

by Stratus Telecommunications, Making Convergence Simple

Security and Admission Control in the Stratus Session Border Controller



Introduction

As all the networks of the world evolve towards IP and ultimately an IMS like future, Stratus Telecommunications ENTICE session controller (E-SC) solves the critical technical issues of connectivity, admission control, security, and regulatory compliance that are common to all session controllers in a solution that's priced right, is easy to use and evolves as your network evolves.

With the ENTICE SC solution, you can peer directly with other service providers using SIP or H.323 and you can connect to the PSTN using any SIP, H.323, H.248 and SIGTRAN controlled gateways. Whether you need to access SIP based applications such as conferencing and unified messaging or whether you need to directly access external SCPs using SS7, Stratus Telecom has a solution that will work for you. The E-SC provides connectivity and interworking for the call control, transport and application layers of the network. This unparalleled connectivity paves the way for a smooth transition to IMS as the networks evolve.

Two of the most important features of a session controller are admission control and security. These will be discussed further in this paper.

Admission Control

The internet has been designed with priority-based class-of-service techniques like DiffServ and 802.1p to work well when there is plenty of bandwidth and when the only concern is managing packet priority. But no priority algorithm, can push voice and data packets beyond capacity limits without adding delay or dropping packets. Prioritization techniques don't work for congested links because they don't control demand. And once links are congested, voice quality will suffer.

If an email message arrives a few minutes late, nobody notices. If a web page loads too slow, it's of no concern. But if the propagation delay in a VoIP call grows too large or if too many packets are lost, the call can be unintelligible. Careful traffic management at bandwidth bottlenecks is essential, therefore, to the success of VoIP, video conferences, and other real-time interactive communication.

The Stratus ENTICE Session Controller (E-SC) employs session admission control to guarantee quality and service for real-time interactive communication across bottlenecks in IP access networks or when connecting any two IP networks together. By controlling the number of real-time sessions allowed through network bottlenecks and ensuring their priority, session admission control provides the tools required by service providers to guarantee both call capacity and quality end-to-end.

To ensure realtime communication works over all network topologies, the E-SC's session admission control is integrated with the layer-5 signal processing. Using this feature, the E-SC can accept or reject real-time sessions before they overload the network. The E-SC's admission control feature address the following:

- Setting policies. Resource group attributes and routing policies can be setup to limit real-time sessions in each direction and to determine the mix of real-time sessions allowed. Other policies can be used to determine such things as how emergency calls are treated.
- Controlling admission. The E-SC can accept or reject new real-time sessions based on policies and current session counts.
- Managing priorities. Real-time media packets can be explicitly marked for prioritization by IP routers and switches.
- Tracking activity. Real-time media sessions are monitored as they pass through the session controller and the number of sessions is monitored and controlled.

Security

Service providers can use the Stratus ENTICE Session Controller to only allow authorized users access to their services and protect their internal service infrastructure from denial of service attacks. This infrastructure may include other softswitches, IP PBXs, application and media servers for unified messaging, conferencing, presence and instant communications or media gateways which terminate or originate to the PSTN.

Routing information must be concealed from inquisitive customers and competitors. If for example, a provider is aggregating services, providing transit or termination services through another provider, a customer might analyze traffic data to determine the original provider and approach them directly for a better price.

The Stratus ENTICE Session controller works with the provider's signaling infrastructure to perform access control based upon layer 5 signaling messages. For authorized communications, it enables media streams into firewalled networks by opening and closing firewall pinholes. It can also hide network topology by performing network address and port translations (NAPT) on all signaling and media IP packets. These NAPT features also preserve IP addresses by enabling the use of private addresses for customer premise equipment.

To protect against infrastructure overload, call counts can be established to intelligently throttle inbound or outbound traffic. If a terminating route can only handle 50 calls before it reaches capacity, setting call count limits allows the E-SC to gracefully reject new call requests for inbound traffic or route advance for outbound traffic when activity reaches this threshold. The E-SC can also be configured to defend against DoS attacks and perform these security functions with minimal latency in order to minimize end-to-end call set-up time and media stream interference.

All businesses and many residential users use firewalls with network address translation (NAT) to protect their IP networks and computers from external attack. A firewall only allows traffic into a network if it has been requested from the inside and presents a single global IP address to the outside world for all the PCs and phones behind it. While this works fine for requests to web, email, IM and other servers, it is a huge roadblock to inbound signaling and media for voice, video or other peer-peer communications.

The E-SC supports a hosted NAT traversal feature that eliminates this roadblock without any new premise-based hardware or software and also without any firewall configuration changes, preserving existing security policies. This feature exploits periodic endpoint registrations to keep a signaling port open in the firewall for incoming signaling messages. As registrations pass through the SBC, it maps the layer 3 IP address/port on the firewall to the layer 5 user name/phone number behind the firewall. When an incoming signaling message is received, the SBC sends it to the right address and port on the firewall for the originating party. During call set-up, the ports for the bi-directional media flows are dynamically established. Since the media flows also pass through the SBC, it can identify the IP address/port on the firewall used for the outgoing media coming from a user name/phone number. It then uses that same firewall IP address/port for sending the incoming media to the correct user name/phone number behind the firewall. For additional security and control, the firewall can be configured to only allow incoming traffic from the IP address of the SBC.

Conclusion

Admission control and security are integral to the Stratus Telecom Session Controller and it in turn is an integral part of all the ENTICE solutions thereby bringing security and control to all our solutions. It can easily be integrated with other ENTICE components to cost-effectively provide high growth and highly profitable solutions like residential VoIP and hosted IP Centrex. Because the session controller is an integrated component there is no need to double pay for licensing by session and by subscriber as is common in other non-integrated solutions.

All ENTICE solutions are flexible, modular, highly customizable and programmable, enabling them to be used to build the solutions that work for our customers. Designed to help optimize and enhance our customers services, the ENTICE session controller incorporates more than 25 years of Stratus Telecom experience and makes it easy for them to turn today's interoperability headache into tomorrow's profit opportunity.