External server specified for routing destinations
Try with Transcoding	Triggers a reattempt to the existing route with transcoding
ENUM Lookup	Dips to an External ENUM Server for TEL>SIP URI translations

3.5.5 External Route Server (SIP Redirect Server)

Interconnection to an **External Route Server** is available. With this feature, operators can configure the BorderNet SBC to consult an external routing engine via the SIP INV/3xx method to receive call routing instructions in the form of route lists.

BorderNet determines the routing destinations based on the configuration in the advanced policy. Customer requests sometimes include the provision that routes from an external least cost routing server provide the destinations to route. These External Routing severs are SIP-based and in response to a request on INVITE provide routes in the form of a 302 response.

Additional features available include the following:

- Ability to control rerouting based on Cause Codes.
- Ability to lookup into the External Route Server for routes/destinations.
- Ability to identify a group of peers as carriers.
- Ability to skip peers for a given carrier.
- Ability to lookup into the external server for **Local Number Portability (LNP).**
- Ability to lookup into an in-switch LNP.
- Ability to define routing templates for a large data of rules (**Matrix** Feature).
- Policy control to reattempt a destination with transcoding.
- A failback mechanism for external route server failures.

To support this feature, the BorderNet SBC WebUI enables the modification of SIP Profiler entries and parameters to provide access and route traffic to the External Route Server.

The BorderNet SBC also supports routing using trunk group parameters as part of this feature.

3.5.6 Local Number Portability (LNP)

Local Number Portability (LNP) is a service that allows subscribers to switch local or wireless carriers and still retain the same telephone number.

BorderNet performs external lookups for LNP and one or more peers can be configured as LNP servers. If one server times out them the lookup is referred to another server. When all external servers are exhausted, the system will lookup into the advanced policy with the parameter 'LNP lookup failed.'

In the case of a 302 response where the LNP dip is performed and the number is not translated, if there is any further treatment, no advanced policy lookup is performed and the call will continue to execute the next treatment. If there is no further treatment, then an advanced policy lookup is performed.

Where the LNP lookup leads to a new translated number, then an advanced policy lookup is performed to 're-analyze' the new data and any treatment if present, will be discarded.

3.5.7 Matrix

All advanced policies define rule parameters and data for making policy decisions. With the introduction of features like **Number Translation**, **Criteria Lookup** and **Directory Lookup,** in BorderNet large data can be bulk-loaded and data kept in isolation to the policy rules, making it quick for access. Criteria Lookup allows rule parameters to have data outside of the policy.

The **Matrix** feature of the Control Switch allows multiple criteria fields defined in the policy to use bulk data configured separately. The Criteria Lookup feature allows the same, but is limited to only one field.

All rule parameters that contain 'Criteria belongs to' and 'Criteria doesn't belong to' actions support the 'Lookup into Matrix' parameter. The Matrix lookup is a Rule type, whose values are in the configured Matrix table. The treatment could be any of the possible values, thereby leaving the Matrix lookup for extracting data, rather than being limited to providing routes.

3.5.8 ENUM

BorderNet supports DNS functionality, and is also able to parse NAPTR and SRV records. This functionality has been enhanced to support **ENUM** routing and ENUM LNP functionality. The user is able to choose by configuration to apply either a SIP LNP or an ENUM LNP. An ENUM server is actually a DNS server, holding NAPTR records with E.164 to URI mappings. When LNP information is queried from the ENUM LNP server, an optional '**rn**' parameter can be added in order to indicate the desired routing for the ported number.

When sending an ENUM query to a configured ENUM server, BorderNet uses an NAPTR record type as the record requested. When an NAPTR response is received from the ENUM DNS server, BorderNet verifies that it contains the proper service parameters for ENUM, namely either 'E2U+SIP', 'E2U+pstn:tel' or 'E2U+pstn:sip'. If no service is present in the answer, or the service is different than the above types then BorderNet shall lookup the advanced policy by setting 'LNP lookup failed'.

3.5.9 GCC Version 8.2

The **GNU Compiler Collection (GCC)** is a **compiler** system produced by the **GNU Project** supporting various **programming languages**.

In the 3.8.0 release, the BorderNet GCC is upgraded to version 8.2.

GCC v8.2 improves the performance of the software transcoding in the BorderNet.

In a 3.8.0 fresh installation, the GCC is already installed, but in an upgrade from a previous release, the user is required to run the following step before the upgrade in order to install the new GCC.

In HA deployment this should first be run on standby.

- Download gcc82 from dialogic web site
- Copy gcc82libs.tar.gz to /tmp and using a "root" user run the following:
- cd /tmp
- tar xvfz gcc82libs.tar.gz -C /
- echo "/usr/local/lib64" >> /etc/ld.so.conf
- ldconfig

(ignore the following warning : "ldconfig: /usr/local/lib64/libstdc++.so.6.0.25-gdb.py is not an ELF file - it has the wrong magic bytes at the start")

- Reboot the BorderNet.

3.5.10 PostgreSQL

PostgreSQL is an **Object Relational Database Management System(ORDBMS)** with an emphasis on extensibility and standards compliance.

The Number Translation, Criteria Set and Directory Lookup DB on SQLite in Release 3.7.6 will be migrated to the **PostgreSQL DB** in Release 3.8.0.

The Number Translation data will be migrated to **PostgreSQL DB** automatically during upgrade. An export and import procedure should be manually performed for the Criteria Set and Directory Lookup data.

The data for Matrix tables will also be on the **PostgreSQL DB**.

3.5.11 BNET EDGE - HP DL20 Platform

New COTS Platform is introduce in this release patch for BNET EDGE on HP DL20 Platform.

The DL20 platform support similar features and functionality as the DL380 platform.

HPE ProLiant DL20 Gen10 Server Specifications:

- Signaling and Media Interfaces - 3 x 1 GB (1 x Private, 2 x Public)
- Management Interfaces - 1 x 1 GB (Management and HA)
- Processor - Intel® Core™ i3-8300 (4 core, 3.7 GHz, 12MB, 62W)
- Memory - 8GB
- Disk - 1TB SATA

3.6 Resolved Issues on Build 3.8.0-238

The following table lists all the resolved problems for Build 3.8.0-238

Defect	Issue	Description
21925	Directory Lookup cannot be deleted when directory has similar name with another directory and one is used in Routing Policy.	The directory and routing name comparing was wrong.
21936	SNMP-get "totalSessionSignaling" returns value 0 if totalSessionMedia is 0 because system performance table is not updated.	Updating the table when either media or signaling, or both, are presented.
22218	BorderNet - SIP 400 reject on INVITE with multipart/mixed content when ISUP part comes before SDP part.	Part of fix for TFS#12730 was causing the issue. Changed the fix so the scenario mentioned in this bug will also be taken care.
22382	In ACCESS scenario after 302 redirect new INVITE is generated with original R-URI and not using URI from Contact header in 302	Merge the fix from 3.7.5-149.
22416	BorderNet updates the C Line according to the C Line received in UPDATE , although the UPDATE is rejected by the BN	Fixed
22475	Extra Semicolon (;) is added to Diversion header when assigning via profiler value into 'counter' SipParam	Made the code changes such that when the sipparam to be modified is the last param an extra semicolon should not be added if there is already a semicolon.
22518	CS-EMS does not clear alarm "Critical System Component Failed" after standby BorderNet reset.	No traps were sent to CS if HA is disconnected - fixed
22526	Search on Peers /Interface peer are case specific, but on Directory search they aren't	Change filtering of database configuration to be also case sensitive.
22545	When the LRBT zip file is uploaded to BorderNet SBC by Customized LRBT menu, the file upload fails and the system is stuck at the "Initializing LRBT upload"	Fix AMR-NB suffix.
22546	BorderNet fails to pass SIP-I Invite parameters Content-Description and Content-Disposition from ingress to egress.	Fix in sip stack.
Defect	**Issue**	**Description**
22551	When DisableLocalCancelResp is TRUE, BorderNet does not send 487 after receiving Cancel on ingress leg for BNAP mode (CS integration) calls.	Add in Routing Service Forward INVITE 4xx Response handling for 487.

Defect	Issue	Description
22580	SIP-REC- BorderNet does not opens pinhole for incoming media after SRS returns 486 Busy here error	Sip Rec Call leg was created with Media Leg based on the Call Proc Media Leg. When the Sip Rec Call Leg is destroyed, the Media Leg was the same as in the Call Proc leg. Fix was to not relay on Call Proc Media Leg when creating the Sip Rec Call Leg.
22627	SIP Re-Invite race condition with TCS	Fix for race condition for H323->SIP Call with REINVITE from Egress before TCS/MSD ACK is awaited. Merge from 3.7.6-216. New added appparam 'disableiwffullcaps' should be set to false only in sip to H323 interworking calls.
22628	Sip Re-Invite to H323 hangs on SIP side if a=sendrecv is present	Fixed - new added appparam 'disableiwffullcaps' should be set to false only in sip to H323 interworking calls.
22698	Trunk-Authentication - cannot put "+" sign in the "Auth Username" field	+ sign support was added
22726	SIPREC metada- closing xml tag for nameID param format not comply	Change Meta data.
22757	severe leak in read buffer pool	Huge number of maxCallLeg - set maxCallLeg according to 32 CPUs
22802	SIP REC Invite to SRS - a lines in SDP set to inactive and not sendonly.	Fixed SipRecService changes.
22891	BorderNet disconnects calls having both way media while Media Inactivity Timer is set and Wireshark is used to remote trace "SignalingWithMedia"	Fixed in Kernel.
22896	BN - 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
22897	BorderNet drops t38 packets when fax mode is pass-through, FAX originating and FAX terminating ends are I-gate (SDP has X-vrzcap attributes)	Fixed- Detect t.38 packets as STAN or DTLS.
22902	Failover and Real-time Core	Lock on semaphore - set the semaphore as recursive.
22904	BorderNet is unable to send SNMP (alarm clear) packet out when nic0 port recovers link fail.	L2/L3 switch interface startup time - Add delay for link up indication in BorderNet.
22910	BNAP Egress Calls not delivering the right cause code back to the Control Switch	PE error fixed
Defect	**Issue**	**Description**
22911	SIPGW Cores in Newly Active BN4K	Fix in sip stack - New stack code merged at the beginning of 3.8.0 stored the "current received message" in the call leg object for Transaction Send Failure state change, But this type of state change was not causing to clear this temporary message from the Call Leg Object. this caused later on to use a deleted Message

Defect	Issue	Description
22912	Midlayer Core in Customer System	Same as defect 22911.
23054	SBC crash => Critical system component failed on vSBC	Same as defect 22911.

3.7 Resolved Issues on Build 3.8.0-197

The following table lists all the resolved problems for Build 3.8.0-197

Defect	Issue	Description
22575	BorderNet - INVITE rejected if combined Remote-Party-ID header present	Fixed - used contact header to parse remote-id.
22442	SIPREC Content-Type header missing boundary param.	Fixed- when re-writing the SIP content re-take the boundary as well as content type and sub type.
22631	"SIP capture" is not working properly	Fixed - only incoming sip leg was capturing
22632	BorderNet does not support Bulk delete for Number translation, Directory Lookup and Criteria Set	Adding support for Bulk delete from GUI.
22530	BorderNet does not apply media inactivity call disconnection procedure on all concurrent calls.	Fax Transcoding flag was not initialize in session manager causing media inactivity triggering randomly.
19459	PRACK not generated locally toward Egress if one side Support and other does not.	Change the behavior at Forward INVITE 1xx Response in this scenario. Fixed is merged from 3.7.0-194

3.8 Resolved Issues on Build 3.8.0-153

The following table lists all the resolved problems for Build 3.8.0-153

Defect	Issue	Description
18059	vSBC documentation requirement missing RAM as minimum 4GB but 2GB per CPU	Updated in 3.8.0 PDD document in section "Product Specifications" Minimum 8 GB or 2 GB per machine CPU (the larger of these as a minimum)
16574	IE11: Cannot edit Interface, Peer and Profiles. Firefox is OK.	Updated in the 3.8.0 Provisioning Guide and Quick Start Guide documentation. IE 11 is not supported.
22188	Merge all 3.7.6 fixes to 3.8.0 release	bug parity is as following: 3.8.0-153 <== 3.7.6-189 <== 3.7.0-188
19273	Max of 200 profiles with 100,000 records per profile and total of 4 million records per DB for NumberTranslation\Criteria Set and directory lookup.	Move to PostgreSQL DB instead of SQLite DB and remove all limitations (TFS#21885).

3.9 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.
22182	Rollback - During rollback process from 3.8.0 to 3.7.6 active calls are dropped.	
	Mirroring issue observed for transcoding calls during upgrade from 3.8.0-197 to 3.8.0-238	