UNIFIED COMMUNICATIONS STRATEGIES

SIEMENS

Solution Review: Siemens Enterprise Communications OpenScape Session Border Controller

Russell Bennett
UC Insights
www.ucinsights.com
russell@ucinsights.com

Introduction

Those familiar with unified communications (UC) will be well aware of the value of rich, multi-modal, presence-driven collaboration tools in enhancing business productivity and speeding decision making within the enterprise. Siemens OpenScape Voice, which was launched in 2003, was the first end-to-end UC system to become available and is designed to match the pace of work and the dynamic nature of modern organizational structures. However, these organizational dynamics are not limited to single sites or single networks:

- A UC system that can only operate within the corporate network significantly limits the ROI that can be achieved with UC;
- Since UC is not ubiquitous, a UC system must provide access to the PSTN.

Nevertheless, the well understood risks of malicious attack from the public Internet make the extension of collaboration beyond the corporate firewalls a risky and difficult undertaking. For these reasons, Siemens Enterprise Communications (Siemens) has just announced the OpenScape Session Border Controller (SBC).

What is a Session Border Controller? How does it work? Why do I need one? Before addressing these questions, we will first examine the challenges and threats of wide area collaboration; and then move on to the opportunities and benefits.

Preventing Network Intrusion

Corporate networks are protected from network intrusion by 'firewalls' in a moat-like structure nicknamed the DMZ. Firewalls are designed to allow only validated traffic to traverse the DMZ, normally only email messages (SMTP) and web page requests (HTTP), both of which are easy to identify and to inspect. However, generic firewalls are wholly unsuited to managing UC data streams:

- UC systems such as OpenScape Voice use exotic real-time media types and complex signaling protocols (e.g. SIP messages) which can have other protocols and message types embedded within them;
- Real-time media (e.g. voice, video, data collaboration) occupies significant bandwidth;
- Inspecting encrypted data packets requires access to the encryption algorithms and the encryption keys;
- Determining the difference between a legitimate SIP message and, say, a virus requires a deep understanding of every potential SIP message structure.

The exponential complexity and load created by UC on firewalls means that network administrators have three choices:

1. Block UC traffic from traversing the firewall (which will be the default action with most firewalls).
2. Open firewall ports to freely allow the traversal of UC (and any other) traffic.
3. Deploy a Session Border Controller (SBC).

The first two options are intuitively bad ideas. But for the second option, if you ever took a look at a firewall log you would see that 'someone' is scanning your network ports several times a day for reasons that we can only imagine. So, for the UC-enabled enterprise, the only viable choice is option three.

Having worked through the issues that firewalls encounter in UC-enabled networks, you will be starting to get a sense for what a Session Border Controller actually is; how it works and why you need one. Since Siemens builds OpenScape Voice, they were able to design a Session Border Controller with a deep understanding of the OpenScape Voice SIP messages and media types.

In order to provide high scalability for SIP sessions (e.g. up to 2,000 voice calls with very low latency), the OpenScape SBC first ensures the validity of the SIP session by inspecting the signaling messages and validating the user credentials. Once the session has been validated, it then allows media packets associated with that session to pass through the assigned port. This is done with very low latency by inspecting the packet header to ensure that it originates from and is destined for the IP addresses of the validated end-points, as well as inspecting the packet contents for protocol compliance.

While OpenScape Voice can operate with a 3rd party session border controller, these more generic devices are expensive to purchase and deploy and typically ship as an appliance form-factor. The OpenScape Session Border Controller is a software module that is installed on the customer's preference of off-the-shelf server hardware and is priced linearly according to the number of concurrent sessions required. Furthermore, the fact that the Siemens element is designed specifically for OpenScape Voice has allowed them to increase security by reducing the 'attack surface'.

SIP Trunking

One of the features of the OpenScape Session Border Controller is the ability to connect to 'SIP Trunking'[1] services in order to gain access to the PSTN. SIP Trunking arose as a mechanism for overcoming the limitations of the existing PBX-to-Service Provider connection technology, the PRI trunk, specifically:

- The 23/30 channel limit;
- The fixed (64k) bandwidth per channel;
- Being tied into telephony toll rate plans for even inter-branch calls.

Since OpenScape Voice natively uses SIP/RTP, the use of a SIP Trunk overcomes all of these issues and can present significant cost savings over PRI Trunks. However, ambiguity within SIP standards has caused varying implementations of SIP Trunk interfaces to be offered by service providers. The OpenScape Session Border Controller can be adapted by configuration to enable connection to all of the current SIP Trunk services and has been tested against many of the major SIP service providers[2]. By mid-2012, Siemens plans to have certified against the emerging SIPconnect 1.1 standard from the SIP Forum (note that Siemens was a key contributor to this standard).

Connecting Teleworkers and Remote Networks

As described above, UC can only fulfill its true potential when collaboration can extend beyond the corporate DMZ to encompass the entire organizational structure. The OpenScape Session Border Controller can simultaneously connect the data center or corporate headquarters to telecommuters[3], roaming workers and remote branch offices (as well as SIP Trunk service providers) using authenticated and encrypted channels. The OpenScape SBC validates the user's credentials before opening a port to allow the passage of encrypted media: thus ensuring network security and business communications privacy. Since the network port is open only for the duration of an authenticated session, 'rogue packets' that may attempt to access the corporate network are easily denied access.

Reliability and Ease of Management

The OpenScape Session Border Controller provides a high degree of reliability and seamless failover to ensure that business communications can continue in various failure scenarios. It can be deployed in a redundant, geographically distributed, 'active-standby' pairing to mitigate the impact of local failures and hardware failure. Call state and other data are synchronized on the redundant nodes, enabling calls to be re-routed in real-time in the event of failure.

As with the remainder of the OpenScape suite, the OpenScape SBC is managed from the Common Management Portal (CMP) via a browser-based graphical user interface (i.e. not a command line system). The CMP provides

[1] Frost and Sullivan have forecasted that, by 2016, SIP Trunking will be a $3.9 billion market in North America, reaching 46 million workers.

[2] Including (at the time of writing) Verizon, AT&T, BT, Skype, Orange, Vodafone, Telefonica, Global Crossing, Qwest, T-Systems, and Colt.

[3] The US Bureau of Labor Statistics estimates that 12% of US full-time employees work from home at some point in their day.

the monitoring, alarm, logging, tracing, back-up and restore functions that you would expect in a system that supports mission critical business functions.

Conclusion

The Siemens Enterprise Communications OpenScape Session Border controller is an invaluable addition to the OpenScape technology suite. While the benefits of wide area network communications are compelling, with all of the well-publicized threats emanating from the Internet, enterprises are understandably fearful of exposing their corporate network to external attack. With the OpenScape SBC, enterprises can not only gain the benefits SIP Trunking, they can also provide remote access to remote workers and branch offices while maintaining network integrity. There are other session border controllers on the market that can interoperate with OpenScape Voice, but none of them can provide the degree of integration, the scalability, the manageability and the low cost of acquisition, deployment and operation that is provided by the native OpenScape option.

This paper is sponsored by Siemens Enterprise Communications.

UCStrategies
St. Helena, CA 94574
Phone: (707) 963-9966
UCStrategies.com

Siemens Enterprise Communications
1881 Campus Commons Drive
Reston, VA 20191
Phone: +1 (703) 262-2000
Toll free: +1 (800) 310-6308