SESM Load Balancing

This chapter contains information about load balancing options for SESM deployments. It includes the following topics:

Cisco Load Balancing Solutions

The following Cisco load balancing solutions are available for use with SESM portals:

- Cisco IOS Server Load Balancer (Cisco IOS SLB)—A feature integrated into Cisco IOS software. Cisco IOS SLB performs Layer 4 load balancing.
- Cisco Content Services Switch 11000 (CSS 11000)—A switch that performs load balancing at Layers 4 through 7, including URL inspection.
- Cisco Content Switching Module (CSM)—A Cisco Catalyst 6500 line card that balances client traffic to farms of servers and other devices. CSM performs load balancing at Layers 4 through 7, including URL inspection.

Configuring SESM for Load Balancing

Subscriber Browsers

To participate in load balancing, the SESM clients (the subscriber browsers) must be directed to the IP address and port of the load balancing tool.

SSG Considerations

If the SESM solution requires SSGs, the load balancing tool must be accessible on the SSG default network.

Using the Cisco IOS Server Load Balancer with SESM Portals

This section contains important information about using the Cisco IOS SLB to load balance traffic among multiple instances of SESM portals.

Load Balancing with Stickiness versus No Stickiness

The Cisco IOS SLB stickiness feature controls whether all TCP connections from the same client session must be handled by the same server or can be load balanced among multiple servers. While a TCP connection is active, all packets from that client are sent to the same server regardless of the stickiness setting. The stickiness setting is relevant after the first TCP connection is released and the session is controlled by the web server.

- Stickiness—The load balancing tool makes all subsequent TCP connections from the same client session, received within the configured stickiness duration, to the server used for the original connection.
- No stickiness—The load balancing tool is free to distribute subsequent TCP connections among all available servers.

Caution Do not enable stickiness if your deployment uses SSGs with port-bundle host key enabled. For more information, see "Stickiness Issues with SSG Port-Bundle Host Key Feature" below.

Tip With no stickiness, we recommend configuring SESM portals with single signon enabled. Otherwise, subscribers might be required to authenticate multiple times during a session—once for each new SESM portal instance that handles requests during a subscriber session. In general, we recommend using single signon enabled in all SESM deployments. It allows subscribers to close their browsers or navigate away from the SESM portal and return later without having to reauthenticate.

Stickiness Issues with SSG Port-Bundle Host Key Feature

Stickiness in a Layer 4 load balancing tool is based on the client's IP address. When port-bundle host key is enabled, multiple subscribers have the same IP address (the SSG port-map source ip address). As a consequence, when Stickiness is enabled on the IOS-SLB, all TCP connections for all clients with the same port map IP address (using the same SSG), are directed to the same SESM server. This is not the desired effect.

Note In general, we recommend enabling the port-bundle host key on SSGs and avoiding the stickiness option in a Layer 4 load balancing tool.

No stickiness works well whether the port-bundle host key option is enabled or disabled.