WAINHOUSE RESEARCH **WHITE PAPER**

Session Border Controllers and Videoconferencing

Using a Field-Proven Solution to Simplify and Improve Multi-Vendor Conferencing Environments

August 2011

Study sponsored by:

WAINHOUSE Research

acme packet

Table of Contents

List of Figures

Introduction

Both the service provider and enterprise worlds are rapidly converging onto an end-to-end IP networking strategy including data and rich media / communications traffic (voice, video, streaming, etc.).

Migrating all forms of communications onto a single network promises many advantages including the ability to integrate and unify communications and offer innovative new services that can drive business transformation. The IP network also presents several challenges to communications solutions. Fortunately, many of these challenges including security, signaling and media compatibility, as well as bandwidth management, can be addressed by a proven solution already in use by almost all service providers and many enterprises … a session border controller.

Session border controllers are network elements that are deployed at the border or interface between two IP networks, and typically within the signaling and media path between two communication devices. This strategic placement within the network enables the SBC to secure and control the signaling and media traffic.

Traditionally, SBCs have been used by service providers to enable and manage secure VoIP (voice over IP) services for residential and enterprise customers. However, these same SBCs can also be used to manage and improve video communications.

This white paper describes the benefits and advantages of using session border controllers to support the most challenging rich media application – videoconferencing – in a converged enterprise environment.

The Videoconferencing Challenge

The ability to conduct face-to-face virtual meetings without the time, expense, and stress of business travel has made videoconferencing a mission-critical application for both large and small enterprises.

Despite wave after wave of price, performance, and feature improvements in videoconferencing solutions, enterprises today still face a wide range of deployment challenges including:

Inter-Company (B2B) Communication Issues

Although an extremely important part of securing a private network, enterprise NAT routers and firewalls often wreak havoc on video communications by …

- Blocking all incoming call/session requests
- Hiding the network addresses of internal devices
- Degrading performance by inspecting each packet that traverses the firewall

There are many ways to circumvent video-related NAT / firewall (FW) issues including:

- Disable / avoid the firewall or place the video system in the network DMZ
- Forward network ports
- Deploy a video-friendly firewall or proxy
- Deploy a video bridge with dual network ports
- Deploy an H.460 or other NAT / FW traversal solution
- Leverage a B2B Video Service Provider

While certainly viable, each of the above options involves security, cost, complexity, managerial, and/or performance compromises such as the need to:

- Bypass network security by disabling the firewall, forwarding up to thousands of network ports, or via pinholing (which also involves opening ports) through the firewall.
- Assign dedicated public IP addresses to each system, which increases cost, limits scalability, and increases security risk.
- Deploy additional hardware or software to provide the enterprise dial plan.
- Deploy a video-specific, or even H.323 specific, NAT / firewall solution.
- Utilize expensive video bridge resources to circumvent the firewall.
- Utilize external services and pay the associated monthly and/or usage-based fees.

In addition, these methods resolve the NAT / FW traversal issues of only one side of the video call. If both enterprises involved in communication have not resolved their NAT / FW issues, the video call will still not connect. Furthermore, these solutions / methods tend to be video-specific, meaning that they do not resolve issues for audio (VoIP), streaming, UC, etc. As a result, enterprises must deploy similar devices for other communication systems, resulting in a series of independent communication silos.

Interoperability Issues

Despite the release of a wide range of videoconferencing standards, enterprises still face interoperability issues, including:

- Protocol Interoperability – results from the use of different communication protocols (e.g. SIP, H.323) or video / audio compression (e.g. H.264, H.263, G.722, etc.).
- Basic Connectivity – an inability to make a successful basic connection, or a loss of functionality, despite the use of the same communication and compression protocols.
- Experience Interoperability – providing a less than optimal user experience based on the devices in use and call speed.

Bandwidth Allocation Issues

Today's enterprise data networks host both non-real-time (email, web browsing, file transfers, etc.) and real-time (VoIP, IP video, video streaming, etc.) data traffic. However, these applications use different network / bandwidth management tools (if any at all). As a result, it is all but impossible for an enterprise to efficiently and effectively allocate available network resources to each application.

Additional Issues

Enterprises also face a variety of additional challenges including:

- Complexity – the need to select, install, configure, manage, and maintain infrastructure devices for each isolated communication environment (VoIP, videoconferencing, and other rich media applications) results in an expensive, overly complex environment.
- Inefficiency – the fact that each separate communication environment requires similar network elements (e.g. a gatekeeper for H.323 video, and a SIP server for VoIP) and often dedicated support resources doing similar jobs within parallel environments is inefficient and also expensive.
- Manageability – the plethora of modality-specific devices and the need to use separate management systems for each application make it difficult, time consuming, and expensive to manage the enterprise communications environment.
- Single-vendor vs. best-of-breed - To avoid interoperability issues, enterprises are often forced to deploy a single-vendor solution, even if that single-vendor solution is not best-of-breed in all areas.

Simplifying and Centralizing with SBCs

There are many reasons for enterprises to use session border controllers within their videoconferencing environment.

Simplicity and Cost Benefits

SBCs allow enterprises to simplify, centralize, and decrease the costs associated with the communications environment.

1) SBCs serve multiple purposes within an IP network by offering a wide range of functions within a single element. For example, an SBC can be used in place of a video proxy server, a NAT / firewall traversal solution, a protocol conversion / transcoding solution, a QoS monitoring / management system, and more. This not only simplifies and drives cost out of the environment by decreasing the number of separate devices that must be purchased and managed, but also eliminates the need (and complexity) for the separate devices to interface and communicate with each other.
2) Unlike protocol and application-specific devices (e.g. video gateways), SBCs are designed to handle and improve the performance of virtually any communication medium ranging from audio (VoIP) and video to instant messaging and streaming. This decreases cost and complexity by allowing an enterprise to deploy a single, centralized set of infrastructure devices to support all communication services.

Security Features

The security functions required for real-time voice and video communications are different from those required for data services. These include the following items addressed by SBCs:

1) Access Control - SBCs permit only authorized traffic (based on traffic type, originating and/or destination IP address, or other factors) to traverse the network boundaries.
2) NAT / Firewall Traversal - SBCs permit authorized traffic to securely traverse the enterprise firewall without the need for expensive, video-only NAT / firewall traversal solutions.
3) Flow-Specific Encryption – SBCs provide encryption on a per-flow basis, allowing each participant to use a different encryption protocol. Participants can even use one type of encryption for signaling, and another for media.
4) Denial of Service (DoS) Protection - there are many ways to disrupt IP-based communication services including:
    a. Malicious attacks (e.g. implantation flaw attacks, flood attacks, application-level attacks, signaling attacks, media attacks, etc.)
    b. Non-intentional issues (configuration issues, BOT searches, interoperability issues forcing frequent resend requests, protocol issues a.k.a. protocol fuzzing, etc.).

    These DoS threats are already commonplace in the VoIP world, and over time will certainly impact the video world in a similar manner. As communication proxies, SBCs buffer communication devices and networks from DoS attacks and can compensate for / correct a wide range of non-malicious issues that could impact service.

Interoperability Features

SBCs act as back-to-back user agents by making individual connections to each participating device and routing the appropriate traffic to and from each device. This allows the SBC to provide:

1) Signaling protocol conversions (e.g. between SIP and H.323)
2) Transport protocol conversions (e.g. between TCP and UDP)
3) Call signaling normalization to eliminate connectivity issues between vendors
4) Protocol mediation / methodology conversion to enable advanced features in multi-vendor environments (e.g. change "refer" to "re-invite" to enable call transfer between Avaya and Cisco systems).
5) Security interworking to enable secure communication sessions between platforms that use different forms of encryption (e.g. interworking when one side is using SRTP and other is using RTP).
6) Enterprise dial plan normalization to enable successful calling between environments using dissimilar dialing plans (e.g. a call that comes in using an E.164 address can be terminate on one side of the SBC, and then re-initiated using a URI-based dial string).

Management and Quality Assurance Features

The fact that all enterprise communication sessions flow through SBCs allows these devices to play a primary role in session management and control. Key features include:

1) Bandwidth management – unlike the protocol / application specific bandwidth management tools used by many enterprises today, SBCs are "session-stateful" and can therefore manage bandwidth independently for each communications session. This allows SBCs to provide enterprise-wide bandwidth management across all communication modalities including video, voice, streaming, etc. – on a connection by connection basis.

   Additional note – Because SBCs manage communications dialogs on a per-session basis, they can allocate bandwidth based on the user experience during each individual communication session and across all modalities. For example, if a streaming session is not providing the appropriate quality of experience, an SBC could increase the bandwidth allocated to that particular stream WITHOUT increasing the bandwidth used by other streams or applications. This level of granularity allows an enterprise to optimize the use of its bandwidth across its global environment and user base.

   SBCs also perform intelligent media management to conserve bandwidth on links where it may be preferable to do so. For users residing on the same network or behind a common firewall, for example, SBCs can "release" the media, allowing it to flow locally between users rather than forcing it upstream, through the SBC and back.

2) Call admission control – since SBCs are aware of all active communication sessions, they are able to provide enterprise-wide call admission control based on a wide array of rules including bandwidth limits, protocol in use, source / destination IP addresses, and more.

3) QoS implementation / translation – by inspecting the call signaling and packet headers, SBCs can review and manipulate the QoS markings of each communication session. This allows the SBC to add QoS as required (based on protocol used or other criteria) or adjust QoS levels as necessary (e.g. in response to packet loss or changing network conditions).

4) QoS-based controls – SBCs can monitor the state and health of the network and any individual communication session. In addition, some SBCs are able to make adjustments (e.g. re-route traffic to avoid compromised network links) to resolve quality issues.

Additional SBC Benefits and Advantages

1) Best of Breed Approach - Unlike dedicated video or VoIP solutions, SBCs tend to be vendor agnostic and have been designed to work in conjunction with other conferencing / rich media infrastructure devices (e.g. video / audio bridges, scheduling systems, etc.). This allows an organization to deploy a multi-vendor environment consisting of best of breed products and solutions without sacrificing efficiency, security, and interoperability.

2) SIP Trunking – In addition to the above, SBCs allow enterprises to replace conventional TDM PRI / BRI lines with SIP trunks that can support voice, video, and other multimedia applications. Similarly, SBCs allow organizations currently using SIP trunks for voice to use those same trunks for video. The benefits of SIP trunking include cost savings and increased reach, all without sacrificing enterprise security.

3) Protecting Internet Boundaries – Enterprises today also leverage the public Internet to integrate mobile and remote employees into the enterprise communications mainstream. The same SBC used for other purposes within the enterprise can also secure the Internet border, encrypt and decrypt communications sessions, block non-conformant or unwanted interactive communications traffic, and enable legitimate video, voice and UC sessions to securely traverse Internet firewalls.

Solution Spotlight – Acme Packet

The sponsor of this study, Acme Packet, is a leading provider of session delivery network solutions that enable trusted, first-class delivery of next-generation voice, video and unified communications services and applications across IP networks. The company's portfolio of interactive IP communications products for enterprises — SBCs, application session controllers (ASCs) and interactive session recorders (ISRs) — scales to meet the needs of the most demanding global enterprises.

Acme Packet's enterprise SBCs are enabled through the combination of its Net-Net OS operating software and a selection of hardware platforms designed to meet the needs of small to very large enterprises, contact centers and government agencies.

An example of how SBCs can simplify and consolidate enterprise communications is shown in the figures below.

Figure 1 below shows an enterprise communications architecture that routes voice, video and data traffic along three functionally separate paths, sometimes referred to as "silos." In this scenario, all traffic in and out of the network passes through the enterprise firewall en route to

its destination. This is an inefficient use of firewall resources since firewalls are not designed to control interactive communications traffic.

In this scenario:

- Videoconferencing sessions (SIP, H.323, RTP, H.239, etc.) are routed through a video-specific gateway/proxy that provides NAT/firewall traversal and connects endpoints to the MCU for multipoint conferences within the enterprise.
- VoIP sessions (SIP and RTP) are routed through an existing SBC to the IP PBX.
- Data traffic is routed through the enterprise firewall to web application servers and/or servers that deliver other business applications.

In other words, within this architecture, the web/data applications and interactive communications (videoconferencing, VoIP, etc.) are not integrated.

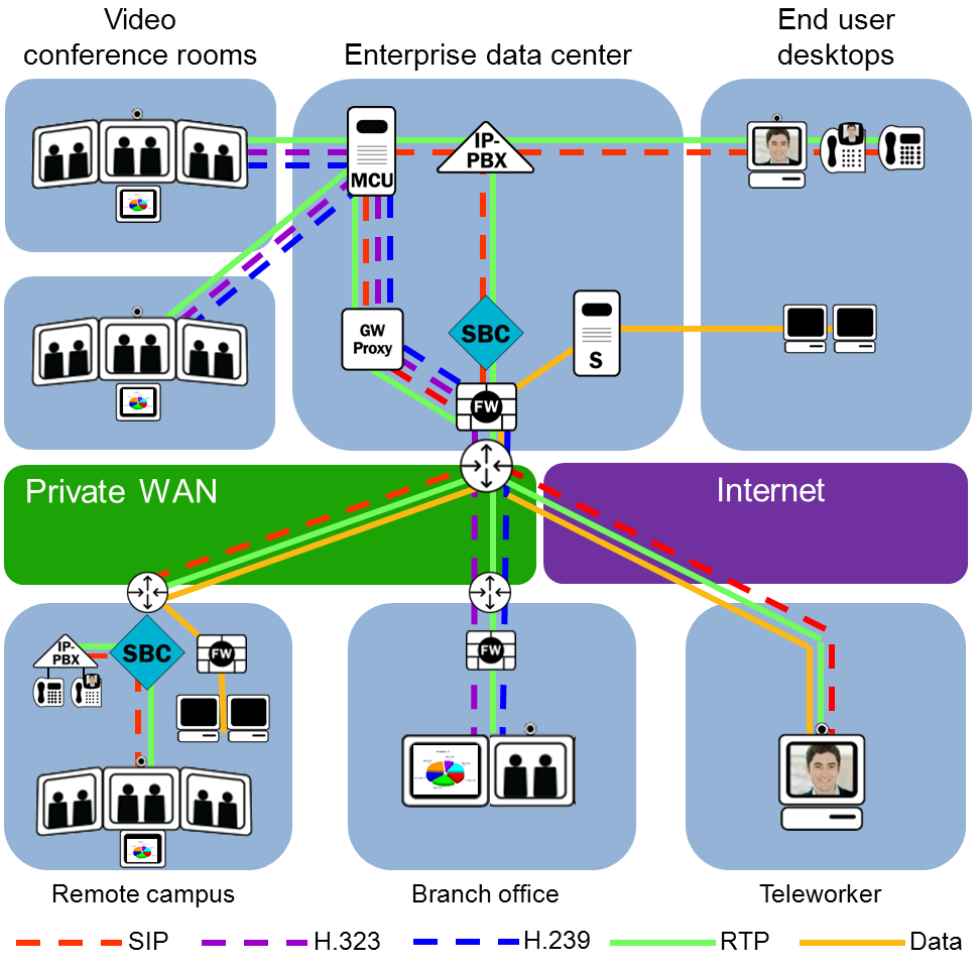

Figure 1 – A "Siloed" Communications Environment

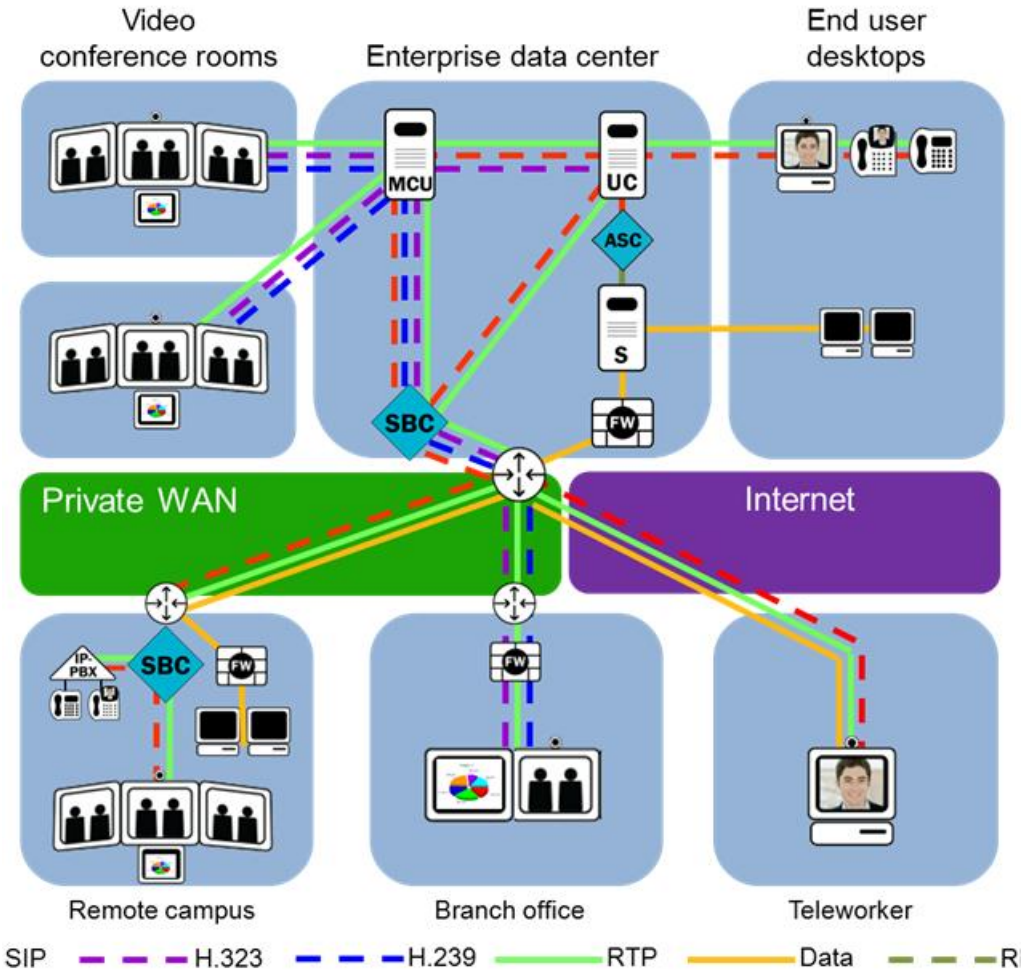

Figure 2 – A Centralized, Integrated Communications Environment

Figure 2 shows the same enterprise, this time with an architecture that reduces cost, simplifies traffic flows and integrates web/data and interactive communications applications without compromising enterprise security or application performance.

The converged architecture routes all voice, video and unified communications traffic (SIP, H.323, RTP, H.239) through an Acme Packet SBC, offloading the enterprise firewall from processing the rich media traffic. Web/data traffic is still passed securely and efficiently through the firewall, which is now deployed in parallel with the SBC. The SBC delivers the same functionality as the video gateway/proxy, making that element unnecessary.

In addition to its vendor-neutral positioning, Acme Packet's solutions address many of the issues and concerns address previously in this document including:

- Protection against malware / attacks
- Signaling header manipulation
- Advanced QoS measurement to enable intelligent session routing
- Hardware-accelerated encryption
- SBC virtualization allowing each SBC to be configured as multiple virtual SBCs
- Interworking between IPv4 and IPv6
- Efficiently integrate business processes and applications with unified communications

While every SBC offers some degree of session security and control, the advanced features described above allow enterprises to simplify their network architecture, decrease cost, increase scale, and improve overall reliability and performance.

Summary / Conclusion

Session border controllers (SBC) have been used by service providers and enterprises to enable highly reliable and secure data and voice (VoIP) communications. However, those same SBCs already purchased, installed, and in use supporting voice applications can also be used to support enterprise-wide videoconferencing and unified communications – with little or no additional cost.

The key benefits of using SBCs to manage enterprise-wide communications and collaboration include enhanced security and reliability, improved interoperability between protocols and communication systems from different vendors, and an improved user experience across all IP-based communications including VoIP, video, streaming, messaging, etc.

In general, using SBCs in lieu of application-specific network devices can cut cost, simplify the deployment and management, and enable a new generation of applications and benefits that are only possible when the communication environment operates as a single system instead of as separate silos.

Whether your organization has yet to deploy its first SBC or is already using SBCs to empower certain aspects of its global communications, the benefits associated with using SBCs to manage an enterprise's global voice, video, and UC communications are simply too compelling to be ignored.

About Wainhouse Research

Wainhouse Research, LLC (WR) provides analysis and consulting on the market trends, technologies/ products, vendors, applications, and services in the collaboration and conferencing fields. Areas of coverage include hardware, software, and services related to audio, video, and web conferencing, unified communications, and enterprise social networking. The Company publishes market intelligence reports, provides customized strategic and tactical consulting and studies, and produces industry events (conferences). Additionally, the Company operates industry-focused and end user-focused Web sites and publishes a weekly sponsored bulletin for news and analysis. For more information on Wainhouse Research, visit www.wainhouse.com.

About the Author(s)

Ira M. Weinstein is a Senior Analyst and Partner at Wainhouse Research, and a 20-year veteran of the conferencing, collaboration and audio-visual industries. Prior to joining Wainhouse Research, Ira was the VP of Marketing and Business Development at IVCi, managed a technology consulting company, and ran the global conferencing department for a Fortune 50 investment bank. Ira's current focus includes IP video conferencing, network service providers, global management systems, scheduling and automation platforms, ROI and technology justification programs, and audio-visual integration. Mr. Weinstein holds a B.S. in Engineering from Lehigh University and can be reached at iweinstein@wainhouse.com.

Andrew W. Davis is a researcher, analyst, and opinion leader in the field of collaboration and conferencing. He is a co-founder of Wainhouse Research. Prior to Wainhouse Research, he held senior marketing positions with several large and small high-technology companies. Andrew has published over 250 trade journal articles and opinion columns on multimedia communications, videoconferencing, and corporate strategies as well as numerous market research reports and is the principal editor of the conferencing industry's leading newsletter, The Wainhouse Research Bulletin. A well-known industry guest speaker, Mr. Davis holds B.S. and M.S. degrees in engineering from Cornell University and a Masters of Business Administration from Harvard University and can be reached at andrewwd@wainhouse.com.

About Acme Packet

(Copy provided by Acme Packet)

Acme Packet (NASDAQ: APKT), the leader in session delivery network solutions, enables the trusted, first-class delivery of next-generation voice, data and unified communications services and applications across IP networks. Our Net-Net product family fulfills demanding security, service assurance and regulatory requirements in service provider, enterprise and contact center networks. Based in Bedford, Massachusetts, Acme Packet designs and manufactures its products in the USA, selling them through over 140 reseller partners worldwide. More than 1,440 customers in 105 countries have deployed over 12,000 Acme Packet systems, including 90 of the top 100 service providers and 34 of the Fortune 100. For more information, visit www.acmepacket.com.