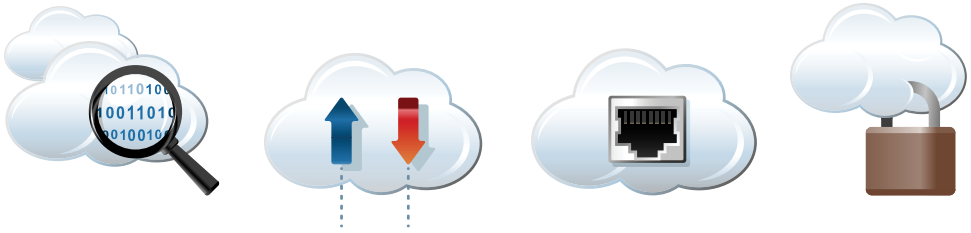
WHITE PAPER

SBC *The Critical Component*



SANGOMA

Table of Contents

Table of Diagrams

SBC – The Critical Component of your VoIP Infrastructure

Voice over internet protocol (VoIP) offers many operational cost, feature and flexibility advantages over the incumbent telephone system, and is rapidly replacing the public switched telephone network (PSTN).

As the compelling advantages of VoIP drive an increasing number of businesses and organizations to switch over to state-of-the-art telephony technology, the complexities and pitfalls of VoIP must be addressed.

Several issues arise when managing a VoIP system:

- **Security**
- **Remote worker applications**
- **Challenges of a complicated network**
- **SIP interoperability/multi-vendor/bring your own device**

The existing security features of a network can make the enabling of media and signal flow between communication endpoints technically challenging. Special measures are required to overcome the obstacles of network security features.

Corporate networks are becoming ever more complicated, due to security issues and by the variety of interoperating devices. Telecommuter applications require remote access, further complicating security issues. Meanwhile, the rise of UC (Unified Communications) means a greater variety of media, including a growing use of video and other rich communication media.

But new systems have new and sometimes unfamiliar or unknown vulnerabilities. Traditional communications via PRI lines may be limited, but they are remarkably reliable and fairly secure in most parts of the world.

When a business switches to VoIP and unified communications, a very high degree of security and reliability is expected. These systems however, are not inherently as secure as their TDM counter parts. Additional network elements are required to achieve the expected characteristics.

While it is true that networks are getting more complicated, it is also true that the equipment to manage the network is getting more sophisticated. This is good news for organizations that care about both their ability to manage the network, and the security of their data and communications systems.

ENTER THE SBC

The Session Border Controller (SBC) provides a number of services that make a VoIP/UC system more secure and better able to integrate SIP-based equipment from a variety of vendors.

Let's first look at what "session border controller" means. The session border controller manages both media and signalling streams.

Each session consists of the collection of signalling and media streams that connect one party to another. A session works in only one direction, so two sessions are required for a two-way phone conversation[1].

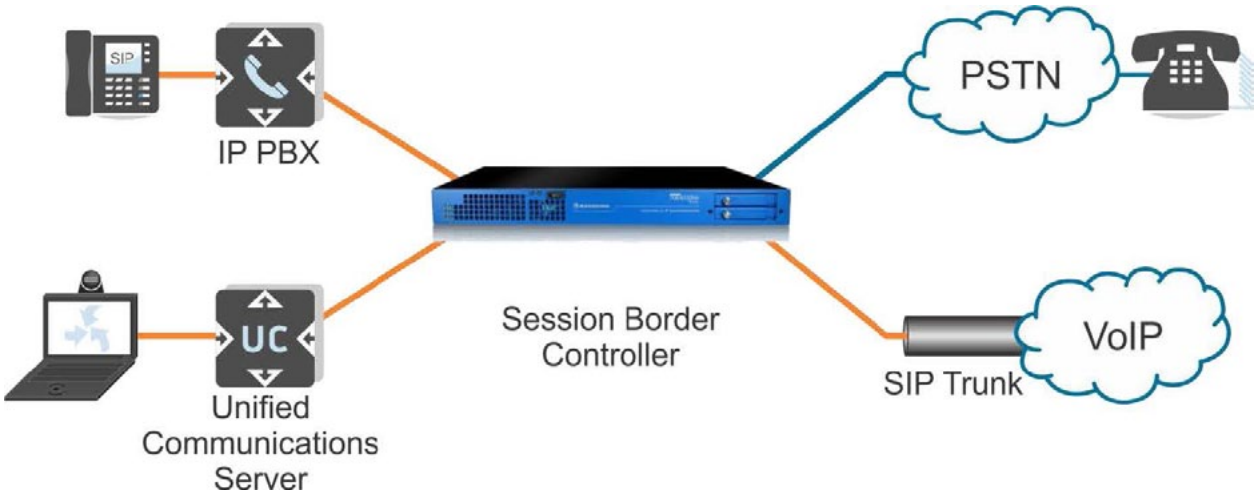


Figure 1: Typical SBC Deployment

For example, a two way telephone conversation would consist of two sessions, each containing a signaling channel and a voice channel. A video session may consist of a signalling channel, an audio channel and a video channel. The situation for conferences may be more complicated, depending on how the conference is set up. The border is the demarcation point between two networks, such as LAN and Internet, or sections of a network, such as segments in a very large and segregated corporate network.

A controller is required to manage routing, taking into account the topology of the network, traversing firewalls, and managing Quality of Service (QoS). The routing equipment controls how traffic flows through the network. If properly configured, routers will use the ToS/DSCP/DiffServ fields in the IP header to make routing decisions. It is up to the SBC to properly set these fields for each packet.

An SBC can also manage multiple SIP trunks, including load balancing, congestion avoidance and fail-over.

[1] Technically, a two-way conversation requires two sessions. However, most SBC specifications use the term session and call interchangeably.

Functions

The session border controller fills a number of important rolls in delivering VoIP services to a local network, including:

- **Security**
- **Encryption**
- **Policy**
- **Call routing**
- **SIP interoperability**
- **Media transcoding**
- **DTMF detection/generation**
- **Scalability**

Each of the above points is discussed in greater detail below.

SECURITY

One of the roles of an SBC is to provide a layer of security to prevent the VoIP system from becoming a point of entry for hackers or toll fraudsters. It must also smoothly route calls through existing security systems on the network.

The SBC terminates each call on one side of the network and re-originates the call on the other side. This approach allows the SBC to maintain complete control over every call, and to dynamically manage security. This hides network topology and presents a brick wall for would-be hackers intent on entering the network. VoIP does not present a security risk when properly managed by an SBC.

As SIP messages work their way through the network, each node adds its own ‘via’ field to every packet. Packets will probably pass through a PBX for example. By the time the SIP packet leaves the network, a series of ‘via’ fields shows the route the SIP message has taken. This reveals the structure of the network behind the firewall to the outside world. Such information can help hackers break a network.

The SBC removes all accumulated ‘via’ fields from each packet, and replaces them with a single ‘via’ field from the SBC, making outside SIP messages appear to have originated from the SBC. This hides the network structure from the outside world.

NAT transversal functions are used to navigate the NAT firewalls that protect typical corporate networks. The SBC opens a pinhole (single port) in the firewall for the duration of the call and performs port remapping to transfer signalling and media packets between the corporate network and internet.

As BYOD (Bring Your Own Device) becomes more popular, the security flaws that can come with BYOD grow. Smart phones may have apps installed which present a security threat. For example, the owner may download a game, which is really a Trojan horse designed to steal bandwidth from the network. By analysing typical traffic versus rogue VoIP traffic, the damage from such Trojans can be controlled.

- **Denial of Service**

  A denial of service (DoS) attack is a common way for hackers to attempt to disrupt service. DoS can be detected by measuring the traffic volume from each source, and blocking unusual patterns at the kernel level. This approach reduces the load on the SBC so that the network can operate normally during an attack.

Malformed packet attack (fuzzing) is an alternate form of DoS attack. The assailant attempts to bring down the service by sending malformed packets to the VoIP system in an attempt to break the SIP stack. The SBC detects malformed packets and blocks them. The IT manager can also configure the SBC to block any IP address that generates malformed packets.

The SBC can deploy other security features as well. Call access control limits the number of concurrent calls each customer can have. SIP registration security detects when too many wrong passwords are attempted within a given time. Known hacker user agents can be blocked.

- **Toll Fraud**

Toll fraud on VoIP networks is a growing problem. Toll fraud has shifted from an activity individuals undertake to make free long distance calls across the conventional phone network, to an activity carried out by more organized groups who steal minutes from unsecured corporate VoIP networks and resell them to their customers. Even the smallest PBX can be hacked and used to rack up bills of tens of thousands of dollars for unauthorized calls in a single month.

ENCRYPTION

Encrypted voice channels are required to prevent eavesdropping as voice packets travel public networks. It also serves the purpose of authenticating endpoints. The standard approach is to use Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) to protect signalling and voice channels respectively. Sangoma uses a hardware-based transcoding system to apply encryption. This frees the server to handle an increased call volume, allowing economical use of the SBC server for high call volumes while still providing voice encryption.

POLICY

Unauthorized use of the company VoIP services can be controlled by putting appropriate policies in place. These are managed by the SBC.

Only allowing calls between known SIP endpoints allows remote workers to access the VoIP system with a SIP phone, but prevents hackers from gaining access with an unregistered SIP phone or user agent.
An integrated security library looks for patterns, such as excessive long distance calls when the office is closed.

CALL ROUTING

Basic call routing directs each phone call so that it arrives at the intended endpoint.

The flexibility of an XML-based routing file and the ability to query an internal or external database adds additional flexibility and capabilities.

Routing rules are applied to each SIP message, based on variables such as time of day; any of the variables found in the SIP header, including originating number and destination number; and SS7 parameters, if encapsulated in the SIP message.

For organizations that are using multiple SIP providers, the SBC can provide least cost routing and load balancing across trunks.

The SBC can also route around network congestion by rerouting calls when the message returned by a SIP invite indicates that the message cannot be processed.

SIP INTEROPERABILITY

Although SIP is considered a standard, it is an extremely flexible protocol leading to tremendous variation. One SIP-enabled device does not necessarily interoperate correctly with another.

One of the major benefits of an SBC is that it allows different devices with varied codecs and SIP protocol flavours to interconnect. This enables multi-vendor systems to operate smoothly and leaves the door open for future equipment to work seamlessly with the current infrastructure.

SIP headers can be modified by the SBC to ensure compatibility between disparate devices. In some cases, equipment such as a phone may add certain SIP headers that other equipment, such as a softswitch, cannot recognize. The SBC can remove these headers to avoid confusing incompatible hardware. SIP header modification can also be used to add extensibility, enabling custom features such as accounting, integration with a specific PBX application, call recording and more.

MEDIA TRANSCODING

Transcoding is necessary to allow incompatible media types to cross the barrier between disparate devices, and to allow optimal use of available network bandwidth. For example, if bandwidth is not an issue and high quality is desired, G.722.1 is a good audio codec option. On the other hand, if bandwidth is constrained or expensive, G.729 is a better choice. In a conference scenario there may be a mixture of codecs, depending on endpoint equipment and individual connections. Transcoding allows a mix of codecs to work together seamlessly.

A variety of approaches are available to undertake media transcoding. Each approach has its pros and cons. The approach taken by different manufacturers varies according to their philosophy.

Transcoding can be done entirely in software. This is flexible and can reduce capital costs, but it is CPU-intensive, leading to a lower call-handling capacity on the SBC.

A hardware-based transcoding approach can be used, with the transcoding hardware installed in the server. If located in the server, the footprint is reduced, but limited space in the server may restrain the number of concurrent calls the SBC can handle.

A third approach is to use externally located transcoding hardware, situated on the network at nearby or distant locations. This is more expandable than when installed in the server cabinet, but requires a bigger footprint and additional expense for enclosures, rack space, power supplies, etc.

Sangoma is the only manufacturer to offer the choice of any of these three approaches. The most appropriate configuration can be chosen depending on specific needs, and can be changed as additional capacity is required. For example, additional transcoding hardware can be purchased and added to the network as required. No matter which approach is chosen, the solution benefits from Sangoma's long history as a transcoding hardware manufacturer.

DTMF DETECTION/GENERATION

DTMF stands for Dual Tone Multi Frequency. Each key pad button on a phone is represented by a pair of sinusoidal frequencies. This 1960's era in-band signalling system is still in wide use today, both for legacy phone handsets, and for interactive voice response (IVR) systems. The entrenchment of IVR systems insures that DTMF will remain an important part of corporate telephone systems for the indefinite future.

The challenge with DTMF signalling on a VoIP network is that some codecs do not reliably transmit DTMF tones due to the use of lossy bandwidth compression algorithms which are optimized for voice. While these compression algorithms can transmit voice that is intelligible to human ears, the audio processed by some codecs may remove some audio information so that DTMF tones cannot reliably be detected at the distant-end. In these cases, it is necessary to detect DTMF tones on the close-end gateway, convert the audio into data, and forward data packets representing the digits to the distant-end gateway. The distant-end gateway regenerates the DTMF tones for the end-point to "hear". RFC2833 tone relay is the standard method for handling this.

SCALABILITY

As the number of users and voice traffic grows, whether planned or not, the network infrastructure must grow to accommodate greater capacity. Transcoding, protocol interworking and the basics of the SBC itself must scale to manage an increased workload.

There are several approaches to this. One way might be to add additional SBCs to the network, and then load-balance amongst them. While such measures may be required in some situations, a more granular control over capacity is desirable so that issues with transcoding or interworking can be addressed separately, according to which subsystem is approaching capacity.

Sangoma systems decouple transcoding and interworking from other SBC systems. While it is possible to house these services in the same physical enclosure as the SBC, it is also possible to have external Sangoma interworking and transcoding appliances to manage scaling.

Transcoding can be handled in increments of 250 – 400 simultaneous calls with the addition of D150 units. These transcoders are simply plugged into the network via Ethernet connection, adding more simultaneous call capacity to the network.

The SBC function can be scaled by virtualizing the software. For organizations with a solid virtual server infrastructure, this approach is very appealing. Resources to a specific VM can be expanded and VoIP load increases or additional VM-based SBCs can be installed.

Virtual SBC

In the appliance version of a session border controller, customers buy a pre-packaged unit, including server, software, and hardware-assisted transcoding. Sangoma offers the NetBorder SBC, suitable for 400 to 4,000 concurrent sessions, and 75 calls per second (CPS) for the carrier version. If less volume is required, the 10 CPS enterprise version may be more cost effective.

The virtual machine (VM) version is ideal in applications where a lower call rate (calls per second) is required and the organization already has a VM infrastructure in place. In these cases, a VM installation can offer significant savings in hardware capital and operating expenses, while providing the same fail-safe operation that is built into the existing VM installation.

There is also a software version of the product, primarily intended for integration into other products on an OEM basis.

Enterprise Use Cases

SIP TRUNKING

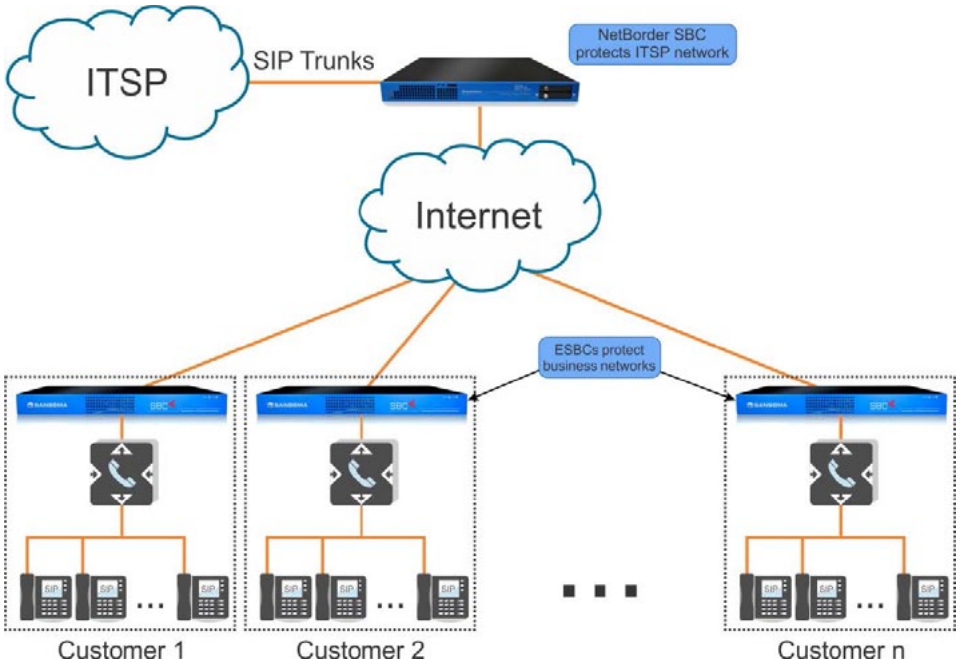


Figure 2: The ITSP and corporate networks are each protected by an SBC.

The SBC provides a defined demarcation point between the internet telephone service provider, and the corporate network. It reduces interoperating issues between the ITSP (Internet Telephone Service Provider) and their clients, saving core resources from attempting to handle interoperation. It can also handle transcoding as needed. Each business also has an SBC for security and to reduce interoperating issues within their network.

REMOTE WORKER

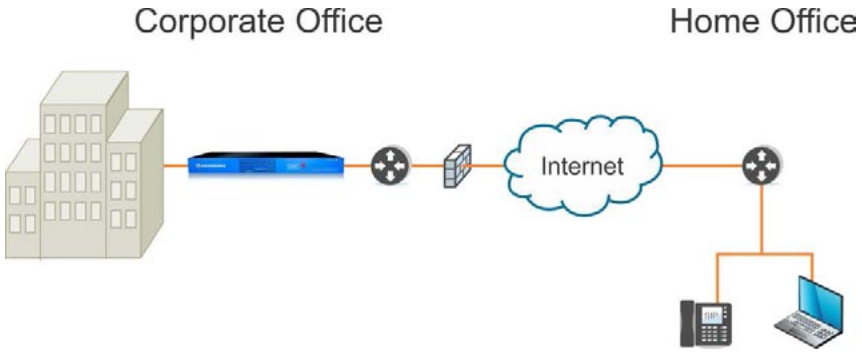


Figure 3: Remote workers with access to network, protected by SBC.

Allow access to authorized endpoints on remote worker premises. Eliminate interoperation and firewall issues on corporate and remote worker networks, maintain security.

HOSTED PBX

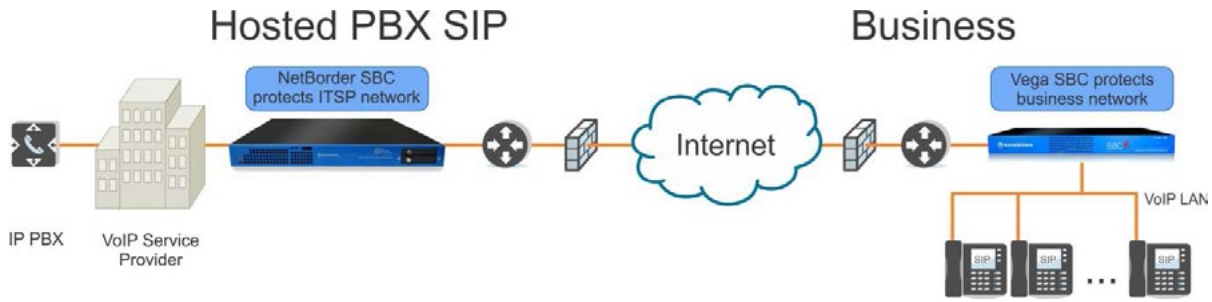


Figure 4: One SBC protects service provider, another protects the corporate customer.

The NetBorder SBC protects the internet telephone service provider's network. It provides a defined demarcation point, and reduces interoperability issues with the core. Transcoding can be provided if required. The business also has an SBC to reduce interoperability issues and enhance network security.

LYNC SBC

Deployed in existing Lync environment:

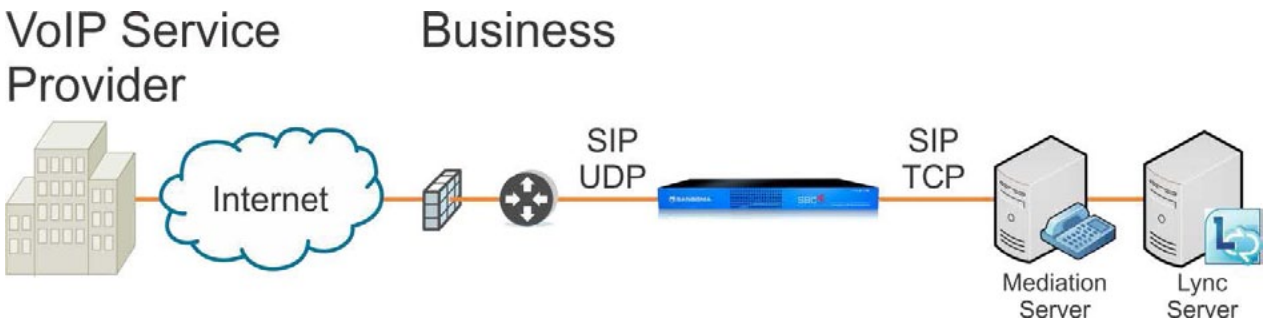


Figure 5: SBC translates MS-SIP (TCP) to standard UDP SIP.

Add SBC and Lync functions with Sangoma Lync Express:

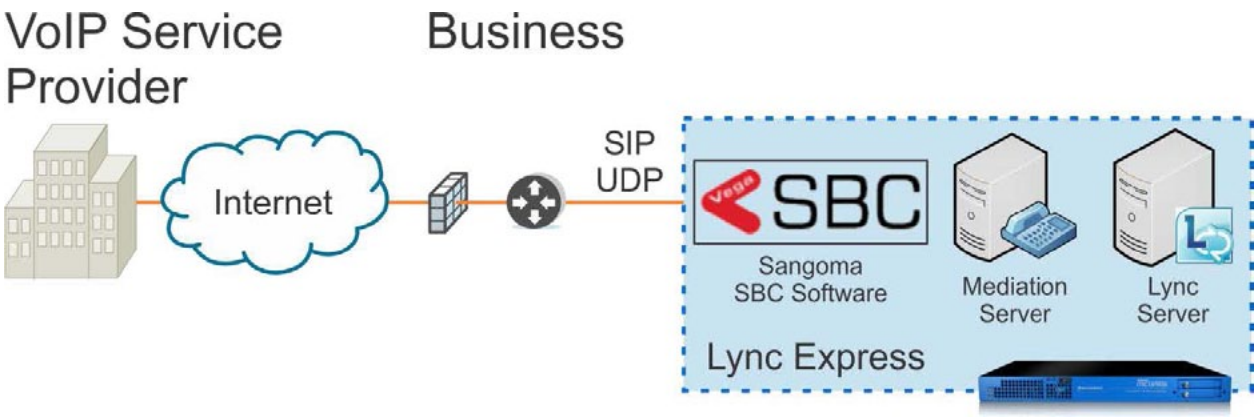


Figure 6: SBC built into Lync Express appliance.

MS SIP is not compatible with non-Microsoft devices. Microsoft Lync uses a different transport protocol (TCP instead of UDP). An SBC normalizes SIP protocol and translates transport protocol for compatibility between endpoints.

The first illustration shows how an SBC can be deployed in an existing Lync environment. The second illustration shows how a Sangoma Lync Express appliance can be used to provide SBC functionality and key Lync components.

LOAD BALANCER

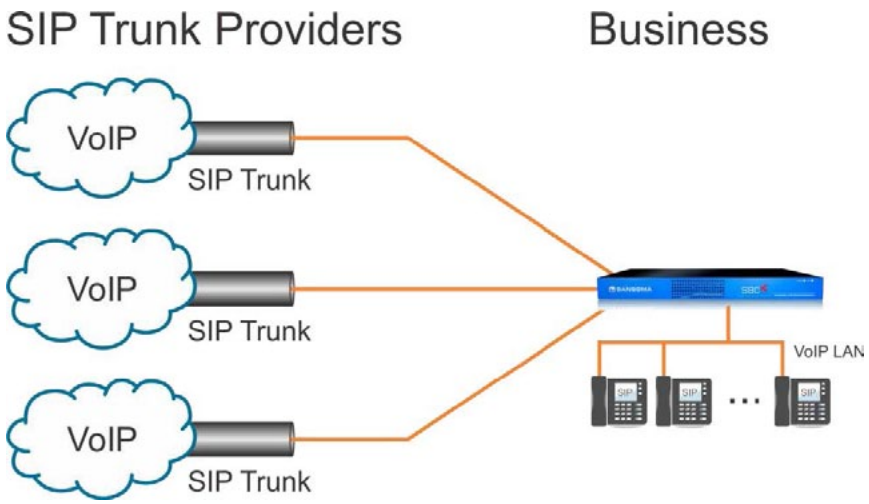


Figure 7: SBC protects VoIP network and provides load balancing across SIP trunks.

Balance call load across multiple SIP trunk providers. Reroute calls in case a trunk fails or becomes congested.

Conclusion

When an organization makes the switch from conventional phone lines to VoIP and SIP trunks, a session border controller is highly recommended to allow VoIP calls to pass through the firewall, route VoIP traffic properly across the network, and to enhance network security. The SBC ensures that VoIP does not become a security issue in the network. The SBC also protects the network from potential security threats that BYOD (bring your own device) policies could expose.

The SBC allows disparate devices to interwork seamlessly, even when those devices use different implementations of SIP.

The SBC can perform load balancing and fail over functions between SIP trunks. This allows an organization to have multiple SIP trunk suppliers and increase the reliability of their phone service.

Meanwhile, VoIP service providers require an SBC to protect their network and correct SIP headers which may not have been properly adjusted for proper routing at the client end.

The Session Border Controller is the critical component necessary to safely and effectively utilize SIP and SIP trunks.