While external participation is possible by controlling port access through a firewall, we highly recommend that you consider a segmented meeting access (SMA) configuration instead. SMA configurations isolate some meetings on the private corporate network while exposing others, designated as external, to the Internet. Users designate their meetings as internal or external during the scheduling process by setting the Allow External Web Participants parameter on the New Meeting scheduling page.

Note: The Segmented Meeting Access-1 Server (SMA-1S) configuration is no longer supported in Cisco Unified MeetingPlace Web Conferencing Release 6.1.

Contents

About the SMA-2S Configuration

Note: For system requirements, see the System Requirements.

In the Segmented Meeting Access-2 Servers (SMA-2S) configuration, Cisco Unified MeetingPlace Web Conferencing is deployed on two separate web servers or two separate clusters of web servers. One is on the internal network, behind the firewall; the other is on another network segment, such as a demilitarized zone (DMZ). The internal server or cluster is only accessible from behind the firewall while the external server or cluster is accessible from inside or outside the firewall.

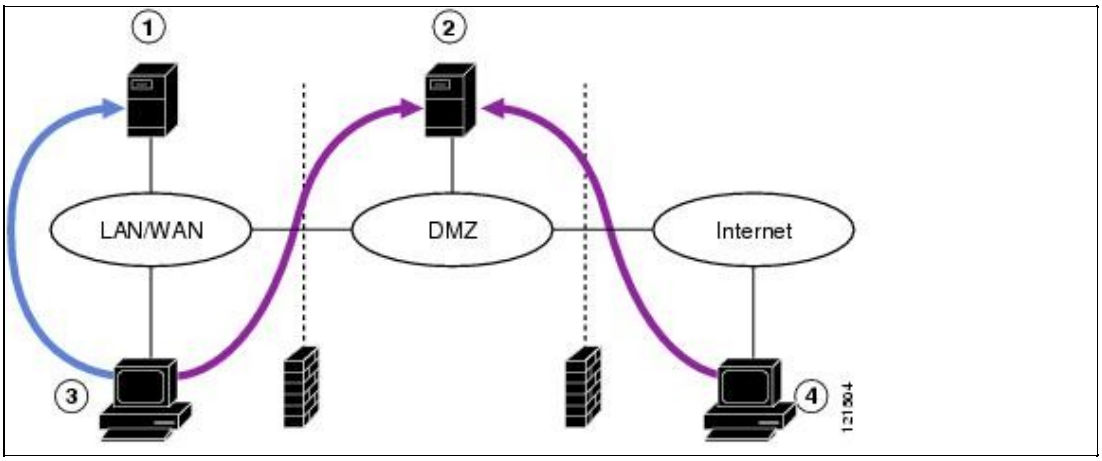
While internal users have access to the full-access Web Conferencing user interface, external users have access to an attend-only web page that only allows attendance to external meetings.

The SMA-2S configuration is the preferred and most secure deployment model if you want to provide external access to Cisco Unified MeetingPlace web conferences.

Note: We recommend that you configure external web servers to use Secure Sockets Layer (SSL). This provides optimum security and resolves proxy server issues that can prevent users from joining a web conference. For SSL configuration instructions, see the How to Configure Secure Sockets Layer.

Note: If you configure SSL on an external web server and users will access the server through a firewall, make sure that TCP port 443 is open inbound on your firewall for both of the hostnames or IP addresses on the server.

Figure: Segmented Meeting Access-2 Server Configuration



1	Internal Cisco Unified MeetingPlace web server. • This web server sits inside the private corporate network.	2	External Cisco Unified MeetingPlace web server. • This web server sits in a network segment, such as a DMZ.
3	Internal user. • Internal users enter internal meetings through the internal web server. • Internal users enter external meetings through the external web server.	4	External user. • External users can enter external meetings only. • Users enter these meetings through the external web server.

About the SMA-2S Configuration with SSL and Segmented DNS

If your Cisco Unified MeetingPlace Web Conferencing system has SSL configured on the external web server and a segmented DNS, the segmented DNS name cannot be the same as the SSL certificate name on the external or internal machine. See the following example for configuration guidelines.

Example

You have a SMA-2S configuration where SSL is required for external users, but not required for internal users who are accessing the internal or external machine.

- The segmented DNS name is *meetingplace.company.com* .
- The SSL certificate name for the external machine should follow the format *meetingplace1.company.com*.

  SSL certificates must use the fully qualified domain name (FQDN) of the server.

- The hostname for the external machine from the internal machine is *meetingplace1*.
- All URLs and click-to-attend links are in the form of http://*meetingplace.company.com*.

When users access http://*meetingplace.company.com* from the external network, the external machine will automatically redirect them to HTTPS plus whatever hostname is configured in the database-in this case, *meetingplace1*.

Note: If you force SSL on all users, both internal and external users will be required to use SSL when they access the external web server.

About the SMA-2S Configuration and Video-Enabled Systems

In a Segmented Meeting Access-2 Server (SMA-2S) deployment, note the following considerations:

- If the Video Integration is deployed on the internal web server, users can schedule internal video-enabled meetings from the web. Requests to schedule external video meetings are denied. (In this case, users must make sure the Allow External Web Participants parameter on the New Meeting scheduling page is set to No.)
- If the Video Integration is deployed on the external web server, users can schedule external video meetings from the web. Requests to schedule internal video meetings are denied. (In this case, users must make sure the Allow External Web Participants parameter on the New Meeting scheduling page is set to Yes.)

Cisco Unified MeetingPlace Release 6.1 > Web Conferencing > Installing and Upgrading > Installing Web Conferencing for a Segmented Meeting Access Configuration