Dialogic® BorderNet™ 3000 Session Border Controller

Easy-to-Manage Robust Security and Session Control for VoIP Networks

Datasheet

The Dialogic® BorderNet™ 3000 Session Border Controller (SBC) is a compact, highly reliable security and session management platform for mobile and fixed VoIP networks. The flexible and standards-based BorderNet 3000 SBC supports both access and interconnect applications in a unique, fully redundant single Rack Unit (1RU) chassis.

By effectively protecting itself and the existing interconnect and access network infrastructure, the BorderNet 3000 SBC helps ensure that VoIP services are continuously available and that performance is unaffected by outside attack. Management is streamlined and operating overhead reduced because the 3000 SBC centralizes management operations in a single interface for policy-based routing and advanced call tracing as well as fault monitoring, configuration, accounting, performance, and security functions.

Features	Benefits
Carrier-ready interconnect (I-BCF) and access (P-CSCF) SBC with five-nines availability in a 1RU	Provides high reliability while reducing capital and operational costs through its small footprint and low power requirements
SIP header and parameter manipulation	Allows rapid addition of new service provider interconnects for streamlined service deployment
Integrated GUI-based local management	Simplifies management and lowers management expense
Integrated local and remote session tracing capability for one or more platforms simultaneously	Provides advanced troubleshooting while reducing capital costs since no special equipment or network configuration is required
RTP multiplexing between units	Reduces IP overhead and bandwidth consumption for VoIP sessions by up to 70% without sacrificing voice quality

Dialogic® BorderNet™ 3000 Session Border Controller

Easy-to-Manage Robust Security and Session Control for VoIP Networks

Unique Redundancy in a Single Unit

The BorderNet 3000 SBC is unparalleled in the industry in providing a fully redundant, highly reliable session control and security platform for both access and interconnect applications in a single Rack Unit (1RU). Hitless failover and hitless software upgrades enable continuous operation with 99.999% (five-nines) availability.

The BorderNet 3000 SBC allows service providers to deploy session control and security solutions for small- and medium-sized sites with outstanding efficiency at a low cost. For larger sites, multiple 3000 SBC units can be managed easily from a single GUI-based management interface.

Built on a standalone Dialogic® platform that is field proven for high reliability, the BorderNet 3000 SBC offers the following functionality:

- IP session control
- IP session security
- SIP interworking
- Bandwidth optimization

IP Session Control

The BorderNet 3000 SBC ensures that adequate resources are always available for legitimate sessions under conditions of high load, attacks, and hardware and network failures. Delay-sensitive traffic, such as voice, receives prioritization dynamically on a call-by-call basis, and bandwidth is limited per call based on codec type. Granular media stream session control enables Service Level Agreement (SLA) requirements to be met for high customer satisfaction.

IP Session Security

The BorderNet 3000 SBC implements a comprehensive and systematic approach to security and service assurance. Every incoming IP packet is processed through a series of checks, classifications, and controls to allow only the processing of valid traffic flows according to SLAs, while malicious traffic is dynamically blocked.

The BorderNet 3000 SBC establishes a security perimeter around the NGN hat identifies and prevents attacks such as Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) from wasting network resources and potentially halting services completely. Every SIP message is checked for both syntax and semantics while access control and topology hiding further enhance security on a per user or application level.

SIP Interworking

As SIP networks proliferate and new SIP-oriented business opportunities arise, service providers must be able to rapidly interwork with new SIP application platforms, carrier interconnects, and SIP endpoints. The “Profiler” function of the BorderNet 3000 SBC enables SIP header and parameter manipulation for both incoming and outgoing SIP messages on any 3000 SBC configured with a SIP interface.

The Profiler enables header changes to be made up to three times for each SIP message in each of these situations:

- When a SIP message is received on an interface (incoming)
- As a routing rule treatment for I-BCF routing policies
- Before a SIP message is about to leave from an interface (outgoing)

Any SIP header field may be manipulated, such as a header value, header parameter, and URI parameter. Because the Profiler is very flexible, rapid interworking is enabled between any type of SIP network.

Bandwidth Optimization

High bandwidth costs for international and long-distance remote links or leased lines increase operational costs for VoIP service delivery. A payload aggregation feature based on RTP multiplexing minimizes bandwidth requirements between BorderNet 3000 SBCs, reducing recurring operational costs. Payload aggregation also creates higher transmission efficiency by stacking multiple voice call streams in each packet, allowing shared overhead that has almost no impact on end-to-end delay. Because payload aggregation is router-agnostic, any router can handle RTP multiplexed IP packets without special configuration or provisioning.

Figure 1 provides an example of how BorderNet 3000 SBCs can be used in a service provider network.

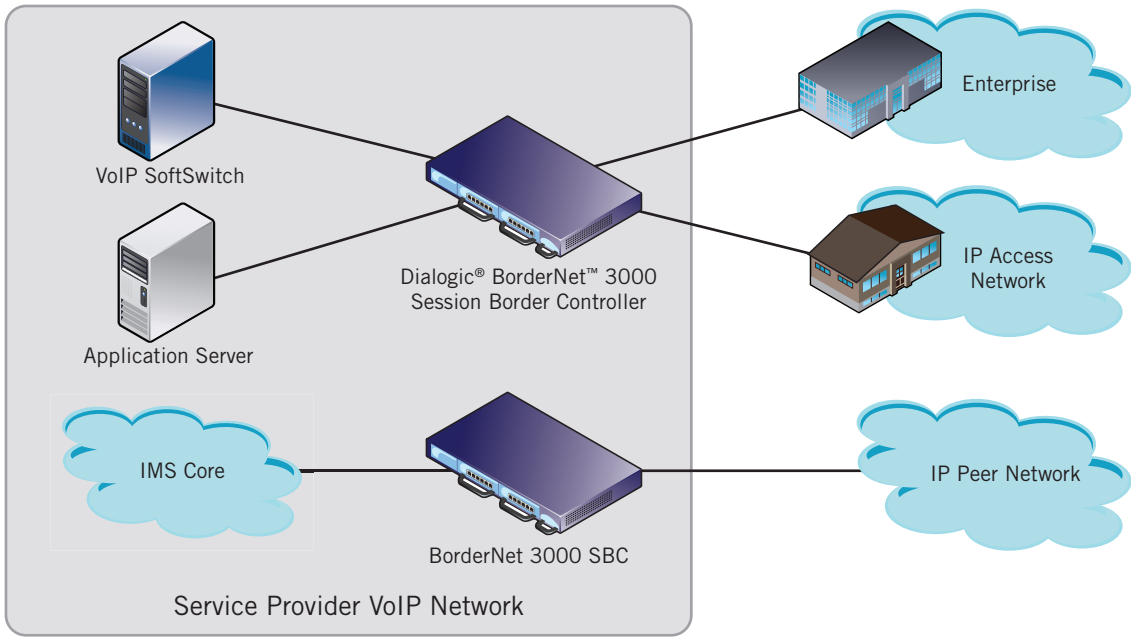

Figure 1. Dialogic® BorderNet™ 3000 Session Border Controllers in a Service Provider Network

Dialogic® BorderNet™ 3000 Session Border Controller

Easy-to-Manage Robust Security and Session Control for VoIP Networks

Technical Specifications

SIP Protocols

SIP Proxy operational mode

RFC3261 Session Initiation Protocol

RFC3262 Reliability of Provisional Responses in SIP

RFC3264 An Offer/Answer Method with SDP

RFC2976 SIP INFO Method

RFC2327 Session Description Protocol (SDP)

RFC2112 Multipart MIME

RFC2617 HTTP Digest Access Authentication

RFC3311 Update

RFC3326 Reason

RFC4244 Diversion

RFC3323 Privacy

RFC3324 Privacy

RFC3325 Privacy

RFC3725 3pcc

RFC3966 tel URI

RFC4694 Number Portability

RFC3515 Refer

RFC4028 Session Timer

RFC2046 Mime handling

RFC3455 P-Headers

Other Protocols

IPv4

RFC768 User Datagram Protocol (UDP)

RFC1889 Real-time Transport Protocol

RFC1890 RTP Profile for Audio and Video Conferences

Security

Access control: Signaled pinhole firewall for media

Network topology hiding via double NAPT for both media flows (Layer 3) and signaling messages (Layer 5)

Network-based NAT traversal

DoS and overload protection for service infrastructure: Rate limiting of signaling messages and media flows

White/black/gray IP address lists

Technical Specifications *(continued)*

Session Admission Control

Based upon maximum number of calls configured per public interface

VLAN Bridging

802.1q (VLAN)

Up to 16 configurable VLANs

Bandwidth Policing

Intelligent dynamic rate limiting per media flow

Media flow rate limiting for authorized sessions based upon the "b" session descriptor

Law Enforcement

Media forking for lawful intercept requirements such as CALEA

SIP Routing

SIP message routing

Interface-to-interface routing

Enhanced routing based on SIP headers (Contact, From, To), time-based conditions, transport addresses

Load balancing and priority-based rerouting

Routing decision-based keep-alive to remote peers

Media Routing

Disable or enable media routing through Dialogic® BorderNet™ 3000 Session Border Controller (SBC)

Separate VLANs supported for signaling and media

Media NAT traversal

Accounting

FTP text-based CDR: Creates text files with comma-separated CDR and transfer them to external FTP servers

CDR session attributes: Includes general session attributes and signaling and media session information

QoS Reporting

QoS statistics: Delay, jitter, and packet loss

Traffic statistics: Total packets and octets transferred

Used for SLA reporting via RADIUS CDR, problem alerting and isolation via SNMP

Technical Specifications *(continued)*

Performance and Capacity

2 Gbps chassis throughput

Signaling latency 1-5 msec

Media latency 2 msec

Maximum INVITE sessions = 8,000 (licensed sessions)

Maximum SUBSCRIBE sessions = 24,000

Maximum SBC sessions = 32,000 (INVITE + SUBSCRIBE)

Maximum registered users (private and public): 50,000

Configuration

Integrated browser-based GUI (HTTP)

xMS centralized management system (optional)

Management

SNMP v2.0 (get/set/trap commands)

Northbound interface to xMS centralized management system enables the following capabilities:

- Traffic Reports: Backup to xMS database
- Configuration Parameters: Can be uploaded to xMS disk
- Various Utilities (Audit logs): SBC local disk backup via xMS

Power Specifications

Power supplies	Redundant power supplies (active/standby) and power feeds
AC power option	Nominal Voltage Input: 100/240 VAC Maximum and Minimum Voltage Input: 90/254 VAC Maximum Power Consumption: 95 Watts Frequency: 50/60 Hz Current: 1.5 amps maximum
DC power option	Nominal Voltage Input: -48/-60 VDC Maximum and Minimum Voltage Input: -40.5/-72 VDC Maximum Power Consumption: 73 Watts Current: 2.7 amps maximum

Technical Specifications *(continued)*

Physical Specifications

Dimensions	1.75 in. H x 17.13 in. W x 13.78 in. D 44.45 mm H x 435 mm W x 350 mm D
Weight	8.8 lbs 3.98 kg
Cabinet	19 or 23 in.
Network Interfaces	Media/Signaling: 2 Gigabit Ethernet (copper) — active 4 Gigabit Ethernet total — HA IEEE 802.3u Full Duplex Management: 1 x 100Base-T

Approvals, Compliance, and Warranty

Hazardous substances	RoHS compliance information at www.dialogic.com/rohs
Country-specific approvals	Contact your local Dialogic sales representative
Warranty	Contact your local Dialogic sales representative

Dialogic®

www.dialogic.com

Dialogic Inc.
926 Rock Avenue
San Jose, California 95131
USA

12/10 12119-02