



The Network-adaptive Border Controller:
The Smart Network Approach to Security for Voice over IP Networks

Copyright © 2008 Veraz Networks, Inc. All rights reserved. Veraz Networks and the Veraz Networks logo are trademarks or registered trademarks of Veraz Networks or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Information in this document is subject to change without notice. Veraz Networks assumes no responsibility for any errors that may appear in this document.

Table of Contents

1. Executive Summary	1
1.1. <i>Overview</i>	1
1.2. <i>The Shortcomings of Today's Session Border Controllers</i>	1
1.3. <i>The Veraz Network-adaptive Border Controller</i>	1
2. Security Requirements for Service Provider IP Networks	2
2.1. <i>Security</i>	2
2.2. <i>Connectivity</i>	3
2.3. <i>Service Assurance</i>	3
2.4. <i>Network Cost Optimization</i>	4
2.5. <i>Regulatory Compliance</i>	4
2.6. <i>OA&M Support</i>	4
2.7. <i>Summary</i>	5
3. Veraz Network-adaptive Border Controller (N-aBC) Overview	5
3.1. <i>Network-adaptive Border Controller Integrated (N-aBC INT)</i>	6
3.2. <i>Network-adaptive Border Controller Distributed (N-aBC DST)</i>	6
3.3. <i>N-aBC Key Benefits</i>	6
3.4. <i>Veraz N-aBC Common Feature Description</i>	8
3.4.1. <i>Security</i>	8
3.4.2. <i>Connectivity</i>	8
3.4.3. <i>Service Assurance</i>	9
3.4.4. <i>Network Cost Optimization</i>	9
3.4.5. <i>Regulatory compliance</i>	9
3.4.6. <i>OA&M Support</i>	9
4. Summary	10

1. Executive Summary

1.1. Overview

This whitepaper describes Veraz Networks' Network-adaptive Border Controller (N-aBC), a service provider next generation security solution that offers a fundamentally new and improved approach to security and session management over today's Session Border Controllers (SBCs).

1.2. The Shortcomings of Today's Session Border Controllers

One of the key issues carriers are grappling with is how to ensure that their networks and applications will be secure when they are directly connected to other service provider's IP networks and the public internet. The open nature of IP networks is such that the security challenges are significantly more complex than for TDM networks; Session Border Controllers (SBCs) were originally developed to address this complexity.

SBCs are now being used in increasingly complex deployments exposing key gaps in their functionality and architecture, such as:

- No support for SS7-based services either through SIP-I or SS7 to SIP/H.323 interworking
- No security for web-services protocols (e.g. HTTP, DNS, XCAP, MSRP)
- Additional operational complexity and cost because they are not integrated into the core call control and management platform
- Sub-optimal security, routing, service quality and service assurance because they do not have access to network-wide real-time information
- Increased network costs through sub-optimal routing decisions and use of network resources

The long-term role of SBCs is now being actively debated within the industry, and service providers are searching for solutions that address their near-term needs and will gracefully evolve to support their next generation network architecture.

1.3. The Veraz Network-adaptive Border Controller

The Network-adaptive Border Controller (N-aBC) is designed to address the short-comings of today's SBCs and provide a true next generation security and session management platform. The N-aBC supports two distinct configurations: the integrated N-aBC (N-aBC INT) for compact access and peering applications and the distributed N-aBC (N-aBC DST) for large scale network peering applications. Some of the unique capabilities built into the N-aBC include:

- **Integrated support for both SIP/H.323 and SS7 services** enabling service providers to fully leverage their investment in TDM services as they migrate toward an all-IP next generation network
- **Built-in security for web-services based applications** enabling service providers to protect their call session handling infrastructure as well as their applications
- **Centralized routing and session management** providing real-time global optimization of session handling, resulting in lower network costs and higher quality services
- **Centralized local and global security and call-admission control policies** significantly simplifying the management of security policies while increasing their granularity and effectiveness
- **Industry leading VoIP compression without sacrificing voice quality** dramatically lowering network transport costs and minimizing the risks of network congestion or overload
- **Application-independent security and session management** simplifying the development and management of new applications
- **Centralized, network-wide, operations support** lowering the cost to deploy, maintain and manage both TDM and IP services

The N-aBC addresses the key shortcomings in current generation SBCs, provides significant additional benefits and delivers graceful network evolution for service providers.

2. Security Requirements for Service Provider IP Networks

Communications service providers, faced with ever increasing pressure from non-traditional, internet-based competitors, are focused on how to migrate their business from one based on a legacy circuit-switched infrastructure to one based on IP. While next generation standards such as ETSI TiSPAN, 3GPP IMS and CableLabs' PacketCable™ have provided a potential blueprint for an all-IP next generation network, the challenge remains how to get there from today's network, and progress has been at best slow.

One of the key issues carriers are grappling with as part of this process is how to ensure that their networks and applications will be secure when they are directly connected to other service provider's IP networks and the public internet. While traditional TDM networks required security measures, the open nature of IP networks is such that the security challenges are significantly more complex.

For example, when the first VoIP services were launched, service providers typically interconnected with other carriers using back-to-back TDM-IP media gateways which provided a natural and familiar security barrier. Unfortunately, while the use of TDM-IP media gateways between networks did address service provider's security concerns, it increased their costs and in many cases significantly lowered the quality of the VoIP services. The cost of media gateways and decrease in quality has led many service providers to directly interconnect their IP networks to other carriers, their end customers and the public internet (see Figure 1), which has raised the question again of how to ensure telecom-grade security.

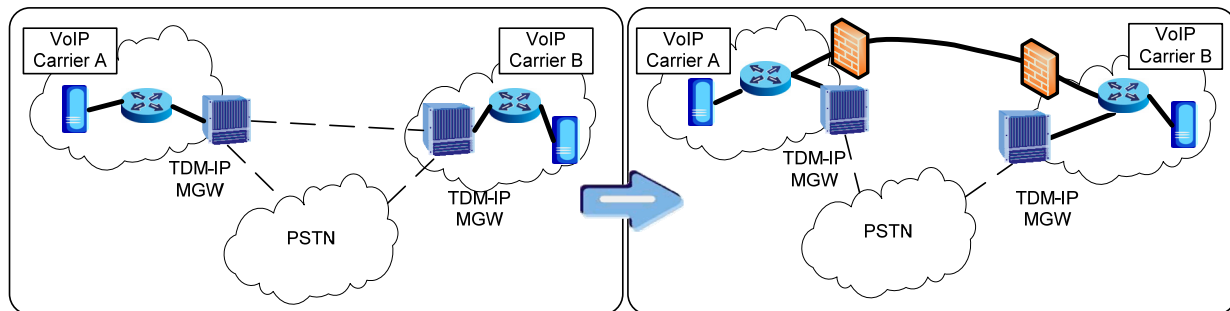


Figure 1 Carriers are moving to directly interconnect their VoIP islands

Session Border Controllers (SBCs) were developed in response to this need. The capabilities provided by SBCs can be grouped into the following six categories:

- Security
- Connectivity
- Service assurance
- Network cost optimization
- Regulatory compliance
- OA&M support

Each of these categories and the degree to which SBCs are able to meet service provider's needs are described in the following sections.

2.1. Security

Today's SBCs provide a number of security capabilities that include: protection from Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, encryption of media and signaling traffic, internal network topology hiding, fraud prevention, call admission control, subscriber authentication, maintenance of subscriber privacy, and detection and rejection of mal-formed SIP and H.323 signaling messages.

While these capabilities have enabled service providers to begin to directly interconnect their IP islands, current generation SBCs are still missing additional security features required. The following examples detail the gaps in existing SBCs:

- SBCs are entirely focused on providing security for SIP and H.323 based services and provide no support for SS7-based applications. The legacy circuit-switched network is not going away, and service providers will need to leverage their investment in SS7/IN based services for many years to come. This implies that in addition to supporting SIP and H.323, service providers need to provide equivalent security for applications that are actually SS7-based but carried in SIP (i.e. SIP-I)
- SBCs typically only provide syntactical checking of SIP and H.323 messages. As hackers get more and more sophisticated, security attacks will increasingly be based on semantic not syntactical holes.
- SBCs do not provide security for web-services based applications. While SIP and H.323 are key protocols for enabling VoIP services, service providers today are increasingly focused on web-like services that rely directly on web-services protocols (e.g. HTTP, MSRP and XCAP). Once a user establishes a session with an application server, SBCs treat these protocols as media, (i.e. transparently), passing them directly into the core. To address this, service providers have to overlay another security layer around their application services further adding complexity and cost to their network.
- Standalone SBCs inherently only support local security policies. Because SBCs are not integrated into the softswitch at the core of the network, they can not implement security policies that reflect real-time network-wide conditions. This means for example that the network is vulnerable to distributed attacks that locally are not detectable but cause network-wide congestion.

2.2. Connectivity

To maximize the business potential of their services, carriers need to maximize the breadth of connectivity of their services. For example, a VoIP service that was limited to only those customers who were subscribers or only those with specific end devices would likely be much less successful than one that offered broad connectivity.

SBCs help service providers achieve broad connectivity by supporting and interworking between a number of variants of SIP and H.323; enabling signaling and media packets to traverse customer's and peer network NAT devices and firewalls; providing transcoding between different media codecs (e. G.711 and G.729); and detecting and interworking in-band DTMF tones, different packetization periods, and silence suppression techniques.

Current generation SBCs do not address services based on SS7/IN protocols either by being able to interpret SS7/IN messages carried in SIP-I packets or by being able to directly interwork between SS7 and SIP. This means that SBCs can, for example, mishandle media for services that either originated from or are ultimately destined for a TDM network or device, resulting in either degraded service or an ability to provide service at all.

2.3. Service Assurance

Service assurance in terms of both service quality and availability is another key requirement that service providers need to be able to provide to their customers. SBCs typically provide service assurance through a combination of call admission control and quality of service features. This combination includes the use of layer 3 (IP) and layer 5 (SIP) access control lists and mapping media flows to appropriate service levels through IP header bit marking and VLAN mapping. In addition, SBCs can also provide network overload and failure detection and attempt to re-route traffic through alternate routes.

However, SBCs do not have access to the real-time network-wide knowledge required to make optimal routing decisions to avoid congestion and far-end failures. This is because most SBCs function as Back-to-Back User Agents (B2BUAs). This means a network of SBCs inherently makes routing decisions on a

hop-by-hop basis and not globally, leading to sub-optimal routing decisions and increased call failure rates.

In addition, standalone SBCs will tend to sub-optimally use transcoders, significantly degrading voice quality. Because the local SBC can not reliably know what the ultimate destination codec will be, some SBC vendors suggest transcoding all incoming media streams to a single network-wide codec. In many cases, this deployment will result in much lower end-to-end voice quality due to repetitive and unnecessary, transcoding.

2.4. Network Cost Optimization

As service providers are faced with ever more aggressive competitors, they are under increasing pressure to lower their end-to-end service costs. To do this they need to implement a network architecture that drives end-to-end and not local cost minimization (e.g. real-time network-wide least cost routing). Service providers also need to limit the number of signaling resources required to properly route each session request and minimize the use of media intensive resources (e.g. codecs). Finally, because traffic patterns and applications are dynamic and will change over time, the ability to independently scale signaling and media resources is important.

Because SBCs are standalone devices that typically integrate both signaling and media handling in a single monolithic product, they can add significant cost and complexity, described below:

- SBCs route on a hop-by-hop basis using only local information and will therefore make sub-optimal decisions especially when network conditions are dynamic. This drives up network bandwidth and port usage.
- SBCs will typically over use media resources (e.g. codecs) especially when providing transit services between IP and TDM based networks.
- SBCs are almost always deployed as monolithic devices handling both signaling and media. This limits service provider's ability to scale media and signaling resources separately leading to inefficient use of network resources.

2.5. Regulatory Compliance

VoIP service providers are increasingly required to support a wide range of regulatory requirements (e.g. in the US CALEA, LI). In addition, they need to ensure that emergency calls (e.g. E911 or GETS calls) are always provided priority service and not blocked.

While current generation SBCs can support regulatory requirements, call tracing and monitoring is significantly more complex and expensive because they are a non-integrated overlay on top of the softswitch. Due to their B2BUA implementation, SBCs break calls up into additional, independent legs that increase the complexity of real-time call tracing and monitoring by requiring service providers to deploy expensive overlay network probes alongside each SBC.

2.6. OA&M Support

Service providers need solutions that enable them to drive down the total cost of operations and support. Therefore, limiting standalone management systems, minimizing the number of CDRs generated per session, and managing IP and TDM services in an integrated and consistent manner are all highly desirable.

Standalone SBCs tend to drive operational costs higher for a variety of reasons including:

- The management system for SBCs and that used to manage the softswitch are completely separate. This limits the ability of service providers to do full flow-through provisioning, increases training costs and increases the likelihood of operational errors.
- SBCs introduce multiple overlay B2BUAs for each call that add significant complexity to operations procedures. For example, to enable end-to-end call tracing and debugging, service providers often

deploy additional, expensive, network probes in conjunction with every SBC which adds yet another element that needs to be managed.

2.7. Summary

SBCs have played a key role in enabling carriers to directly connect their IP networks to other carriers and end users, yet they have important limitations and their future role is now being actively debated¹. Service providers are increasingly looking for a next generation security and session management solution that addresses the inherent limitations of today's SBCs including:

- No support for SS7-based services either through SIP-I or directly through SS7 to SIP or H.323 interworking
- No security for applications using web-services protocols (e.g. HTTP, DNS, XCAP, MSRP)
- Additional operational complexity and cost because they are not integrated into the core call control and management platform
- Sub-optimal security, routing, service quality and service assurance because they do not have access to network-wide real-time information
- Increased network service costs because they make sub-optimal routing decisions and use of network resources

The N-aBC has been designed to directly address these issues and provide service providers with a next generation security and session management platform that scales as their network evolves.

3. Veraz Network-adaptive Border Controller (N-aBC) Overview

The Network-adaptive Border Controller supports two distinct configurations (see Figure 2) both of which are integrated with Veraz's Multimedia Generation Network Control product: the Veraz ControlSwitch:

- The integrated N-aBC, or N-aBC INT, for compact access and peering applications in which signaling and media are managed on the same platform, and
- The distributed N-aBC, or N-aBC DST, for large scale network peering applications in which the signaling and media handling functions are distributed across separate platforms.

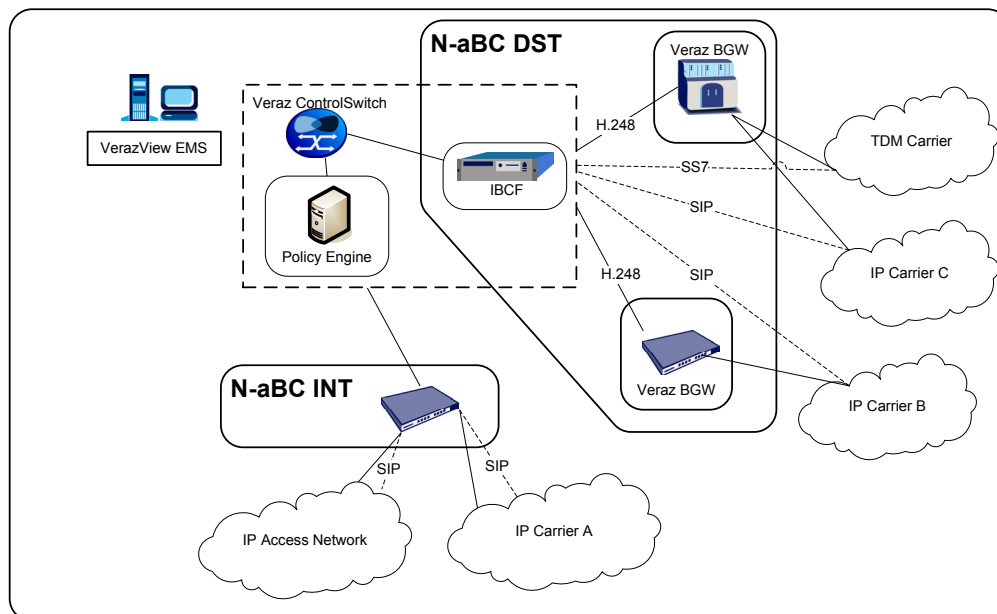


Figure 2 – Veraz's Network-adaptive Border Controller

¹ For example see: <http://www.fiercevoip.com/story/dialogic-tdm-lives-sbcs-doomed-shopping-uc-domination/2008-04-17>

3.1. Network-adaptive Border Controller Integrated (N-aBC INT)

The N-aBC INT integrates SIP signaling and IP media security and session management for access and peering network applications in a compact 1RU and fully redundant platform. The N-aBC INT includes the following functions:

- Layer 1 – 4 IP security device including firewall and NAT features
- SIP Proxy (IMS P-CSCF compliant) for session management
- Application Level Gateway for SIP, HTTP, DNS, XCAP and MSRP security
- RTP relay node to support far-end NAT traversal

Management of the N-aBC INT is integrated into the VerazView EMS platform which eliminates the need and cost of a separate security only element management system.

3.2. Network-adaptive Border Controller Distributed (N-aBC DST)

The N-aBC DST supports distributed IP network peering applications and includes two distinct components: the Veraz Border Gateway (BGW), which handles media streams, and the ControlSwitch IBCF, which handles signaling and controls the Veraz BGW via a standards compliant H.248 interface.

The Veraz BGW provides media security and management functions and is available in two versions: the 1RU I-Gate EDGE BG, and on the Veraz I-Gate 4000 PRO Media Gateway. In both cases, the Veraz BGW is controlled through a standard's compliant H.248 interface.

The ControlSwitch IBCF, a software component of the Veraz ControlSwitch, consists of two distinct software elements: the IBCF-ALG and the IBCF-BGC. The IBCF ALG supports all of the signaling security, protocol interworking and control functions while the IBCF BGC is used to control the Veraz BGW through its H.248 interface. Consistent with the distributed architecture of the Veraz ControlSwitch, the IBCF ALG and IBCF BGC could be deployed in geographically remote locations but managed as a single entity. The ControlSwitch IBCF can also be used to control 3rd party border gateways (e.g. routers) that support an H.248 interface.

Like the N-aBC INT, the N-aBC DST is managed through the VerazView EMS eliminating the need for a separate operations system.

3.3. N-aBC Key Benefits

Both the N-aBC is fundamentally different from traditional SBCs in that it is architected as Application Layer Gateway (ALGs) and not a B2BUA. This architectural choice means that the N-aBC provides all of the security capabilities of an SBC while being application independent. An SBC architected as a B2BUA provides signaling security but is not truly application independent. This lack of application independence means that the SBC's B2BUA function can interfere with the required flow of signaling messages between an end users' client and applications servers, causing the application to not work as intended. This leads to service providers testing every new application that they want to launch with their SBCs and in many cases requires an upgrade to the SBCs to support the new application. The N-aBC's ALG architecture eliminates this issue because it provides security but is transparent to the end-to-end flow of signaling messages.

The functionality and architecture of the N-aBC addresses the key shortcomings in today's SBC products and provides significant benefits to service providers including:

- **Semantic checking of signaling and application layer messages:**
Traditional SBCs only check the syntax of incoming SIP messages to evaluate whether or not they pose a threat to the core network. The N-aBC not only checks the syntax but the semantics of messages to ensure that they are properly formed and do not pose a threat. For example, when the

N-aBC receives a SIP message with a content type marked PIDF² (e.g. as part of a presence application), it will ensure that the data it contains is actually PIDF compliant XML and not syntactically correct but possible malicious XML.

- **Extensive support for SS7 applications**
Current SBCs are exclusively IP/SIP products and offer little support if any for SS7 protocols. Most service providers though have a large investment in SS7 infrastructure and the vast majority of their revenue today is generated from SS7 signaled services. In response, protocols such as SIP-I have emerged that enable service providers to interwork their SIP and SS7 networks. The N-aBC DST supports over 40 variants of SS7 for SIP-I interworking and native SS7 to SIP interworking. These capabilities are especially important in international network peering applications because of the diversity of the signaling protocols that are likely to be used.
- **Application Layer Gateway security for web-application protocols:**
Traditional SBCs provide security and session management for SIP based applications. Any other protocol is handled as a media flow and has to be processed by an application-specific device. Today, many of the applications that service providers are most interested in use protocols such as HTTP, XCAP and DNS. The N-aBC includes the capability to screen web-services protocols including (DNS, HTTP, XCAP and MSRP) in the same way it screens SIP messages to prevent attacks and block unauthorized usage.
- **Network-optimized routing and transcoding**
Traditional SBCs can only make routing, security and transcoding decisions using local information. Because of this SBCs tend to overuse transcoders, which leads to loss of voice quality, and make sub-optimal routing decisions, resulting in lower ASRs. The N-aBC is fully integrated into the Veraz ControlSwitch routing engine which means the use of codecs can be minimized and security and routing decisions for both signaling and media can be globally optimized, call-by-call, against a diverse set of parameters (e.g. least cost, highest quality, time of day, destination network). In addition to optimized routing, the ability to dynamically route media flows across multiple IP nodes enables the network to route in real-time around node failures and congestion.
- **Local and network-wide security policies:**
Traditional SBCs support security policies that are driven by local information. The N-aBC works with the ControlSwitch Policy Engine to enable the use of security policies based on network-wide, real-time data that prevent attacks that are distributed across the network.
- **10:1 VoIP bandwidth reduction without degradation in voice quality:**
Traditional SBCs support either high compression or high voice quality but not both simultaneously. The N-aBC supports Veraz's RTP Mux feature which reduces the bandwidth required to carry VoIP sessions by 90+% without sacrificing voice quality
- **Application-independent security and session management:**
Traditional SBCs are implemented as SIP B2BUAs which means they fully stop and then re-start each session request. Because of this, the SBC must be aware of how any application that a user might try to access is expected to behave to ensure proper performance. As a result, whenever a new service is launched the SBC's behavior must be checked and potentially updated.

The N-aBC is architected as a SIP ALG making it is transparent to the user's client and application except as required to ensure privacy and security. This means that as service providers develop new applications with different message flows there will never be a need to update the N-aBC to enable users to properly access and use the service.

² PIDF – Presence Information Data Format is an XML format for presenting presence information

- **Simplified OAM&P through integrated, network-wide, operations**

Current SBCs are managed through separate element management systems (EMS) and generate independent logs, CDRs and reports that need to be correlated with other information to fully debug and analyze network performance. The N-aBC eliminates the need for a separate security and session management EMS because it is managed as an integral part of the Veraz ControlSwitch through the VerazView EMS. The benefits of this include the following:

- From a single management system, operations personnel can perform network-wide end-to-end call tracing and fault management and produce and analyze network-wide reports.
- A single end-to-end CDR is produced for each call minimizing the need to correlate multiple, independent CDRs generated by standalone nodes.
- For mixed TDM and IP applications, VerazView provides a single consistent interface for managing IP and TDM trunks minimizing training costs and the chances for errors.
- Local and network-wide security policies can be managed centrally and then deployed in real time via the ControlSwitch Policy Engine across the entire network.

3.4. Veraz N-aBC Common Feature Description

The following sections describe the N-aBC features common available in both the N-aBC INT and N-aBC DST configurations.

3.4.1. Security

The N-aBC provides a full suite of security features that protects both the border and the core of the network from attacks, ensures access even during attacks for trusted users, and provides subscriber privacy and core network topology hiding. The N-aBC common security features include:

- NAT and firewall
- Protection against DoS/DDoS attacks
- Detection and rejection of mal-formed SIP signaling messages
- ALG security for HTTP, DNS, MSRP and XCAP
- Network topology hiding
- Subscriber authentication (P-CSCF for access applications)
- Support for local and, when used with the Veraz ControlSwitch Policy Engine, network-wide security policies
- Customer privacy through SIP header manipulation
- VLAN support
- Fraud detection and prevention through signaling and media flow correlation
- TLS and IPSec encryption

3.4.2. Connectivity

The N-aBC supports a variety of core features designed to maximize service connectivity including:

- Far-end firewall and NAT traversal
- DTMF interworking
- Packetization period and silence suppression interworking and QoS optimization
- T.38 fax support
- Minor signaling protocol fix-ups and repair
- ALG/proxy implementation to minimally alter user-to-user and user-to-application signaling flows
- Call-by-call transcoding to maximize voice quality
- Inter-VPN connectivity without sacrificing privacy

3.4.3. Service Assurance

The N-aBC includes a strong set of features to ensure end user quality of service including:

- L3 and L5-based call admission control through static and dynamic access control lists
- Ensured access for trusted users during attacks
- Call-by-call QoS monitoring and reporting
- ToS bit marking, VLAN mapping
- RTP Mux which by reducing the network bandwidth required to support VoIP sessions by 90%, lowers the risk of network overload and call blocking
- When used with the Veraz ControlSwitch, optimized network-wide routing that detects and routes around core and border network failures and load balances across core and border resources to avoid congestion

3.4.4. Network Cost Optimization

The N-aBC provides a number of features that enable service providers to lower the cost of delivery of VoIP and multimedia services:

- When used with the Veraz ControlSwitch, true real-time network-wide least cost routing
- ALG/proxy implementation for security which limits the number of signaling resources required to properly route and control a session request
- When used with the Veraz ControlSwitch, optimized use of media intensive resources (e.g. codecs)
- RTP Mux which by reducing the network bandwidth required to support VoIP sessions by 90%, lowers the risk of network overload and call blocking

3.4.5. Regulatory compliance

The N-aBC enables service providers to fully comply with regulatory requirements such as lawful intercept (e.g. CALEA in the US). In addition, the management of the N-aBC is fully integrated via the VerazView EMS which significantly simplifies call tracing, audit and troubleshooting activities.

3.4.6. OA&M Support

The N-aBC is managed by the VerazView EMS which provides integrated, uniform management across all of Veraz's products and, when combined with the Veraz ControlSwitch, provides a sophisticated suite of OA&M capabilities. including:

- Integrated operations support that minimizes the generation of multiple CDRs and their correlation
- Consistent and integrated management of IP and TDM trunks to reduce training costs and the potential for errors
- Full end-to-end audit trails to support network performance, fraud and attack analysis
- Elimination of the need for a standalone SBC-specific EMS system

4. Summary

Over the last few years, service providers have begun to directly interconnect their IP networks and extend IP-based services all the way to customer's premises. Session Border Controllers were originally developed to support this trend by providing a secure gateway for both signaling and media traffic between IP networks. While SBCs enabled basic IP network interconnection, they lack key features that service providers need as they continue to expand their IP services, while leveraging their investment in SS7/IN services.

The Network-adaptive Border Controller (N-aBC) is designed to address the short-comings of today's SBCs and provide a true next generation security and session management platform. The N-aBC is available in two distinct configurations: the integrated N-aBC (N-aBC INT) for compact access and peering applications and the distributed N-aBC (N-aBC DST) for large scale network peering applications. Both products are architected to be deployed in conjunction with the Veraz ControlSwitch.

Some of the key capabilities built into the N-aBC that distinguish it from traditional SBCs include:

- **Integrated support for both SIP/H.323 and SS7 services** enabling service providers to fully leverage their investment in TDM services as they migrate toward an all-IP next generation network
- **Built-in security for web-services based applications** enabling service providers to protect their call session handling infrastructure as well as their applications
- **Centralized routing and session management** providing real-time global optimization of session handling, resulting in lower network costs and higher quality services
- **Centralized local and global security and call-admission control policies** significantly simplifying the management of security policies while increasing their granularity and effectiveness
- **Industry leading VoIP compression without sacrificing voice quality** dramatically lowering network transport costs and minimizing the risks of network congestion or overloads
- **Application-independent security and session management** simplifying the development and management of new applications
- **Centralized, network-wide, operations support** lowering the cost to deploy, maintain and manage both TDM and IP services