Session Border Controllers: A Primer

Why SBCs are indispensable for any IP real-time communications network

ORACLE WHITE PAPER | JULY 2017

Introduction

This white paper provides basic knowledge and understanding of the need for, and capabilities of, the network element known as a session border controller (SBC). The paper is divided into two parts.

Part 1 describes what drove, and continues to drive, the need for SBCs, including

» The respective abilities of the Public Switched Telephone Network (PSTN) and Internet Protocol (IP) network, including the internet, to effectively control and transport interactive communications
» The basic components and methods used in session-based IP communications
» The roles and limitations of other network elements used in IP communications

Part 2 provides basic information about SBCs, including where they are typically deployed in the network and the set of functions they deliver. The paper concludes with an overview of Oracle Communications network session delivery and control infrastructure products and platforms.

Part 1: A Tale of Two Networks

Voice and data services and applications have traditionally been delivered over disparate networks—voice over the PSTN; private networks based on time-division multiplexing (TDM) technology; or data over IP networks, such as enterprise local area networks (LANs), private wide area networks (WANs), and the public internet.

TDM networks such as the PSTN were created decades ago to provide seamless, reliable, and secure global voice communications services—with an emphasis on the word voice. These networks deliver high reliability and security for users in activities such as banking and commerce. TDM networks, however, are limited in their ability to support high-bandwidth video and other interactive multimedia services.

IP networks have historically provided global reach for a broad range of information services such as e-mail, Web browsing, electronic commerce, and research. IP is a data-oriented protocol that provides global addressing among computers. The service quality over IP networks, although adequate for these types of information services, can vary significantly, depending on factors such as available bandwidth, web server activity, the number of active users at any given time, and the activity being performed.

Although IP networks are capable of cost-effectively transmitting any form of traffic that is IP-based—including interactive voice, video, and data—many IP networks, especially the Internet, transmit only on a best-effort basis in which all forms of traffic have equal priority. This can result in significantly varying degrees of perceived quality for the same or similar types of traffic transmissions.

In addition, IP communications, unlike those over “closed” networks such as the PSTN, are subject to disruptive and fraudulent behavior, including identity theft, viruses, unsolicited e-mail (spam), unauthorized use, and attempts to circumvent or bypass security mechanisms associated with those services (hacking). Although internet users have adopted many security measures to protect themselves, their networks, and their websites, these current measures are not adequate to provide highly secure, real-time interactive communications.

Evolution to a Converged IP Network

IP networks can be designed and operated more cost-effectively than TDM networks. In addition, IP networks can deliver converged voice, video, data services, and applications to businesses and consumers. Many leading service providers are leveraging IP Multimedia Subsystem (IMS), an IP-based service delivery architecture developed and standardized by the Third-Generation Partnership Program (3GPP), as a means for effectively and efficiently delivering IP communications services globally. Enterprises are searching for ways to unify their communications by seamlessly integrating voice, video, instant messaging, and collaboration while reducing costs.

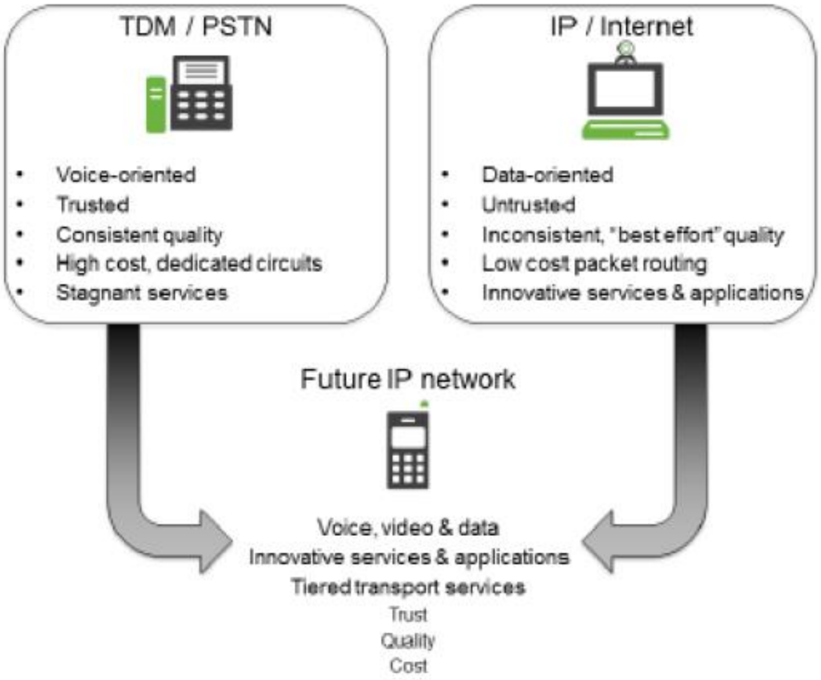

Figure 1: Service providers and enterprises are migrating from traditionally disparate networks to a single IP network architecture

Managing two distinct networks—TDM and IP—is not a viable economic proposition, so service providers and enterprises have begun to migrate to a single IP network architecture as the foundation for their next-generation services and applications. To successfully transition to a single IP network, however, they must maintain the same reliability, quality, and security that have exemplified their delivery of voice services for decades.

Challenges of Delivering Interactive Communications over IP

IP networks were initially designed to provide reliable delivery of data services such as file downloads and web interactions, which are not sensitive to latency or time delay. If data packets are lost or misdirected, an IP network will exhibit tremendous resilience in retransmitting and eventually executing the desired user request—a generally acceptable result for these types of services. However, IP networks have historically not guaranteed secure delivery of high-quality interactive communications such as voice and video.

A session is a communications interaction that has a defined beginning and end and is effective only when transmitted in real time without latency or delays. Enabling session-based communication requires control of the session from its origination point to its defined endpoint. However, no single IP network extends far enough to enable that level of control, and the internet lacks the fundamental quality of service (QoS) and security mechanisms necessary to consistently deliver the security and quality that users expect for real-time multimedia communications.

What is a session?

A session is a communications interaction that has a defined beginning and end and is effective only when transmitted in real time without latency or delays. Enabling a session-based communication requires control of the session from its origination point to its defined endpoint.

To gain the acceptance of users, service providers and enterprises must be able to assure secure and high-quality interactive communications end-to-end as sessions traverse multiple IP networks.

Managing Session-Based Communications

To provide secure and high-quality interactive communications, IP networks must be able to manage and integrate the communication flows that constitute a session. Each session includes three sets of bidirectional communication flows:

- **Session signaling messages** – messages used to initiate, modify or terminate a session
- **Media flows** – data packets containing the actual media being exchanged
- **Media control messages** – messages used to compile information to report on QoS levels

A session is initiated with signaling messages. These messages establish a virtual connection between the participants' personal computers, IP phones, or other endpoints. In addition, they negotiate the IP addresses used for the session's media streams and control the messages and algorithms (codecs) used to digitize analog voice and video.

Various codecs are available for voice and video transmission, each offering trade-offs between quality and bandwidth efficiency. Once the call is initiated, media streams and control messages flow in both directions between participants. Signaling messages are also used to transfer a call, place a call on hold, and terminate a session.

Every session includes three sets of bidirectional communication flows:

Session signaling messages
Media flows
Media control messages

The management of session-based communications is complicated by the following characteristics of today's IP networks:

- The identities of the participants are difficult to ascertain, and security needs are complex
- The number of session signaling protocols, codecs, and related standards continues to grow
- Addressing schemes are not consistent or compatible across networks
- Bandwidth and signaling element resources are finite
- Interactive communications service provider business models and regulatory compliance requirements continue to evolve and require network flexibility.

Additionally, unlike typical data communications, not all session-based communications can be treated with the same priority. For example, an emergency services (911) call or a high-quality enterprise videoconference should take priority over watching TV.

Limitations of Existing Network Elements

Successful session-based communications requires tight integration between signaling and media control. However, existing network elements such as soft-switches, IP private branch exchanges (PBXs), Unified Communications (UC) servers, routers, and data firewalls do not provide the control functions required for session-based communications.

- » **Soft-switches, IP PBXs, and UC servers**. Soft-switches, IP PBXs, and UC servers set up interactive communication sessions with signaling protocols such as Session Initiation Protocol (SIP), H.323, Media Gateway Control Protocol (MGCP), and H.248. Session agents associated with these protocols process only signaling messages while performing a variety of signaling-based functions, such as user registration, authentication, authorization, and session routing based on telephone numbers or SIP addresses

  These session agents do not currently provide functions related to media control for interactive communication sessions or protection against signaling-based denial of service and distributed denial of service (DoS/DDoS) attacks. DoS/DDoS attacks prevent network equipment from receiving legitimate network traffic, by flooding the network with unrequested information or inundating targeted equipment with noncompliant-protocol messages
- » **Routers**. Routers make simple routing decisions for discrete IP packets based on IP addresses but do not participate in call signaling and are therefore unable to recognize the multiple individual data packets that make up a session. Without signaling intelligence, routers are currently unable to perform key border control functions such as signaling overload prevention or session routing based on quality and cost requirements.

  Routers may use several QoS technologies, such as Multiprotocol Label Switching (MPLS), differentiated services (DiffServ), and Resource Reservation Protocol (RSVP), to grant preferential treatment to certain IP packets.

  However, routers using these technologies are currently incapable of classifying all the communications flows associated with a single session and handling those communications flows correctly as a single entity. Without the ability to identify the multiple individual packets that constitute a session, control call signaling, or understand the access link capacity and utilization, the router is unable to make any call admission or rejection decisions.

  Thus, the router will continue to send packets along a path even though the session should have been rejected because the quality was insufficient for the requested session. When this overloading occurs, not only is the quality of the session associated with that packet unacceptable but other sessions using that same path also suffer degradation.
- » **Data firewalls**. Data firewalls are the most common security element in IP networks. Firewalls work by allowing only inbound traffic that has been requested from inside the network and by presenting a single IP address for all the personal computers, phones, and other devices behind it. The firewall effectively blocks session-based communications, because it does not allow incoming calls from unknown endpoints.

  Like the router, the firewall is unable to group the multiple media flows associated with a single session and apply a consistent policy. Furthermore, firewalls can’t identify and protect against service overloads or DoS/DDoS attacks on other signaling elements such as soft-switches.

Part 2: An Introduction to Session Border Controllers

Session border controllers enable the delivery of secure, high-quality interactive communications across multiple IP networks.

For a service provider, these include the separate IP networks that constitute fixed-line, mobile, and cable networks. SBCs are deployed at the borders between IP networks, such as between two service providers or between a service provider and its enterprise, residential, or mobile customers.

For an enterprise, SBCs are used to interconnect communications “islands” that exist within the enterprise, connect the enterprise to a wide area service designed for interactive communications (such as a SIP trunk), or enable “federations” between multiple enterprises for B2B communications. Enterprise SBCs (E-SBCs) also enable selected remote locations or mobile workers to securely access enterprise interactive communications services via the internet.

SBCs are the only network element capable of integrating the control of signaling messages and media flows used by interactive communications. This capability complements the roles and functionality of routers, soft-switches, and data firewalls that operate within the same network.

SBCs support a broad range of next-generation services and communications applications, providing key control functions for enterprises and service providers alike to uniquely ensure

- Security
- Interoperability and service reach maximization
- Quality of experience (QoE), availability, and service-level agreement (SLA) assurance
- Service revenue optimization and cost management
- Regulatory compliance

What makes SBCs different?

SBCs are the only network element capable of integrating the control of signaling messages and media flows used by interactive communications. This capability complements the roles and functionality of routers, soft-switches, and data firewalls that operate within the same network.

The Evolution to SBC-Enabled IP Communications

Prior to the advent of the SBC, IP network infrastructure equipment (such as that discussed in Part 1) could initiate and route undifferentiated data but lacked the ability to specifically target the management of interactive communications sessions. The development of the SBC, unlike many other emerging networking products, was not initially catalyzed by standards bodies. Rather, SBCs came about as the result of pragmatic needs of service providers and enterprises that were not met by other types of network elements.

To date, SBCs (now more frequently recognized by standards bodies) have been deployed around the world to support next-generation interactive communications services and applications such as Voice over Internet Protocol (VoIP), video-conferencing, instant messaging (IM), and presence as well as the routing of voice conversations over private as well as public IP networks, including the internet.

SBC Deployment at Access, Interconnect, and Trunking Borders

SBCs are deployed at the borders of IP networks. The border between two service providers is referred to as an interconnect border; the border between a service provider and its enterprise, residential, or mobile customers is referred to as an access border. Enterprises also deploy E-SBCs at the border between their IP network and their service provider’s network, referred to as the trunking border.

The border between enterprise data centers and their employees is referred to as the enterprise access border. SBCs act as the source and the destination for all signaling messages and media streams entering and exiting the network. To that end, SBCs complement rather than replace existing network and service infrastructure.

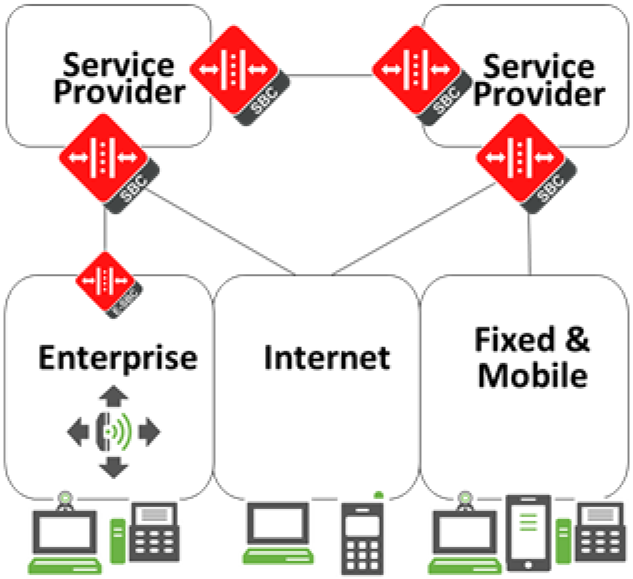

Figure 2: SBCs are deployed at enterprise and service provider network borders

At all borders, SBCs are deployed in front of session agents—such as soft-switches, IMS Call Session Control Function (CSCF) elements, IP-enabled mobile switching centers (MSCs), IP PBXs, UC servers, and application servers—and make call acceptance or rejection decisions. This protects the session agent from signaling attacks initiated by hackers and from non-malicious overloads. It also ensures that calls are accepted only when adequate network quality and soft-switch resources are available.

At many borders, SBCs function in parallel with data firewalls, which protect web and application servers and PCs from attacks while the SBC protects session agents. SBCs augment the simple, discrete, packet-by-packet routing decisions that routers make. Unlike routers, SBCs classify flows as interactive communication sessions and make more intelligent routing decisions to ensure secure, high-quality communications.

SBC Functions

SBCs apply controls to signaling and media flows as they traverse network borders, enabling the effective delivery of session-based IP communications. For service providers, these controls fall into five basic categories: security, service reach maximization, SLA assurance, revenue optimization and cost efficiency, and regulatory compliance.

- **Security**. SBCs protect themselves, session agents, and other elements of the service delivery infrastructure as well as customer networks, systems, and relationships. They protect customer networks and session privacy and provide DoS/DDoS protection from attacks and non-malicious overloads
- **Interoperability and service reach maximization**. SBCs extend the reach of IP communications services and applications by maximizing the different types of networks and devices supported

  SBCs enable sessions to traverse existing data firewall and network address translation (NAT) devices and to bridge networks that use overlapping IP addresses, virtual private networks (VPNs), and IPv4 and IPv6 addresses.

  SBCs can also mediate between different signaling, transport, and encryption protocols; convert between incompatible codecs; and translate signaling layer telephone numbers, addresses, and response codes.
- **Quality, availability, and SLA assurance.** SBCs play a critical role in assuring session capacity and quality. They perform admission and overload control to ensure that both the network and the service/application infrastructure have the capacity to provide high-quality support for sessions.

In IMS networks, they also integrate with standard admission control functions such as the Policy Charging and Rules Function (PCRF) and Resource and Admission Control Subsystem (RACS). Additionally, SBCs control the quality of network transport and monitor and report actual session quality to determine compliance with performance specifications set forth in SLAs between service providers or enterprises and their users.

» **Revenue optimization and cost management.** SBCs can help service providers increase revenues and profits by protecting against bandwidth and QoS theft, by routing sessions to minimize costs, and by providing accounting and related mechanisms to maximize the number of billable sessions.

They also help enterprises manage costs by consolidating network infrastructure and increasing the efficiency of bandwidth utilization. Enterprises can leverage SBCs to simplify the introduction of new UC applications that improve business processes, to increase customer satisfaction, or to maintain competitive differentiation.

» **Regulatory compliance.** SBCs enable service providers and enterprises to comply with government-mandated regulations worldwide, including emergency services (such as E-911) and lawful intercept, which involves law enforcement agencies' electronic surveillance of circuit and packet-mode communications, as authorized by judicial or administrative orders (such as the Communications Assistance for Law Enforcement Act [CALEA]).

SBCs deliver wide-ranging controls in many functional areas:

Security
Interoperability
Service reach maximization
Quality
Availability
SLA assurance
Cost management
Revenue optimization
Regulatory compliance

Session Border Controllers from Oracle

Oracle's SBCs are a combination of powerful full-featured software that operates on hardware platforms specifically engineered and optimized to assert the critical functions necessary for controlling session-based communications without adding quality-degrading latency, jitter, or delay to the bidirectional media flows that constitute those communications. These systems deliver the highest-quality border control functionality, performance, capacity, scalability, availability, and manageability while enabling service providers and enterprises to deliver high-quality, secure, real-time, interactive communications.

Acme Packet OS is the operating software on which Oracle's SBCs are based. It offers rich border control functionality in terms of architectural flexibility, signaling protocol breadth, control function, and feature depth, and carrier-class availability and manageability.

Acme Packet OS supports all five required border control functions:

» **Security**. Net-SAFE, Oracle's SBC security framework, defines the SBC functions necessary for protecting service delivery infrastructure, customer/subscriber networks, systems, and relationships with support for DoS/DDoS protection, access control, topology hiding, session privacy, VPN separation, service infrastructure DoS/DDoS prevention, and fraud prevention

» **Interoperability and service reach maximization**. Oracle's SBCs extend the reach of IP communications by resolving differences between the many types of networks and devices supported. Critical features include

    - NAT traversal (the ability to enable communication sessions to be carried over existing data firewall and NAT devices)
    - Bridging of private and public IPv4 and IPv6 address spaces
    - Interworking between VPNs, signaling, encryption, and transport protocols
    - Transcoding
    - Translation of number, address, and response codes
- **Quality, availability, and SLA assurance**. Oracle's SBCs support several features designed to guarantee session capacity and quality. These features include
    - Rerouting around failed links or upstream elements
    - Admission control based on signaling element load, bandwidth availability (including policy server interfaces), and observed QoS
    - QoS marking and mapping
    - QoS reporting
- **Revenue optimization and cost management**. Oracle's SBCs include features that help service providers and enterprises maximize revenues and minimize network CapEx and OpEx. To protect against revenue leakage from service theft, Oracle's SBCs feature
    - Bandwidth policing
    - QoS theft protection
    - Accounting
    - Session timers
    - Least-cost routing
    - Load balancing

    Support for virtual SBCs is yet another capability designed to help enterprises and service providers minimize costs.
- **Regulatory compliance**. Oracle's SBCs enable compliance with government-mandated regulations worldwide, including emergency services (such as E911), the Government Emergency Telecommunications Service (GETS), and lawful intercept (such as CALEA in the United States).

Other features of Oracle's SBCs include the following:

- **Multiprotocol support**. A broad range of signaling protocols enables interworking, load balancing, and routing.
- **Programmable signaling manipulation**. Oracle's SBCs offer powerful, flexible capabilities for inspecting and manipulating any field in SIP headers as well as protocols transported by SIP, such as Session Description Protocol (SDP) and ISDN User Part (ISUP). In this way, Oracle's SBCs address a practically unlimited range of signaling interworking and interoperability challenges.
- **High availability**. Oracle's SBCs protect against loss of service in the event of hardware or software failures. The checkpointing of media, signaling, and configuration state is designed to prevent loss of active calls or to provide support for new call requests.
- **Management**. Oracle's SBCs provide a comprehensive collection of element management tools and operational support system interfaces.

***Oracle Communications SBCs feature**:*

Support for all five types of required border control functions
Multiprotocol support
Architectural flexibility
Programmable signaling manipulation
High availability
Strong management

Oracle Communications SBC Purpose-Built Platforms

Oracle Communications SBC hardware platforms address a broad range of performance, capacity, and bandwidth requirements:

- **Acme Packet 4600**. This platform is the new generation Oracle Communications product in mid-tier service provider and larger enterprise IP real-time communications deployments. Its unique hardware design is purpose-built to control complex, high volume signaling and media traffic at network borders. Its network interface unit (NIU) offers 1 Gbps or 10 Gbps connectivity and integrated acceleration for encryption and transcoding. Acme Packet 4600 also features carrier-grade high availability (HA) and is compliant with stringent Network Equipment Building Systems (NEBS) standards, ensuring nonstop operation and survivability in business-critical environments.
- **Acme Packet 6100**. This platform is based on a new generation of hardware design that leverages state of the art components and 64-bit symmetric multiprocessing in a modular system designed from growth and flexibility. Its rear slots accommodate dual-port 10GB/sec network interface units (NIUs). The Acme Packet 6100 provides for flexible deployment at high-volume network access or interconnect borders or within the service provider signaling core.
- **Acme Packet 6300**. This groundbreaking platform offers the highest levels of performance, availability, and capacity to service providers. Its 3U modular chassis accommodates multicore symmetric multiprocessing, 10 Gbps I/O, ultra-high-capacity transcoding, and encryption hardware to support future-generation services such as Voice over LTE (VoLTE), HD VoIP, and high-volume video calling.

Oracle Communications SBC as a Virtual Network Function

Network Functions Virtualization has been gaining substantial mindshare in the past few years ever since the 2012 publication of a white paper from a group of network operators and the subsequent formation of an ETSI Industry Specifications Group (ISG). Virtualized network functions have several advantages over their purpose-built counterparts including network agility, elasticity, and reduction in capital and operational expenses as these functions run on commercial hardware. However, for SBCs, virtualization comes with a lot of challenges regarding the CPU intensive nature of the functions it performs and the expectation that these functions be performed at near wire-speed to maintain its strict performance criteria.

Oracle Communications SBC is offered as a virtualized network function (OCSBC-VNF) and certified to run on commercial off-the-shelf (COTS) x86 based platforms. OCSBC-VNF utilizes several advanced technologies to perform those functions in software that were done using hardware acceleration on purpose-built platforms. Some of these capabilities and how operators can introduce SBC-VNF into their networks is described below.

- **Faster packet processing**: OCSBC-VNF uses Intel’s Data Plane Development Kit (DPDK) libraries for maximizing packet processing and throughput. OCSBC-VNF also offers a choice of network I/O drivers including those that help cut through the several software layers inherent in a virtualized platform and enable applications quicker access to data

- **Separation of workloads**: To minimize potential interference between distinct SBC functions, OCSBC-VNF separates these functions out to different vCPU cores. The result is that these time-critical threads are not swapped in and out and achieve maximum performance. OCSBC-VNF defines “D” cores for DoS and DDoS protection, “S” cores for signaling traffic, “F” cores for forwarding or media traffic, and “X” cores for transcoding
- **Affinity placements**: In addition to separating out tasks among vCPUs, OCSBC-VNF also ensures that the right task is assigned to the right vCPU that will maximize its performance by the underlying Linux OS
- **Software and pooled transcoding**: OCSBC-VNF can perform transcoding between the most popular codec pairs in software using dedicated vCPU cores. For scale, for codecs that are not supported in software, and for efficiency purposes, it can utilize an offboard DSP bank in an Acme Packet platform
- **Orchestration**: OCSBC-VNFs may be created or terminated automatically depending on demand under software control with a process known as orchestration. OCSBC-VNF provides the hooks necessary for integration with popular open-source orchestrator available in the marketplace

Conclusion

Service providers and enterprises have begun to migrate to a converged IP network and are seeking ways to unify their communications by seamlessly integrating voice, video, instant messaging, and collaboration while reducing costs. Managing and integrating session-based communications effectively and securely is challenging, and the existing network elements have limitations. However, SBCs enable the delivery of secure, high-quality interactive communications across multiple IP networks and are the only network element capable of integrating the control of signaling messages and media flows used by interactive communications.

Oracle’s SBCs deliver high-quality border control functionality, performance, capacity, scalability, availability, and manageability while enabling service providers and enterprises to deliver high-quality, secure, real-time, interactive communications.

References

Oracle Communications Session Border Controller Website:
https://www.oracle.com/industries/communications/service-providers/products/session-border-controller.html

Oracle Communications Session Border Controller Product Documentation:
http://docs.oracle.com/en/industries/communications/session-border-controller/index.html

Network Functions Virtualization Whitepaper: https://portal.etsi.org/nfv/nfv_white_paper.pdf

ORACLE®

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

B blogs.oracle.com/oracle

f facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

Session Border Controllers: A Primer
July 2017