Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Protecting IP Communications - and Your Customer's Experience

By: Bryan Davies

Digital transformation and the customer experience

The term “digital transformation” has been hot for the past few years, appearing frequently in blogs and articles, but it’s not always defined the same way. Its true meaning is making business changes to take full advantage of new technologies – the web, mobility, the cloud, and more. These technologies offer enormous opportunities to improve customer experience, business agility, and operational efficiency for most enterprises.

Notice that the customer experience tops that list. This is because a business’s ability to create meaningful differentiation from its competitors depends heavily on customers' perceptions of their interactions with the company. Consistently great customer experiences lead to business growth, a key component of business success.

The impact of digital technology

No area has been more profoundly impacted by technology advances in the past decade than communications. The tools we use to interact with each other socially have changed fundamentally, and we expect to use those same tools in our work with businesses. As a result, the technology behind voice, video and messaging strongly affects customer satisfaction. Clear, high-quality connections for communications are critically important to achieving digital transformation goals.

There are three major disruptive technology events that have had the most influence on communications.

The first of these was the emergence of the internet and the web, which allowed consumers to browse and buy nearly everything online. Voice over Internet Protocol (VoIP) also made its debut during this time, as consumers chose to start making ‘free’ phone calls over the internet. The second was the advent of smartphones and tablets, which really took off with Apple’s introduction of the iPhone in 2006. Mobility and the applications that run on smartphones quickly became a cornerstone of our daily interaction. The third disruptive event was the emergence of cloud-based services, for which communications is a natural fit.

Each of these disruptive events has something key in common: each heavily depends on delivering data over Internet Protocol (IP), which relies on ‘best effort’ packet delivery. This is a fundamental change in the way telephone voice has been transmitted for more than a hundred years.

Voice communications over IP can suffer from dropouts, stuttering and poor audio quality. Further, because of the nature of IP packet delivery, voice and video connections can be intercepted more easily and are more open to fraud and attack. For example, it is possible to launch a Session Initiation Protocol (SIP) call with low bandwidth, and then change the bandwidth mid-call to a higher, more expensive value – this is called bandwidth hijacking. Plus, a single individual can launch a Distributed Denial of Service (DDoS) attack against a company and completely disable its communications, isolating it from the rest of the world.

Despite these issues, IP-based communications provide many benefits that strongly outweigh the drawbacks. For example, it's much easier to create new converged capabilities where voice and video are embedded into an application as a native component – such as the ability to click on a button on your banking app on a tablet and have an immediate voice connection with a banker with no need to pick up a phone at all. IP communications lend themselves easily to delivery as cloud services, and they work well with unified communications approaches. Finally, IP-based communications make it easier to create new communication channels to customers that improve the customer experience – addressing the most important digital transformation goal.

In order to gain these advantages most effectively, there is a need for some software or technique to do 'housekeeping' around the IP communications interfaces. That's typically the job of a session border controller (SBC).

Enter the session border controller

Session border controllers were originally created in the early 2000s as a way of protecting the IP-to-IP interface between two communication service providers in a peering arrangement.
Today there are a large number of SBC products on the market from many vendors, for use both in communication service provider and enterprise networks.

Session border controllers provide several essential functions whenever a voice or video call carried over an IP-based protocol crosses the network boundary of an enterprise.

Security - The SBC protects the network against Denial of Services (DoS) or DDoS attacks and malicious or fraudulent access attempts. It also provides topology hiding. The SBC protects the IP interfaces for signaling and media that the communication service exposes to the public internet with an application-aware firewall.

Quality-of-Service - The SBC polices and prioritizes voice and video traffic in the network so that the underlying IP network does not become overloaded, using call admission control and rate limiting and implementing MPS overload prioritization and DSCP control.

Connectivity – The SBC provides SIP normalization so that devices from different manufacturers can coexist in the same network. It also handles interworking between IPv4 and IPv6 as well as between different VoIP and Video over IP protocols.

Media Manipulation – The SBC provides transcoding between different voice and video CODECs, encryption via TLS and IPsec, and for media with SRTP, fax interworking, and sometimes media insertion like tones and announcements.

Network Functions – The SBC provides underlying regulatory capabilities that support media recording, as well as lawful call interception. SBCs play an important role in SIP trunking and the routing of call traffic between SIP trunk endpoints.

Originally, session border controllers were implemented as a hardware appliance – much like a router or a firewall – that enterprises and service providers deployed as part of their overall IP network design. Recently, as the transition to the cloud has gained momentum across the industry, SBC vendors have launched cloud versions of their SBC product. Some of them simply pushed their SBC code into a virtual machine (VM), but other vendors have gone the full distance and virtualized their SBCs into a cloud-native format with Virtual Network Functions (VNFs) and VMs, together with support for cloud orchestration systems.

In all cases, the main purpose of the SBC is to sit at the border of an IP communication network and provide a controlled gate for voice and video media and signaling streams. It may be in place to control access from endpoint devices, such as VoLTE endpoints in a private LTE network, or to control interworking functions between network peers, such as for SIP trunking or to provide control over voice traffic to an external cloud-based service.

Typical SBC use cases

SIP trunking is one of the first applications requiring an SBC that an enterprise typically deploys. For many years, the standard interface between on-premises PBXs and IP-PBXs to the PSTN carrier was ISDN PRI, over a T1 trunk. As communications move to IP, these can be replaced with SIP trunks to the carrier at a much lower cost. In addition, SIP trunks can be defined internally to simplify the routing, reducing dropped calls and making it easier for call agents to direct customers to the right department or person. This directly impacts customer experience and how the customer perceives the business.

Another important use case is for the interconnection to cloud-based services that support voice or video. Many enterprises have an extensive set of endpoints, including soft phones for internal calling, with a premises-based call server. However, as part of their digital transformation, they may choose to move to a cloud-based communications solution. This results in a large amount of voice traffic that crosses the enterprise boundary, requiring an SBC to manage and protect that traffic. An example of this is enterprises that have premises-based Microsoft Skype for Business but are now moving to Microsoft Teams.

Unified Communications solutions also create a strong need for an SBC, especially when employees are remote and using smartphones or tablets to access the company voice network. In this case, the SBC provides the IP interface for the devices that are external to the enterprise network. Since this IP interface is directly exposed to the internet, it’s a prime target for attackers, and so a level of application-aware protection is needed.

SBCs and digital transformation

As enterprises deploy digital transformation programs, communications move to an all IP environment – whether it is voice, video or messaging. When enterprises combine this with a strategy that moves some or all of the infrastructure to the cloud (whether public, private or hybrid), it means that the sheer quantity of IP communications crossing the enterprise boundary vastly expands. This includes communication with customers – covering the full cycle of sales associates reaching out to prospective clients all the way through to the customer support call center.

The role of the session border controller is to manage and protect those IP voice and video streams, ensuring that the quality of service is maintained, calls are not dropped and customers receive the best experience possible. And that’s why the SBC is critical to the digital transformation process: it plays an important role in making sure that the primary goal – stellar customer experience – is achieved.