
RESONATE | APPLICATION NOTE

Traffic Scheduling and Optimized Service Level for Secure Sessions Using SSL3 Session ID-Based Scheduling

Resonate Central Dispatch Application Note



RESONATE®

At companies with high volume internet sites, system administrators have the difficult job of determining how to best accommodate and provide high quality service for both secure and non-secure connections.

Resonate's Central Dispatch™, a distributed software-based traffic management solution, can help. With its ability to load balance secure SSL 3.0 transactions across multiple servers based on session IDs, Central Dispatch provides a high level of control, resource efficiency, and optimized end-user service levels for secure sessions.

Increasing Precision of Traffic Control

Traditionally, SSL persistence has been accomplished by associating a particular client source IP address with a particular server node. All subsequent transactions originating from the same client IP address are then forwarded to the server with the initial transaction, regardless of whether they are part of the same SSL connection. With the exception of the first transaction, the load-balancing criteria used to select a server is ignored. In contrast, by using SSL 3.0 session IDs to uniquely identify individual secure sessions, Central Dispatch can intelligently forward each secure session to the most suitable server, even if sessions originate from the same IP address or multiple IP addresses. This is common with multiple users on a corporate network accessing the Internet through a proxy or multiple proxies.

Corporate sites typically have a single proxy server for all users. In this scenario, using only source IP-based scheduling, all users behind the proxy would be directed to a single content server since they would all appear to originate from the same source IP,

Efficiently Utilizing Server Resources

Intelligently distributing secure SSL 3.0 connections across all available servers makes optimal use of system resources. In environments where there are a large number of secure transactions

KEY BENEFITS OF SSL3 SESSION ID-BASED SCHEDULING

- Enables precise control of secure connections
- Efficiently utilizes server resources through intelligent traffic distribution
- Improves serviceability
- Controls site administration costs

the proxy server (Figure 1). Scheduling secure sessions with ISPs, including AOL can exhibit the same problems associated with a single proxy (multiple secure sessions associated with a single IP address), and introduce an additional problem, associating a single session with multiple proxies (and therefore multiple IP addresses). This can wreak havoc with traffic management solutions which schedule traffic based on source IP address, as a user could be scheduled to multiple content servers, breaking the persistent session.

By scheduling based on SSL3 session IDs, Central Dispatch assures the integrity of a secure persistent session, regardless of the proxy assigned to the session. Each secure session is identified as an individual session by the Central Dispatch scheduler and initially directed to the most available server, and subsequently to the same server for the duration of the persistent session.

with the same source IP address—for example, where Web proxy servers are used to provide corporate Internet access, or to forward SSL transactions from ISPs to advertised Internet

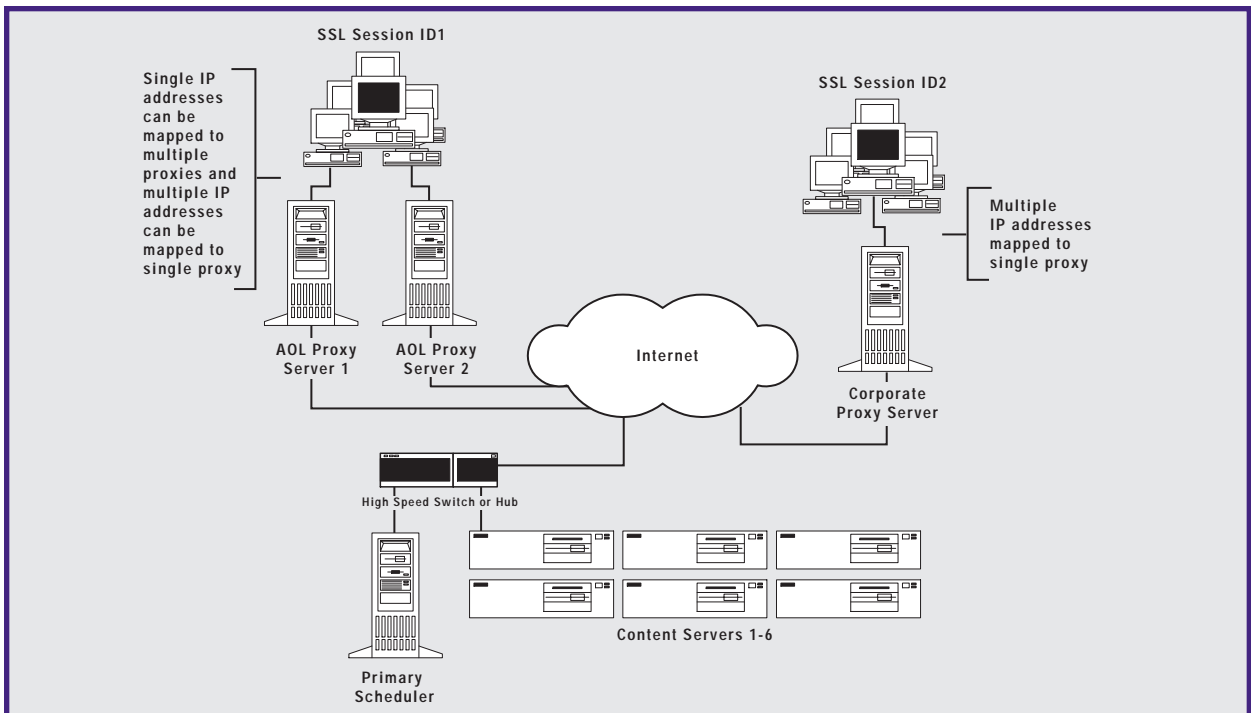


Figure 1—SSL3 Session ID-Based Scheduling for Granular Traffic Management

Commerce sites—session ID-based load balancing becomes critical. With client IP-based schemes, all users are forwarded to a small number of servers (potentially only a single server if there is one proxy server), resulting in varied traffic distribution with

some SSL-capable servers becoming overloaded, and others left idle. With session ID-based load balancing, all server resources are equivalently and effectively utilized.

Improving Serviceability

Efficiently using all SSL server resources also improves end-user response times. This is particularly applicable in high traffic sites, where client IP-based schemes result in some servers being over utilized and others under utilized. This translates into a broad range of end-user response times, with users

of heavily loaded systems experiencing slow responses. By appropriately load balancing requests across all available servers, and through Resonate's triangular data flow for direct server-to-client responses, Central Dispatch ensures that end-users receive the fastest response times possible.

Controls Costs

Central Dispatch allows system administrators to cost-effectively manage and grow their internet sites. Because session ID-based load balancing uses all available SSL servers,

regardless of where requests originate, administrators of large sites can fully utilize existing system capacity and reduce the need and expense associated with upgrades and new systems.

Considerations When Evaluating Alternative Solutions

- How are SSL 3.0 secure sessions originating from the same source IP handled? Can the sessions be forwarded to multiple SSL 3.0 capable servers (SSL 3.0 session ID-based load balancing) or will they all be forwarded to the same server (source IP scheme)?
- When the TCP connections making up a single SSL 3.0 transaction originate from multiple IP addresses, will the connections be correctly forwarded to the same server?
- What happens (with and without SSL 3.0 session ID-based load balancing) as traffic volumes increase or where proxies are used, with respect to (a) server scheduling and utilization, and (b) client response times?
- How does SSL 3.0 session ID-based load balancing effectively use system resources and minimize the potential for over or under-utilized resources?
- How does it impact system administration costs?

Conditions for Considering SSL 3.0 Session ID-Based Load Balancing

- Does the site service SSL 3.0 secure connections?
- If so, do the secure connections appear to originate from a few or multiple source IP addresses? For example, are the SSL 3.0 secure connections forwarded to the site from other partner sites? Are proxies used at the site or at the forwarding sites?
- Are there SSL 3.0 secure connections where the TCP connections making up a single SSL connection originate from multiple IP addresses?
- Are the SSL 3.0 capable servers showing fairly equivalent utilization levels, or are some more highly utilized than others? Are some even idle, while others are highly utilized?
- Do different end-users running simultaneous SSL 3.0 secure sessions experience very different response times?

SSL3 Session ID-Based Scheduling Summary

Central Dispatch's SSL3 session ID-based scheduling provides a high level of control, resource efficiency, and optimized service levels for secure sessions. Scheduling and load balancing of secure sessions based only on source IP address can be problematic when a large number of user sessions originate behind

proxies, as is common with Internet Service Providers (ISPs) and corporate sites. Central Dispatch's session ID-based approach offers the ideal solution for secure sites, scheduling traffic on a more granular level and supporting secure transactions for all users.



Resonate, Inc.

385 Moffett Park Drive, Sunnyvale, CA 94089

tel: 408.548.5500 fax: 408.548.5679

www.resonate.com