# Cisco Application Networking for Microsoft Office Communications Server 2007 Deployment Guide

Cisco Validated Design

February 18, 2009

## Integrating Microsoft Office Communications Server 2007 into the Cisco Data Center

This document provides design and configuration guidance for Cisco advanced network services, including Cisco network-based server load balancing and firewall deployed with Microsoft Office Communications Server 2007 Enterprise Edition in a data center. Specifically, the Cisco Application Control Engine (ACE) and Firewall Services Module (FWSM) are highlighted in this document.

An overview of Microsoft Office Communications Server 2007 Enterprise Edition deployment models is given to provide the reader with some context as to how the application environment is impacted by the Cisco advanced network services. The contents of this document were developed through a joint project with Cisco and Microsoft, including collaboration on lab setup, testing definition, and solution documentation.

## Audience

This document is intended for network engineers and architects who must understand both the basics of a Microsoft Office Communications Server 2007 environment and the design and configuration options when introducing Cisco advanced network services.

**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Objectives

The objective of this document is to provide customers with guidance on how to leverage Cisco advanced network services to support a Microsoft Office Communications Server 2007 environment to achieve the following goals.

- Shorten Microsoft Office Communications Server Enterprise Edition 2007 deployments by providing step-by-step instructions on configuring Cisco solutions.
- Identify high availability and security benefits of specific Cisco and Microsoft Office Communications Server 2007 deployment options.
- Demonstrate scalability and availability characteristics of a consolidated deployment of Microsoft Office Communications Server 2007 in a Cisco data center environment.

The document is not meant to introduce the reader to basic Cisco data center design configurations, nor is it meant to be a resource to learn the details of Microsoft Office Communications Server 2007. The reader must be familiar with basic Cisco data center concepts and products as well as the basics of Microsoft Office Communications Server 2007 components, roles, and deployment scenarios as documented by Microsoft Corporation. The prerequisite knowledge can be acquired through documents and training opportunities available from both Cisco and Microsoft.

A few recommended resources that readers would find useful in these areas include:

- Cisco data center solutions:

  http://www.cisco.com/go/dc

- Cisco Validated Designs (CVD):

  http://www.cisco.com/go/cvd

- Microsoft Office Communications Server 2007 product pages:

  http://office.microsoft.com/en-us/communicationsserver/default.aspx?ofcresset=1

# Summary

Solution validation testing with Microsoft Office Communications Server 2007 and Cisco ACE and FWSM products yielded interesting insights about the details of Microsoft Office Communications Server 2007 operation and how Cisco ACE and FWSM can be configured to support Microsoft Office Communications Server 2007 Enterprise Edition in both consolidated and expanded mode deployments.

The Cisco ACE configuration required to support Office Communications Server 2007 is not complicated and can be easily deployed.

- Layer 3 Virtual IP (VIP) can be used to simplify load balancing configuration. Office Communications Server 2007 uses many different protocols to support various features of the product. The hardware load balancer configuration can be simplified by configuring the virtual IP address on the load balancer to listen on all IP ports and utilize Access Control Lists (ACLs) to restrict traffic to the VIP.
- The ACE Source Network Access Translation (SNAT) feature for server-initiated connections can be used to simplify Microsoft Office Communications Server 2007 deployments and traffic analysis. For simplicity, Microsoft recommends using source NAT for all pool traffic; however, further Cisco and Microsoft testing found it is only necessary to use source NAT for server-initiated traffic destined for VIP, thus saving resources. Cisco ACE supports this type of SNAT, which dramatically decreases the size of the NAT translation table and preserves source IP addresses of external client connections, which can be useful in troubleshooting and log file analysis.

Functional and performance testing with Cisco ACE in a Microsoft Office Communications Server 2007 consolidated deployment provides application availability and scalability:

- 22,000 concurrent IM users can be supported by two dual-core Xeon-based servers with 2 GB RAM.
- Tests running a mix of instant messaging and conferencing traffic generate up to 45 Mbps of traffic.
- High availability failover scenarios have minimal impact on application operation to end users.

# Application Architecture

Microsoft Office Communications Server 2007 provides the following unified communications functions:

- Presence information (user availability detection)
- Instant messaging (IM)
- Voice over IP (VoIP) telephony
- Web and A/V conferencing

Office Communications Server 2007 is available in two versions, Standard Edition and Enterprise Edition. The primary difference between these two versions is whether the deployment model is single server versus multi-server. Standard Edition combines all functions, including the SQL server, onto the same server platform, whereas Enterprise edition is intended to be deployed on multiple servers, providing scalability for enterprise deployments.

Office Communications Server 2007 Enterprise Edition can be deployed in two different topologies, consolidated and expanded, to support scaling user populations. Microsoft recommends the use of a hardware load balancer for Enterprise Edition deployments to distribute user traffic to the front end servers of a pool. Software load balancing products such as NLB are not recommended for use with Office Communications Server 2007.

Client access to Office Communication Server 2007 is provided via either Microsoft Office Communicator 2007 and Live Meeting Client desktop software.

## Server Components

Office Communications Server 2007 is a distributed server environment. Independent software modules work in conjunction to provide the features of Office Communications Server 2007. The principal function of the front end server is to provide the following services to end users and control the application environment.

- Registration and presence
- Instant messaging
- Telephony
- Web conferencing
- Audio/video conferencing
- Health monitoring and conference set up

These services are supported via the following software modules:

- Instant Messaging—The Instant Messaging Media Conferencing Unit (IM MCU) is responsible for user registration into Office Communications Server 2007, instant messaging traffic, and presence state for users.

- Telephony Conferencing Server—Known as the ACP Media Conferencing Unit (MCU), it is responsible for facilitating conference calls between end users.
- Web Components Server—This is an Internet Information Server (IIS) service. The Web Components Server enables organizers to upload presentations and other data for use in a Web conference. Participants download this content via the Web Components Server. This IIS service also performs distribution expansion for Office Communicator clients and distributes address book files to clients.

**Note** The Web Components server resides on the front end servers or can be installed on a dedicated pool of servers front ended by an ACE load balancer for scalability.

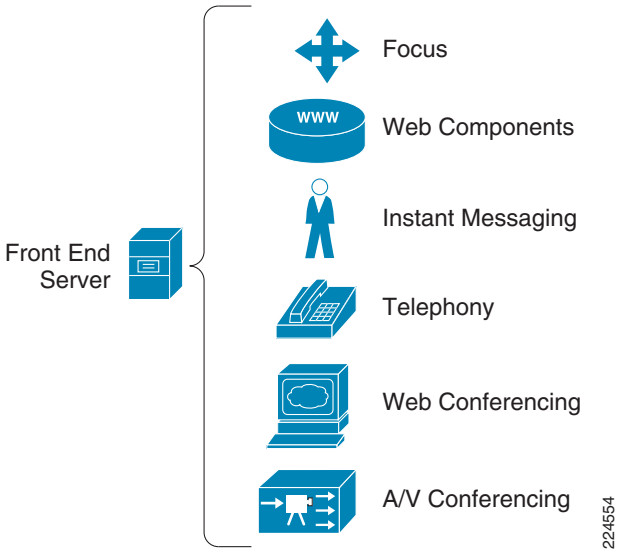
- Web Conferencing Server—The Web Conferencing Server (MCU) enables on-premise conferencing. Web Conference users require the Microsoft Office Live Meeting 2007 client. Additionally, Web Conferences can be scheduled using the Audio/Visual Conferencing Server (see below).
- Audio/Visual Conferencing Server—The A/V Conferencing Server (MCU) enables users to share audio and video streams during multipoint Web Conferences.

**Note** The Web and A/V Conferencing servers can either reside on the front end servers or be installed on separate, dedicated servers or pool of servers. These two pools are load balanced by the Focus element of Office Communications Server 2007, not by the ACE module.

- Focus—This service is responsible for conference setup and signaling for the duration of the conference.

Figure 1 depicts these modules installed on a front end server.

***Figure 1 Office Communications Server 2007 Front End Server Components***

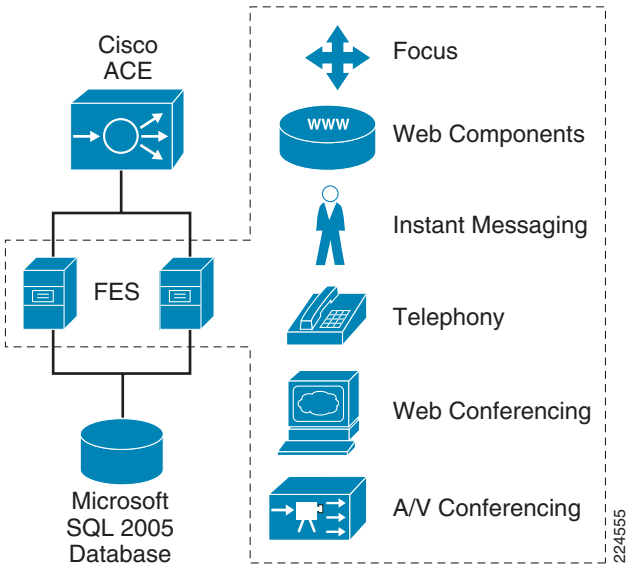


# Consolidated Deployment Option

Office Communications Server 2007 consolidated mode deployments typically consists of an enterprise pool where all server components are co-located on the pool's front end servers. All front end servers in the enterprise pool are configured identically. The back end server running a SQL database resides on a separate dedicated physical server. The consolidated configuration provides scalability and high availability and t is easy to plan, deploy, and manage.

- Requires two or more front end servers deployed behind a hardware load balancer.
- Each of the Office Communications Server 2007 components are installed onto each server in the pool.
- A dedicated SQL server is required to support the pool.
- All servers in the enterprise pool must be deployed on the same subnet.

***Figure 2 Consolidated Deployment Option***

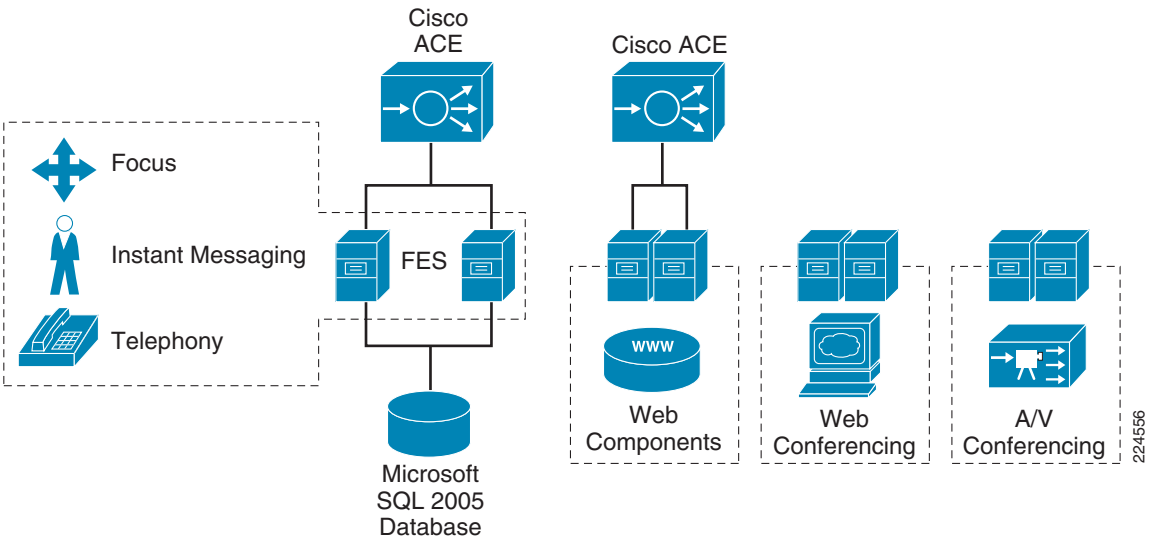



# Expanded Deployment Option

This option offers maximum scalability, capacity, performance, and availability for large organizations. Expanded configuration enables organizations to scale up audio/video or Web conferencing requirements independently from other Enterprise Edition server components:

- Separate servers dedicated for each of the following server roles: font end, IIS Web components, Web and A/V conferencing
- Hardware load balancer required for front end servers and Web Components Servers

*Figure 3 Expanded Deployment Option*




As Figure 3 shows, the IM Conferencing Server and Telephony Conferencing Server are co-located on the front end server, while the Web Conferencing Server, A/V conferencing Server, and IIS are installed on separate, dedicated computers.

**Note** Front end servers are connected to one hardware load balancer and the servers running IIS (Web Components Servers) are connected to a separate hardware load balancer. No load balancer is required by the Web Conferencing or A/V Conferencing servers. Traffic distribution to these servers is handled by the Focus server component residing on the front end servers.

# Network Traffic Flow in Office Communications Server 2007 Consolidated Mode

Figure 4 illustrates the various network protocols and communication flows used to support Office Communications Server 2007 consolidated deployment application traffic. Understanding the network flow of servers of an enterprise pool in consolidated mode is important to configure your Cisco ACE hardware load balancer and Firewall Services Module for the enterprise pool. The primary protocol used for instant messaging and application control is Session Initiation Protocol (SIP) implemented over Transport Layer Security (TLS) or SSLv3. SIP over TLS standard port definition is TCP 5061, but Office Communications Server 2007 also uses other TCP ports for SIP/TLS communication to support other conferencing functions.

The Cisco ACE hardware load balancer primarily serves to distribute client SIP requests across all of the front end servers. Cisco ACE hardware load balancer also serves to source NAT the network connections from the IM, Telephony, Web, and Audio/Video Conferencing Servers (referred to as MCUs) to the Focus element and MCU Factory residing on the front end servers. Since all of these server components reside on the same front end servers, the load balanced network connections need to appear as if originating from a different server on a different subnet. Source NAT provides the ability to translate the source IP address of the originating servers to one that is owned by the ACE hardware load balancer which supports the server to server network connections between different Office Communications Server 2007 components residing on the same physical servers.

*Figure 4 Microsoft Office Communications Server 2007 Consolidated Deployment Traffic Flow*

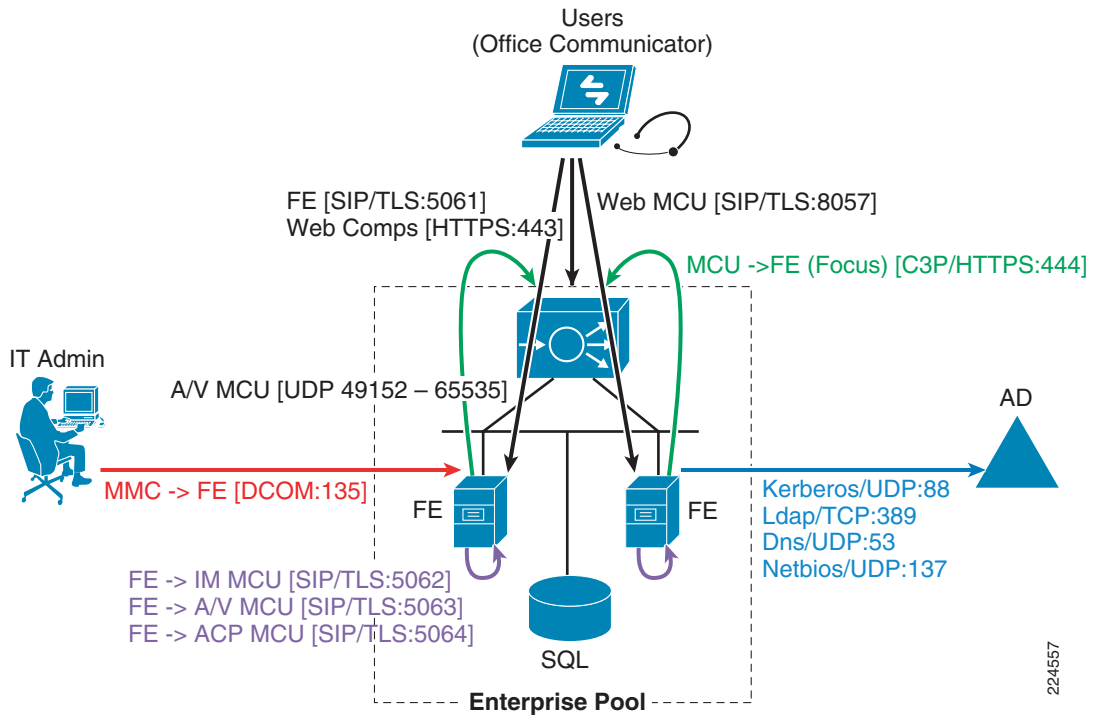



*Table 1 Inbound Traffic*

| Port Required | Source | Destination | Description |
|---|---|---|---|
| TCP 5061 | Client PC | VIP for pool | Client instant messaging traffic encrypted via SIP/TLS |
| TCP 444[1] | FES real IP | VIP for pool | Conference MCUs to Focus and MCU Factory to track health and schedule meetings |
| TCP 443 | Client PC | VIP for pool | Web Components Server traffic (HTTPS) to download content for meetings |
| TCP 8057 | Client PC | FES real IP | Web Conferencing MCU traffic (SIP/TLS) for meetings |
| UDP 135 | Admin PC | FES real IP | DCOM traffic for Office Communications Server 2007 Admin tool |
| UDP 49152 – 65535 | Client PC | FES real IP | A/V Conferencing traffic |

1. TCP 444 traffic is classified as inbound traffic, however you will not see it ingress on the outside interface of the ACE module. Due to the ACE bridged mode deployment, the VIP and server IP addresses are all in the same local subnet and traffic stays within the ACE module.

*Table 2 Outbound Traffic*

| Port Required | Source | Destination | Description |
|---|---|---|---|
| UDP 88 | FES real IP | Active Directory | Kerberos |
| TCP 389 | FES real IP | Active Directory | LDAP |

*Table 2 Outbound Traffic*

| Port Required | Source | Destination | Description |
|---|---|---|---|
| UDP 53 | FES real IP | Active Directory | DNS |
| UDP 137 | FES real IP | Active Directory | NetBIOS |

# Network Traffic Flow in Office Communications Server 2007 Expanded Mode

Office Communications Server 2007 expanded deployment option introduces a number of new flows since dedicated servers have been established for the different server roles. Ii is important to note that the load balancing function for Web and A/V conferencing when using multiple servers is handled by the Focus element residing on the front end servers. Therefore, a hardware load balancer is not required for the Web and A/V Conferencing servers in an enterprise pool.

As with the consolidated deployment, the primary protocol used for instant messaging and application control is SIP implemented over Transport Layer Security (TLS) or SSLv3.

*Figure 5 Expanded Deployment Traffic Flow*

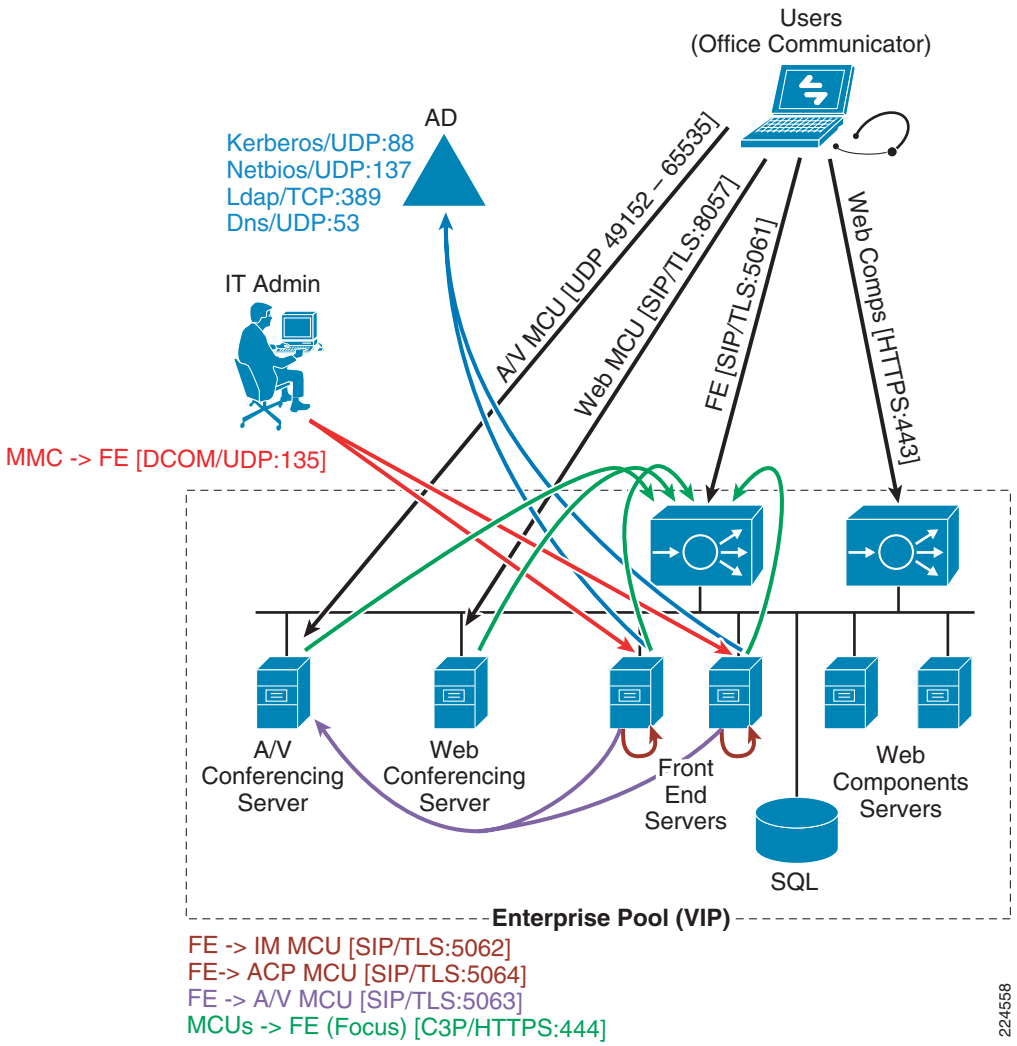



*Table 3 Inbound Traffic*

| Port Required | Source | Destination | Description |
|---|---|---|---|
| TCP 5061 | Client PC | VIP for pool | Client instant messaging traffic encrypted via SIP/TLS |
| TCP 444[1] | FES real IP | VIP for pool | Conference MCUs to Focus and MCU Factory to track health and schedule meetings |
| TCP 443 | Client PC | VIP for pool | Web Components Server traffic (HTTPS) to download content for meetings |
| TCP 8057 | Client PC | Web Conferencing server | Web Conferencing MCU traffic (SIP/TLS) for meetings |
| UDP 135 | Admin PC | FES real IP | DCOM traffic for Office Communications Server 2007 Admin tool |
| UDP 49152 – 65535 | Client PC | A/V Conferencing | A/V Conferencing traffic |

1. TCP 444 traffic is classified as inbound traffic, however you will not see it ingress on the outside interface of the ACE module. Due to the ACE bridged mode deployment, the VIP and server IP addresses are all in the same local subnet and traffic stays within the ACE module.

*Table 4 Outbound Traffic*

| Port Required | Source | Destination | Description |
|---|---|---|---|
| UDP 88 | FES real IP | Active Directory | Kerberos |
| TCP 389 | FES real IP | Active Directory | LDAP |
| UDP 53 | FES real IP | Active Directory | DNS |
| UDP 137 | FES real IP | Active Directory | NetBIOS |

# Load Balancing Requirements

The following requirements for load balancing are referenced from the Office Communications Server 2007 Enterprise Edition Deployment Guide and Enterprise Edition Planning Guide.

Microsoft states that in order to achieve maximum performance, scalability, and resiliency for an Office Communications Server 2007 deployment, it should be installed in the enterprise expanded mode using a hardware load balancer. Cisco and Microsoft have worked closely together to validate that the Cisco ACE hardware load balancer works optimally with Office Communications Server 2007.

Cisco ACE supports all of the requirements (listed below) of a hardware load balancer and can load balance Microsoft Office Communications Server 2007 Enterprise (either expanded or consolidated configuration) in a bridged, routed, or one-armed topology.

The Microsoft TechNet article “Office Communications Server 2007 Planning Guide” states the following requirements for a hardware load-balancer.

- A static IP address for servers within a pool—This means the (real) servers within a pool (server farm) should have a unique, predictable, static IP address; i.e., a hard-coded IP address and not one dynamically allocated through DHCP. This is required since the load balancer addresses the individual servers using the Layer 3 IP address.
- The load balancer is not required to decrypt TLS (Transport Layer Security) or parse SIP messages—The Microsoft model utilizes HTTPS and Transport Layer Security (TLS) encrypted traffic between the client and the server. This means the load balancer is only required to perform Layer 3 or Layer 4 (i.e., based upon VIP/port) load balancing of traffic. Microsoft states that an alternate approach is to allow the load balancer to terminate the HTTPS traffic, which provides performance, administrative, management, and potentially cost benefits. This is supported on the ACE module, but is not covered in this guide.
- A VIP address is required for servers within a pool—A virtual address (VIP) is configured on the load balancer and this should forward traffic to a pool (server farm) of real servers.
- Using a load balancer in SNAT or DNAT mode—The Microsoft Office Communications Server 2007 Enterprise Edition Deployment Guide uses the terms SNAT and DNAT to describe the mode of operation of the hardware load balancer. DNAT means the load balancer is only required to translate the destination IP Address of the incoming IP packet from the VIP address to the real server IP address (the source IP is maintained). SNAT means the load balancer is required to perform both Destination Network Address Translation as well as Source Network Address Translation (i.e., changes the source IP address from that of the client to an address “owned” by the load-balancer).

- Allows multiple ports to be opened on a single VIP—The load balancer should be able to accept traffic to a VIP address on multiple destination ports. The Cisco ACE can do this either as single virtual server listening on all ports (Layer 3 VIP) or as a single VIP listening on multiple ports (Layer 4 VIP).
- Provides TCP-level affinity stickiness (server affinity)—The load balancer must ensure that when a single client initiated multiple sessions to a load balanced server, all of those sessions must be load balanced to the same physical server. This is termed stickiness (Microsoft uses the term "affinity"). The Cisco ACE is able to provide stickiness/affinity based upon source IP address, HTTP cookies, SSL session ID (ACE 2.x software required), as well as other methods, such as fields in the HTTP header.
  - Source IP address based stickiness is the simplest to configure, however is not suitable in environments when clients are behind a pool of proxy servers that translate their source IP address. This is often encountered when applications are facing the Internet and users are accessing via mega-proxy services, such as AOL.
  - HTTP cookies and headers can only be used when the load-balancer is able to see the HTTP headers; i.e., it requires the ACE to terminate the HTTPS/TLS connection.
  - SSL session ID based stickiness is supported with ACE 2.x versions of software, however they may be issues when the SSL session ID changes mid session.

**Note** Since Office Communications Server 2007 Enterprise Edition is intended for Intranet deployments, source IP based sticky is sufficient for most deployments.

- Each front end server must be routable within the internal network—It must be possible to connect to a specific server using its real IP address for management and conferencing traffic.
- The load balancer must have a configurable TCP timeout—Due to the nature of CS 2007 traffic, it is likely that user sessions are idle for some time. In order to prevent the load balancer from incorrectly thinking that these sessions are inactive and closing them, it should be possible to set the inactivity timer to 15-30 minuets. By default the ACE TCP idle timer is set to one hour, however this is configurable to between 0 to 4294967294 seconds.
- TCP resets must be enabled for idle timeouts and disabled for down servers—This is the default behavior of the ACE. The ACE sends a TCP reset to both the client and the backend server when the TCP idle timer has expired; however, servers that are "down," either by management or keep-alive failure, do not have their sessions reset.
- FES must be able to communicate with each other without an intervening NAT device—The servers can either be all placed in the same VLAN/subnet or on different VLANs/subnets as long as there is no intermediate device that performs network address translation.
- FES real IP address must be directly manageable—Each front end server must be reachable from the outside of the ACE module for administration of the Office Communications Server 2007 environment. If an access list is used to protect servers, it must allow UDP port 135 for Microsoft Management Console access to servers.
- Load balancer must support the least connections-based load balancing algorithm—The ACE supports this load balancing algorithm. Least connections tends to provide a more even spread of traffic across servers in a server farm (pool), since it directs new clients to servers with the least number of connections. Algorithms such as round-robin, on the other hand, can result in a less effective distribution of the load due to such things as long- or short-lived connections.

- Load balancer must support enabling/disabling servers in a pool without affecting live traffic—This is referred to as graceful server shut down and is supported on the ACE by lowering server weight to zero, which stops any new connections from being sent to that server. Then after the TCP idle timeout, the server can be taken out of rotation from the pool.
- Load balancer should be able to monitor real server availability—This is termed either server “probes' or “keepalives” and is supported by the ACE.

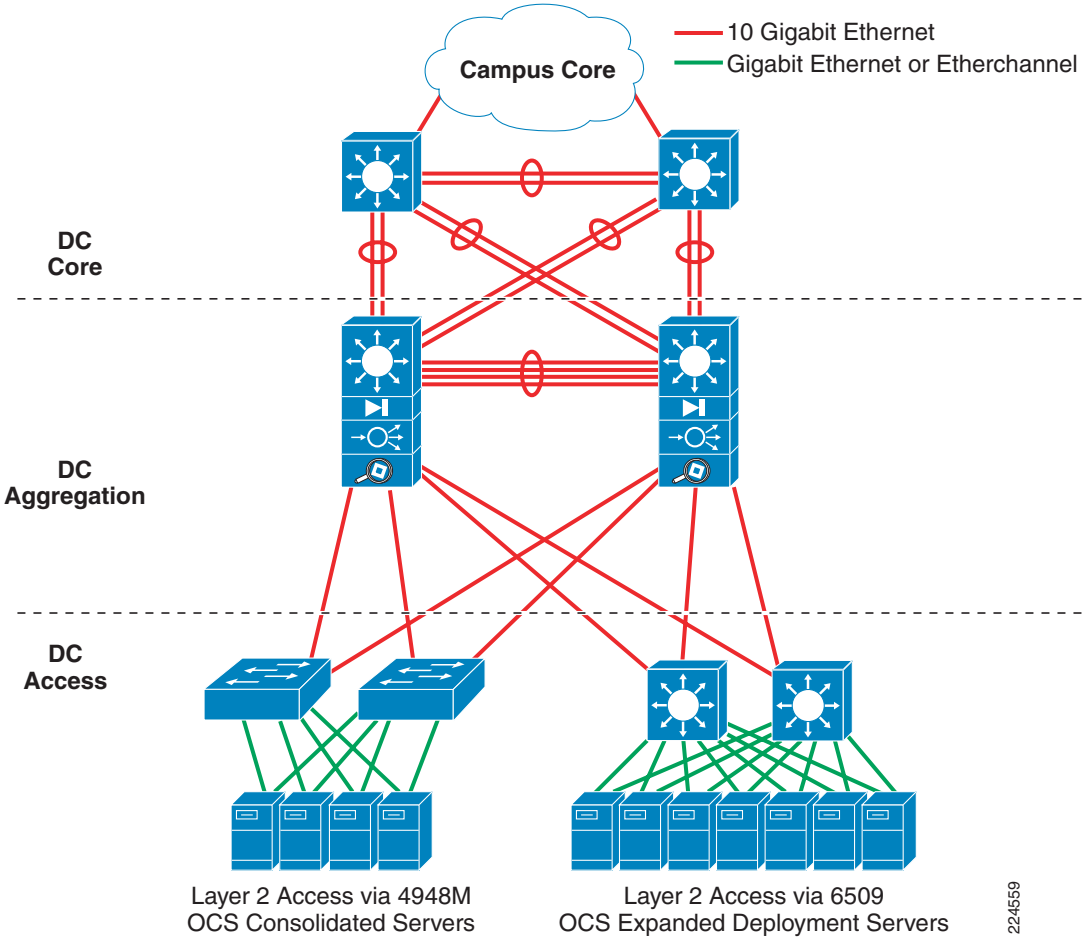
# Data Center Network Components

The Office Communications Server 2007 Solution was validated within a three tier Cisco data center architecture. The topology of the data center infrastructure consists of three distinct functional layers:

- Core
- Aggregation
- Access

Figure 6 shows a multi-tier network topology and some of the services that are available at each of these layers.

***Figure 6 Data Center Multi-Tier Model Topology***



## Core Layer

The core layer provides high-speed connectivity to external entities such as the WAN, intranet, and extranet of the campus. The data center core is a Layer 3 domain where efficient forwarding of packets is the fundamental objective. The data center core is built with high-bandwidth links (10 GE) and employs routing best practices to optimize traffic flows.

## Aggregation Layer

The aggregation layer is a point of convergence for network traffic that provides connectivity between server farms at the access layer and the rest of the enterprise. The aggregation layer supports Layer 2 and Layer 3 functionality and is an ideal location for deploying centralized application, security, and management services. These data center services are shared across the access layer server farms and provide common services in a way that is efficient, scalable, predictable, and deterministic.

The aggregation layer provides a comprehensive set of features for the data center. The following devices support these features in the Office Communications Server 2007 Solution:

- Catalyst 6509 Multilayer aggregation switches
- ACE Module for server load balancing
- Firewall Services Module for security
- Network Analysis Module for traffic analysis

## Access Layer

The primary role of the access layer is to provide the server farms with the required port density. In addition, the access layer must be a flexible, efficient, and predictable environment to support client-to-server and server-to-server traffic. A Layer 2 domain meets these requirements by providing the following:

- Layer 2 adjacency between servers and service devices
- A deterministic, fast converging, loop-free topology

Layer 2 adjacency in the server farm lets you deploy servers or clusters that require the exchange of information at Layer 2 only. It also readily supports access to network services in the aggregation layer, such as load balancers and firewalls. This enables an efficient use of shared, centralized network services by the server farms.

In contrast, if services are deployed at each access switch, the benefit of those services is limited to the servers directly attached to the switch. Through access at Layer 2, it is easier to insert new servers into the access layer. The aggregation layer is responsible for data center services, while the Layer 2 environment focuses on supporting scalable port density.

Layer 3 access designs are not widely deployed in current data centers. However, to minimize fault domains and provide rapid convergence, network administrators are seeking to leverage the benefits of Layer 3. Layer 3 designs do not exclude the introduction of network services, but the transparency of the service at the aggregation layer is more difficult to maintain. As with all access layer designs, the requirements of the application environments drive the decision for either model. The access layer must provide a deterministic environment to ensure a stable Layer 2 domain regardless of its size. A predictable access layer allows spanning tree to converge and recover quickly during failover and fallback.

**Note** For more information on Cisco data center designs or other places in the network, see http://www.cisco.com/go/srnd.

# Service Modules and Deployment Options

When deploying these services, there are a number of choices to make, including:

- Inline versus one-arm design
- Routed versus transparent mode

The following sections describe some of the considerations taken into account when making these choices.

## In-Line versus One-Arm Server Load Balancing

To protect resources, firewalls are always deployed inline, but when deploying the ACE module there is an alternate option. The ACE module can also be placed in one-arm mode where it is only inline for load balanced flows and direct server traffic bypasses it altogether. From a load balancing perspective, inline deployment has the advantage of simplicity, because the VIP is directly in the path between clients and servers.

Although one-arm mode improves performance by offloading non-load-balanced traffic, there is additional complexity because either source NAT or policy-based routing (PBR) must be used to ensure the return flow of traffic. Source NAT might not be a good fit for customers that are using the source IP address to track client usage patterns. PBR avoids this problem but adds other considerations such as asymmetrical routing for non-load-balanced flows.

## Bridged versus Routed Mode on ACE and FWSM

Both ACE and the FWSM can be deployed in either bridged or routed mode. Bridged mode is selected here to simplify the Layer 3 topology. Firewall Services Module terminology refers to “bridged” mode as “transparent” mode. These names are somewhat arbitrary in that bridging technology is used in each. In both designs, the ACE and FWSM contexts are deployed in bridged mode.

Consider the following restrictions when making this decision:

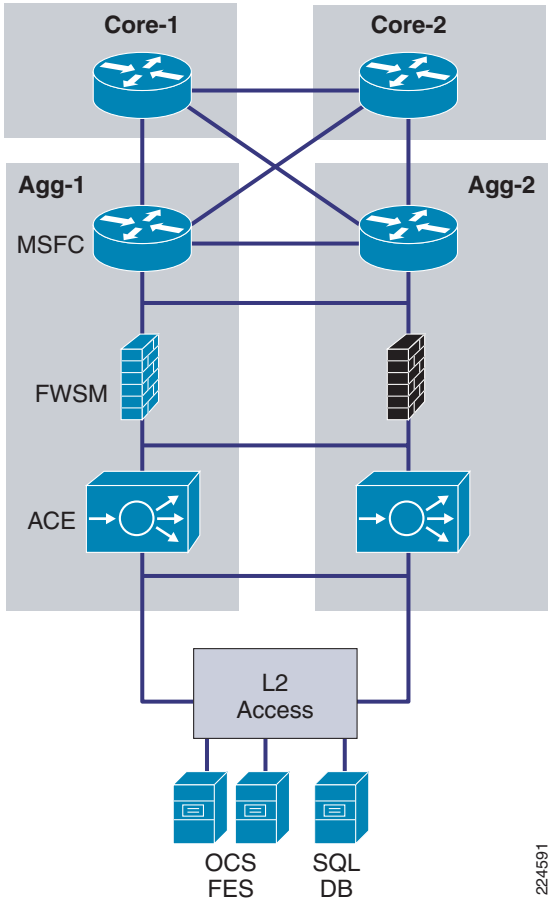
- Routing support—ACE does not support any routing protocols, but only static routing. FWSM supports the OSPF routing protocol. By confining the routing function to the Catalyst 6500 and simply bridging flows across the service module contexts, there are no constraints on which routing protocol can be deployed.
- Number of interfaces per context—There are no practical limitations on the number of bridged or routed interfaces on an individual ACE context. It can bridge two interfaces together and route between others. An FWSM context can support either bridging or routing, but not both. The number of bridged interface pairs is limited to eight with FWSM 3.1. As a result, if there are going to be more than eight interfaces on a given FWSM context, routed mode is required.
- Loops in the aggregation layer—Introducing back-to-back service module contexts in bridged mode allows the possibility of loops. Normally there is not a loop because the standby context does not forward traffic; the event of an active-active scenario between the primary and secondary contexts opens up this possibility. This can happen when heartbeat messages are lost due to inter-switch link failure or configuration error and both contexts believe the other is down. This scenario is mitigated

by forwarding Bridge Protocol Data Units (BPDU) across the services modules. If the intention is to completely remove the possibility of a loop, at least one of the contexts (either ACE or FWSM) must be placed in routed mode.

# Solution Overview

Figure 6 illustrates the data center networking topology used to support validation and performance testing of the Office Communications Server 2007 Solution for the consolidated deployment option. There is a core, aggregation, and access tier to support the server farm. The aggregation switches are equipped with the global Multilayer Switch Feature Card (MSFC), Firewall Services Module (FWSM), and Application Control Engine (ACE). The access switches connect to the aggregation switch over a Layer 2 looped link.

***Figure 7 Data Center Networking Topology for Testing Consolidated Deployment***

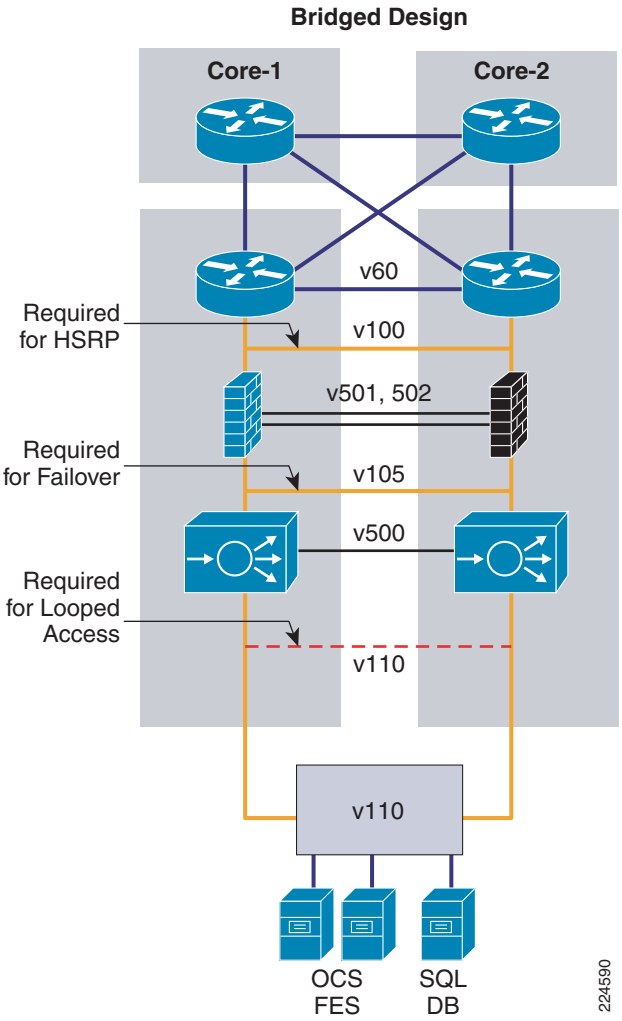



Two Microsoft Office Communications Server 2007 front end servers and one SQL server are connected to the access layer and are located in the same VLAN/IP subnet. In addition, there is an Active Directory server connected to the access layer, but not behind the ACE or Firewall Services Module. This is done so Active Directory traffic that is not related to Office Communications Server 2007 operation does not have to traverse the Firewall and ACE module.

# VLAN Extension

Figure 8 highlights which VLANs need to be extended for this design. The Layer 3 VLAN (v99) is extended for routing updates. VLAN 100 is extended for HSRP so the MSFC, which is the default gateway for all servers, can exchange HSRP keepalives across VLAN 100 to know which should be active. Failover VLANs are also extended for FWSM (v501 and v502) and ACE (v500).

***Figure 8 VLANS Required for this Design***




Each of the vlans that are extended between the aggregation layer switches are carried on 20 Gigabit Ether-channel (interface PO1) which is configured as a 802.1q trunk.

```
sh etherchannel 1 summary
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          -        Te1/5(P)    Te1/6(P)

sh int po1 trunk

Port          Mode         Encapsulation  Status        Native vlan
Po1           on           802.1q         trunking      60
```

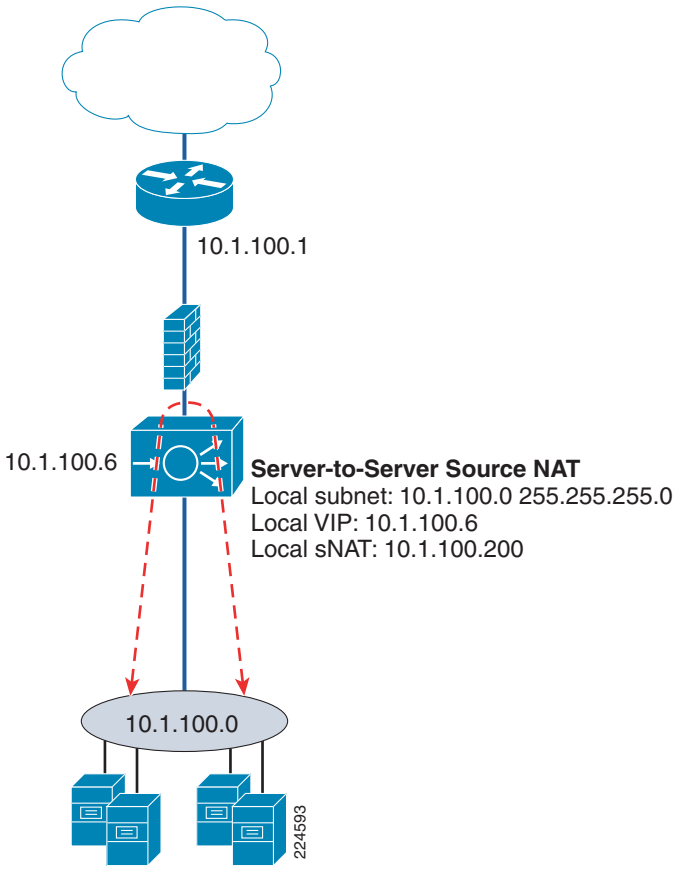
```
Port          Vlans allowed on trunk
Po1           60,70,99-100,105,110,500-503
```

# Server-to-Server Load Balancing

In addition to client-server load balanced connections, there are also cases when the Office Communications Server 2007 front end servers need to originate load balanced connections back into the pool. This is required in Office Communications Server 2007 environment for the Focus element of the front end servers to connect to the Conferencing MCUs in order to track their state, load, and schedule conferences. Since the Office Communications Server 2007 front end servers are both on the same side of the ACE (same subnet), Source Network Address Translation is required to ensure that the traffic traverses the ACE symmetrically. Without source NAT the destination real server would return traffic directly to the originating server, bypassing the ACE and breaking the connection.

Figure 9 shows an example of how this works in our "bridged mode" deployment. The MSFC has a VLAN interface on the 10.1.100.0 subnet and everything below it is also in that same subnet, including the Bridged Virtual Interfaces (BVI) of FWSM and ACE and the servers.

***Figure 9 Load Balancing in Bridged Mode Deployment***




ACE can be configured to perform source NAT only on server initiated connections and not client to server load balanced connections. This is done with multiple class statements under the multi-match load balance policy map, as shown in the following example. ACE intercepts all messages directed to the VIP regardless of whether they originated from the local subnet or externally. Traffic originating from external clients only matches the class EEPOOL-VIP and not the class for the real servers defined by

their source IP address. Traffic originating from the front nd servers matches both the class EEPOOL-VIP and REAL_SERVERS and the additional NAT action is performed. Note that the source NAT address is identified on the actual interface that the traffic is expected to be seen on, in this case, the server-side VLAN 110.

```
class-map match-any EEPOOL-VIP
  2 match virtual-address 10.1.100.6 any

class-map match-all REAL_SERVERS
  2 match source-address 10.1.100.0 255.255.255.0

policy-map multi-match Office Communications Server-POLICY-MAP
  class EEPOOL-VIP
    loadbalance vip inservice
    loadbalance policy EEPOOL-LB-POLICY
    loadbalance vip icmp-reply
    connection advanced-options TCP_IDLE_30min
  class REAL_SERVERS
    nat dynamic 1 vlan 110

interface vlan 110
  description Server-side-vlan
  bridge-group 1
  access-group input BPDU-Allow
  access-group input Office Communications Server-Traffic-Outbound
  nat-pool 1 10.1.100.200 10.1.100.200 netmask 255.255.255.0 pat
  service-policy input Office Communications Server-POLICY-MAP
  no shutdown
```

The connection table shows a server 10.1.100.21 sending to the VIP 10.1.100.6. Then it shows it is load balanced to 10.1.100.20, returning the traffic to 10.1.100.200, which is the address for source NAT, as identified in the NAT pool.

```
ACE1-DC2/ocs# sh conn
conn-id    np dir proto vlan source                destination           state
----------+--+---+-----+----+--------------------+---------------------+------+
6          1  in  TCP   110  10.1.100.21:4270      10.1.100.6:444        ESTAB
39         1  out TCP   110  10.1.100.20:444       10.1.100.200:4161     ESTAB
```

The NAT (XLATE) table shows the originating from VLAN110 from source address 10.1.100.21 destined for VLAN 110 with translated address of 10.1.100.200 which is the NAT pool address.

```
ACE1-DC2/ocs# sh xlate
TCP PAT from vlan110:10.1.100.21/4270 to vlan110:10.1.100.200/4161
```

Microsoft Office Communications Server 2007 front end servers also establish load balanced connections back to themselves. This is because the Focus element of the front end servers acts independently from the other elements, as if it were on a different server altogether. In the connection table you also see connections destined to the same sever from which they originated. An example of this can be see in the following:

```
ACE1-DC2/ocs# sh conn
conn-id    np dir proto vlan source                destination           state
----------+--+---+-----+----+--------------------+---------------------+------+
20         1  in  TCP   110  10.1.100.20:3123      10.1.100.6:444        ESTAB
30         1  out TCP   110  10.1.100.20:444       10.1.100.200:4163     ESTAB
```

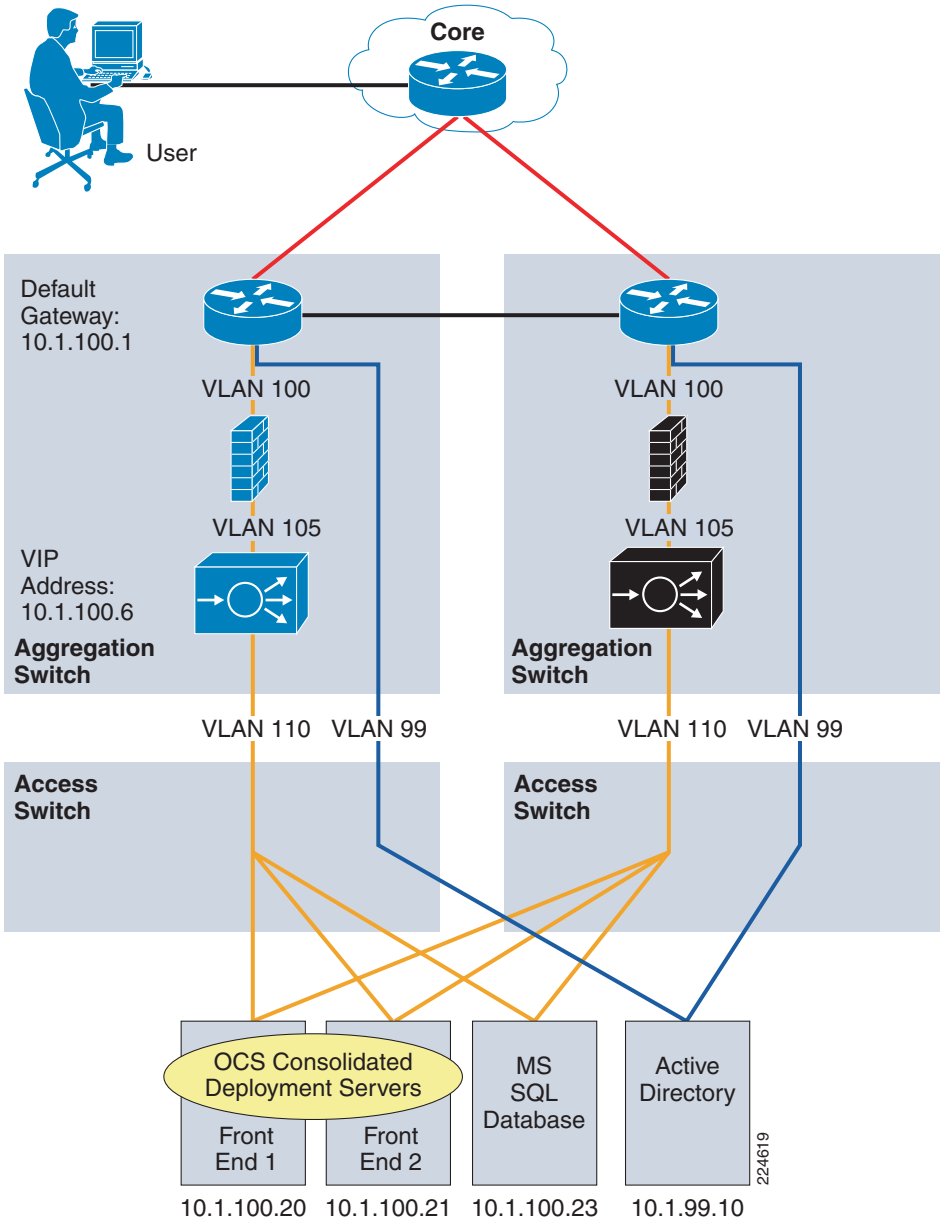
Here you can see a sever at 10.1.100.20 is connecting to the VIP address at 10.1.100.6, which is then load balanced back to the same server at 10.1.100.20 with the source NAT address of 10.1.100.200.

# Solution Configuration Procedure

This section summarizes the configurations of the various components of the solution using the bridged mode design as an example. Catalyst configurations, including service module VLAN assignment, access configuration, ISL configuration, and the ACE and FWSM configurations, including failover, are provided to guide you through the deployment process. At each step of the process appropriate **show** commands are introduced to verify correct operation of the components of the solution. A complete listing of all configurations used in validation is included in Device Configurations.

Figure 10 illustrates the IP addressing scheme used in the test topology.

***Figure 10 IP Addressing Scheme Used in Test Topology***



# Service Module VLAN Assignment

Figure 11 shows how the VLANs are assigned to the service modules. In this case FWSM needs VLAN100, 105, 501, and 502. ACE needs VLAN105, 110, and 500. Because both service modules need VLAN105, three SVCLC groups are created. Group 1 is specific to ACE, group 3 is specific to FWSM, and group 2 is common to both.

# Access Configuration

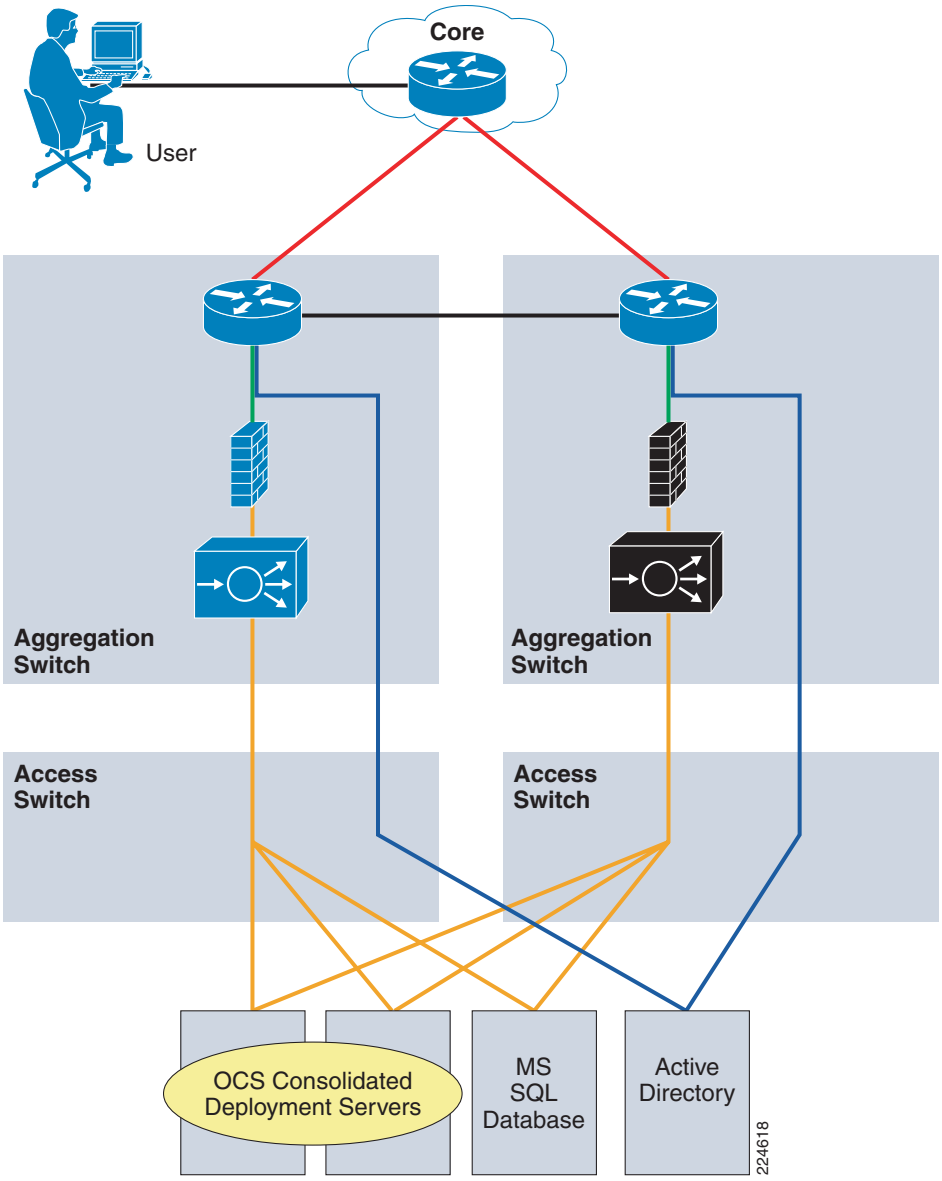
VLAN100 is configured as an interface on the MSFC with HSRP primary on AGG-1. It is the default gateway for the servers. Ten4/3 is the trunk to the access, and in this case only VLAN110 is assigned to it.

# Inter-Switch Link (ISL) Configuration

Port Channel 1 is the trunk between the two aggregation switches and the following VLANs are extended across the link.

```
VLAN99:         L3 link between Agg-1 and Agg-2 MSFCs
VLAN100:        Access VLAN on MSFCs
VLAN105:        Intermediate VLAN between FWSM and ACE contexts
VLAN501:        FWSM fault tolerant vlan
VLAN502:        FWSM state vlan
VLAN500:        ACE ft VLAN
```

*Figure 11 Inter-Switch Link Configuration*




# Service Module Context Configurations

Before configuring the application specific contexts on the FWSM and the ACE module, you must first create them, associate with VLANs, and configure the failover interfaces. The following configuration output illustrates the basic configuration required in the System context of the FWSM and the Admin context of the ACE module to get them up and running with one context defined to support the Office Communications Server 2007 solution.

## FWSM System Context

```
hostname FWSM-A
```

```
!
interface Vlan100
!
interface Vlan105
!
interface Vlan197
!
interface Vlan501
 description LAN Failover Interface
!
interface Vlan502
 description STATE Failover Interface
!
failover
failover lan unit primary
failover lan interface failover Vlan501
failover polltime unit msec 500 holdtime 3
failover polltime interface 3
failover replication http
failover link state Vlan502
failover interface ip failover 192.168.51.1 255.255.255.0 standby 192.168.51.2
failover interface ip state 192.168.52.1 255.255.255.0 standby 192.168.52.2
failover group 1
  preempt
!
admin-context admin
context admin
  allocate-interface Vlan197
  config-url disk:/admin.cfg
  join-failover-group 1
!
context ocs
  allocate-interface Vlan100
  allocate-interface Vlan105
  config-url disk:/ocs.cfg
  join-failover-group 1
!
```

## ACE Admin Context

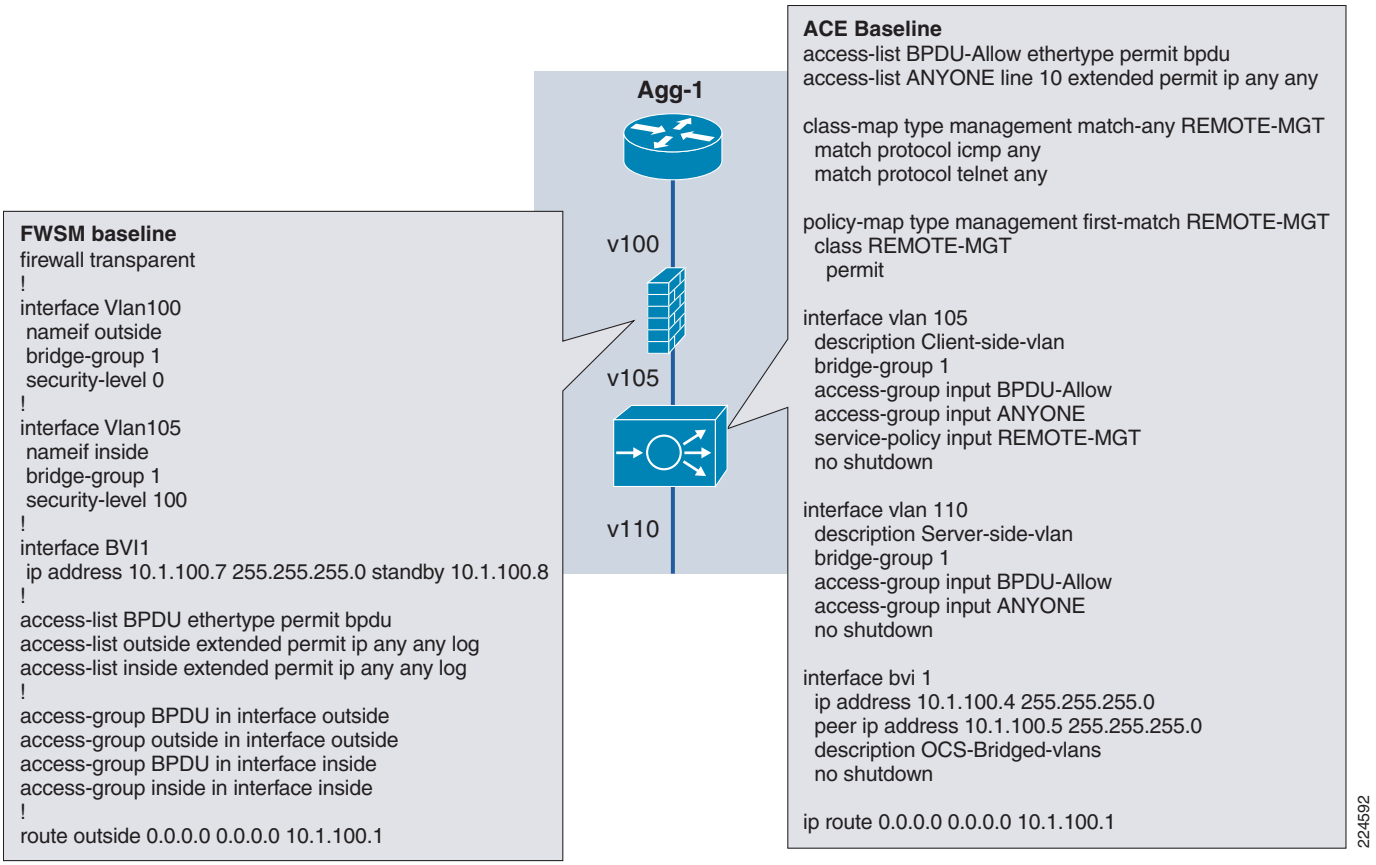
```
hostname ACE1-DC2
!
resource-class Gold
  limit-resource all minimum 10.00 maximum unlimited
  limit-resource conc-connections minimum 10.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited
!
access-list ANYONE line 10 extended permit ip any any
!
ft interface vlan 500
  ip address 192.168.50.1 255.255.255.252
  peer ip address 192.168.50.2 255.255.255.252
  no shutdown
!
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 500
!
ft group 1
  peer 1
  no preempt
```

```
  priority 200
  associate-context Admin
  inservice
!
context ocs
  description Office Communications Server Consolidated
  allocate-interface vlan 105-110
  member Gold
!
ft group 2
  peer 1
  no preempt
  priority 200
  associate-context ocs
  inservice
!
```

Once the application contexts have been defined in the system and admin context of the service modules, they can then be configured. Figure 12 shows the minimum baseline configurations required to get started with the FWSM and the ACE modules. Access Control Lists are wide open and server load balancing is not configured at this point.

As shown in Figure 12, both the FWSM and ACE contexts are configured with an Access Control List to permit BPDU forwarding. This is essential with VLAN100 and VLAN105 extended because if an Active/Active failover scenario occurred with either ACE or FWSM, looping would be prevented using Spanning Tree Protocol.

*Figure 12 Minimum Baseline Configurations for FWSM and ACE Modules*




The Access Control List and bridge-group configuration is very similar between the ACE and the FWSM, except for the following differences:

- The ACE BVI has an alias which serves an HSRP-like function. It can also be used to test connectivity with pings and to remotely telnet or SSH to the context, however, the connection must be made to the actual BVI address, not the BVI alias.
- The class-map/policy-map/service-policy statements are unique to ACE and are not required for simply passing traffic through the context. They are used for load balancing and other functions, such as the management access shown here. These are required for any direct remote access or pinging of the ACE address itself.
- Access groups are applied with Cisco IOS syntax on the ACE module and PIX syntax on FWSM.

# Verifying Operation

Once the initial service module configuration has been completed, a few basic **show** commands verify that everything is running as expected.

The **show interface** command on the ACE module indicates if the VLANs are correctly assigned from the supervisor via the **svclc** commands and are up and running.

```
ACE1-DC2/ocs# sh interface vlan105

vlan105 is up
```

```
  Hardware type is VLAN
  MAC address is 00:07:0e:0f:21:39
  Mode : transparent
  Bridge group number: 1
  FT status is standby
  Description:Client-side-vlan
  MTU: 1500 bytes
  Last cleared: never
  Alias IP address not set
  Peer IP address not set
  Assigned from the Supervisor, up on Supervisor
     9579 unicast packets input, 44171031 bytes
     592394 multicast, 25529 broadcast
     0 input errors, 0 unknown, 0 ignored, 0 unicast RPF drops
     23 unicast packets output, 1395136 bytes
     0 multicast, 21776 broadcast
     0 output errors, 0 ignored
```

Similarly on the FWSM, the **show interface** command shows you that the connection between the module and the Catalyst supervisor is functioning correctly. Here you can see that VLAN 100 has been assigned from the supervisor and is available to be assigned to a context.

```
FWSM-A# sh interface vlan100

Interface Vlan100 "", is up, line protocol is up
  Hardware is EtherSVI
        Available for allocation to a context
        MAC address 001f.6c67.5f00, MTU not set
        IP address unassigned
```

Failover configuration and status of the ACE module can be verified by issuing the **show ft group summary** command on the primary device from the Admin context.

```
ACE1-DC2/Admin# sh ft group summary

FT Group                    : 1
Configured Status           : in-service
Maintenance mode            : MAINT_MODE_OFF
My State                    : FSM_FT_STATE_ACTIVE
My Config Priority          : 200
My Net Priority             : 200
My Preempt                  : Disabled
Peer State                  : FSM_FT_STATE_STANDBY_HOT
Peer Config Priority        : 100
Peer Net Priority           : 100
Peer Preempt                : Disabled
Peer Id                     : 1
No. of Contexts             : 1
```

Failover configuration and status of the FWSM can be verified by issuing the **show fail** command from the system context of the primary device.

```
FWSM-A# sh fail
Failover On
Failover unit Primary
Failover LAN Interface: failover Vlan 501 (up)
Unit Poll frequency 500 milliseconds, holdtime 3 seconds
Interface Poll frequency 3 seconds
Interface Policy 50%
Monitored Interfaces 3 of 250 maximum
failover replication http
Config sync: active
Version: Ours 3.1(6), Mate 3.1(6)
Group 1 last failover at: 22:30:18 UTC Jun 15 2008
```

```
This host:    Primary
Group 1       State:          Active
              Active time:    3679 (sec)

              admin Interface outside (172.28.197.30): Normal
              ocs Interface outside (10.1.100.7): Normal
              ocs Interface inside (10.1.100.7): Normal

Other host:   Secondary
Group 1       State:          Standby Ready
              Active time:    0 (sec)

              admin Interface outside (172.28.197.31): Normal
              ocs Interface outside (10.1.100.8): Normal
              ocs Interface inside (10.1.100.8): Normal
```

# ACE Load Balancing Configuration Procedure

Server load balancing configuration procedure for the ACE module involves defining the following elements of the ACE module:

- Health check probes
- Real servers
- Serverfarm
- TCP timeout parameter map
- Server persistence (sticky)
- VIP class map
- NAT class map
- Load balance policy map
- Multi-match policy map
- NAT pool association to VLAN interface

## Health Check Probes

In the following example, we configure two different probes on the ACE to be used together to determine the health of the Office Communications Server 2007 servers and take them out of rotation when a problem is detected. The first probe is a simple ping probe which is issued every two seconds. This is intended to detect hardware failures quickly.

The second probe is configured to test TCP port 5061 used for SIP, which is the primary communications protocol used by Office Communications Server 2007. This probe is issued every 30 seconds so as not to put an unnecessary load on the Office Communications Server 2007 application environment.

```
probe icmp PING
  interval 2
  passdetect interval 2
  passdetect count 1

probe tcp SIP
  port 5061
  interval 30
  passdetect interval 2
```

```
  passdetect count 1
```

## Real Servers

Two real servers were used for testing of the consolidated deployment option.

```
rserver host OCS1
  description Front End Server 1
  ip address 10.1.100.20
  inservice

rserver host OCS2
  description Front End Server 2
  ip address 10.1.100.21
  inservice
```

## Serverfarm

Here the serverfarm EEPOOL is defined with the least connections load balancing predictor and associated health check probes and real servers.

```
serverfarm host EEPOOL
  predictor leastconns
  probe PING
  probe SIP
  rserver OCS1
    inservice
  rserver OCS2
    inservice


TCP Time-out parameter map
TCP idle time  out is configured for 30 minuets.

parameter-map type connection TCP_IDLE_30min
  set timeout inactivity 1800
```

## Server Persistence (Sticky)

Stickiness based on client source IP address is used for server persistence.

```
sticky ip-netmask 255.255.255.255 address source EEPOOLGP
  timeout 30
  replicate sticky
  serverfarm EEPOOL
```

## VIP Class Map

This is where we define the virtual IP address. It is configured to listen on “any” port which simplifies the configuration. Access to this VIP is restricted by the firewall module.

```
class-map match-any EEPOOL-VIP
  2 match virtual-address 10.1.100.6 any
```

## NAT Class Map

This is where we define the source IP address of the servers that are subject to source NAT when initiating connections to the VIP address.

```
class-map match-all REAL_SERVERS
  2 match source-address 10.1.100.0 255.255.255.0

Load balance policy map
Here we associate the serverfarm with a load balancing policy map.

policy-map type loadbalance first-match EEPOOL-LB-POLICY
  class class-default
    sticky-serverfarm EEPOOLGP
```

## Multi-Match Policy Map

```
policy-map multi-match OCS-POLICY-MAP
  class EEPOOL-VIP
    loadbalance vip inservice
    loadbalance policy EEPOOL-LB-POLICY
    loadbalance vip icmp-reply
    connection advanced-options TCP_IDLE_30min
  class REAL_SERVERS
    nat dynamic 1 vlan 110
```

## Add NAT Pool to Server VLAN

```
interface vlan 110
  nat-pool 1 10.1.100.200 10.1.100.200 netmask 255.255.255.0 pat
```

## Verifying Operation

At this point the basic components for the solution are in place. No security has been applied at this point to facilitate functional testing. Issue the following ACE **show** commands to verify basic load balancing elements are in place:

- **show Rserver**—Both servers should be OPERATIONAL.
- **show Service-policy**—Should be INSERVICE.

You will notice active connections on your real servers and through the VIP via the **sh service policy** command even though there are no active users logged into the system. These connections are made by the Media Conference Servers on the front end servers connecting back to the VIP to be load balanced back to the Focus element residing on each front end server.

Typically you see four times the number of servers connections for each server. So in a two server deployment, you should expect eight connections to the VIP and through the NAT table. This varies during the course of normal operations, as additional connections are added to support conferencing activities.

The following is an example of this steady state behavior of a two server consolidated deployment of Office Communications Server 2007 Enterprise Edition. The output of ACE **sh conn** and **sh xlate** commands are provided below and provide an example of what you would expect to see when you first get your environment up and running. The output has been shortened to focus on the server-initiated connections to the VIP. Here you can see the connections to the VIP address on TCP port 444 and in the NAT table you can see that the source address of these connections are translated to the NAT address of 10.1.100.200.

```
ACE1-DC2/ocs# sh conn

conn-id    np dir proto vlan source               destination          state
----------+--+---+-----+----+--------------------+--------------------+------+
10985      1  in  TCP   110  10.1.100.21:2680      10.1.100.6:444       ESTAB
```

```
10984      1  out TCP   110  10.1.100.20:444       10.1.100.200:1363     ESTAB

15013      1  in  TCP   110  10.1.100.21:2684      10.1.100.6:444        ESTAB
15012      1  out TCP   110  10.1.100.20:444       10.1.100.200:1370     ESTAB

15561      1  in  TCP   110  10.1.100.21:2682      10.1.100.6:444        ESTAB
16514      1  out TCP   110  10.1.100.20:444       10.1.100.200:1365     ESTAB


ACE1-DC2/ocs# sh xlate
--------------------------------------------------------------------------------
TCP PAT from vlan110:10.1.100.21/2680 to vlan110:10.1.100.200/1363

TCP PAT from vlan110:10.1.100.21/2684 to vlan110:10.1.100.200/1370

TCP PAT from vlan110:10.1.100.21/2682 to vlan110:10.1.100.200/1365
```

## Firewall Services Module Configuration Procedure

The FWSM has already been placed in line at this point and all that is left in the configuration process is to apply the access control list (ACL) to protect the ACE VIP address and the Office Communications Server 2007 real servers from unwanted traffic. The following access control list can be applied to the outside interface of the FWSM on VLAN 100 or alternatively to the ACE module outside interface VLAN 105, if not using the FWSM in the solution.

```
access-list OCS-Traffic-Inbound extended permit tcp any host 10.1.100.6 eq 5061
access-list OCS-Traffic-Inbound extended permit tcp any host 10.1.100.6 eq https
access-list OCS-Traffic-Inbound extended permit tcp any 10.1.100.0 255.255.255.0 eq 8057
access-list OCS-Traffic-Inbound extended permit udp any 10.1.100.0 255.255.255.0 range
49152 65535
access-list OCS-Traffic-Inbound extended permit udp any 10.1.100.0 255.255.255.0 eq 135
access-list OCS-Traffic-Inbound extended permit udp any eq domain 10.1.100.0 255.255.255.0
access-list OCS-Traffic-Inbound extended permit tcp any eq ldap 10.1.100.0 255.255.255.0
access-list OCS-Traffic-Inbound extended permit udp any eq kerberos 10.1.100.0
255.255.255.0
access-list OCS-Traffic-Inbound extended permit udp any eq netbios-ns 10.1.100.0
255.255.255.0
access-list OCS-Traffic-Inbound extended deny ip any any
```

Apply to FWSM outside interface:

```
access-group OCS-Traffic-Inbound in interface outside
```

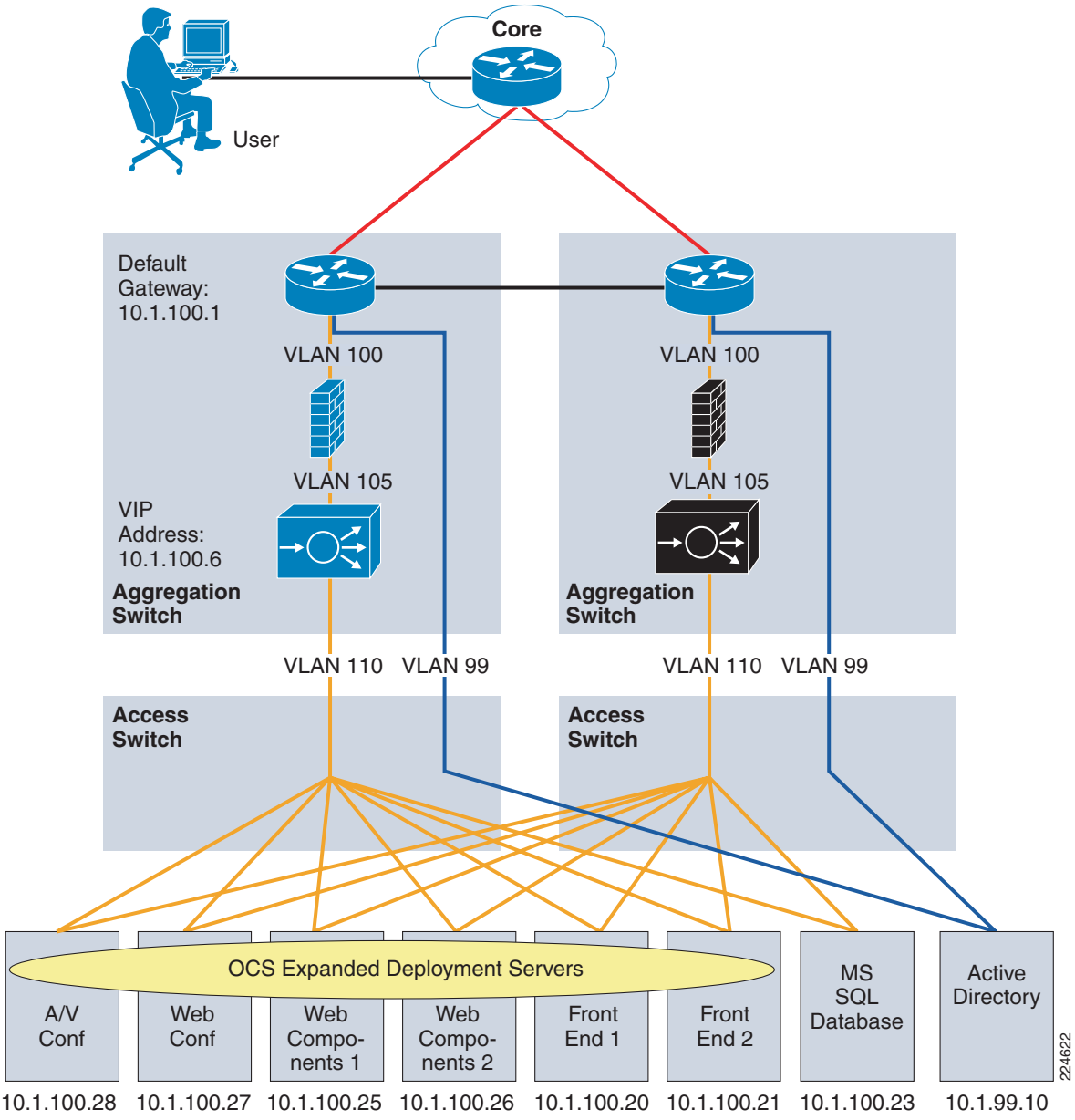
Alternatively apply to ACE outside interface:

```
interface vlan 105
access-group input OCS-Traffic-Inbound
```

# Expanded Deployment Option

Figure 13 represents a typical expanded deployment scenario. Although this was not tested during this initial phase of the project, lessons learned from validation testing of the consolidated deployment option have been expanded to suggest this possible topology and device configurations.

*Figure 13 Expanded Deployment Scenario*




In the expanded deployment option, the function of Web Components, Web Conferencing, and A/V Conferencing have been deployed on their own dedicated servers. In the Web Components case, we have used two servers and are load balancing traffic to them via the ACE module. In this example, we only have a single server for Web Conferencing and A/V Conferencing. It is possible to have multiple servers in the Web Conferencing and A/V Conferencing pool, but they would not be load balanced by the ACE module due to the Focus element on the fron end server controlling this type of traffic.

The following ACE configuration can be added to the consolidated configuration to support the expanded topology described in Figure 13.

```
rserver host WC1
  description Web Components Server 1
  ip address 10.1.100.25
  inservice
```

```
rserver host WC2
  description Web Components Server 2
  ip address 10.1.100.26
  inservice

serverfarm host WCPOOL
  predictor leastconns
  probe PING
  probe SIP-TLS
  rserver WC1
    inservice
  rserver WC2
    inservice

sticky ip-netmask 255.255.255.255 address source WCPOOLGP
  timeout 30
  replicate sticky
  serverfarm WCPOOL

class-map match-any EEPOOL-VIP
  2 match virtual-address 10.1.100.7 any

policy-map type loadbalance first-match WCPOOL-LB-POLICY
  class class-default
    sticky-serverfarm WCPOOLGP

policy-map multi-match WC-POLICY-MAP
  class WCPOOL-VIP
    loadbalance vip inservice
    loadbalance policy WCPOOL-LB-POLICY
    loadbalance vip icmp-reply
    connection advanced-options TCP_IDLE_30min

interface vlan 105
    service-policy input WC-POLICY-MAP
```

# Performance Monitoring

There are many counters available to assess the health and performance of the Office Communications Server 2007 application environment via the Microsoft Server Perfmon tool. These can be used to assess the load on the various components of Office Communications Server 2007 to determine if there are any problems and if additional servers are need to support scaling.

To monitor the overall computer health of Office Communications Server 2007 servers, the performance counters listed in Table 5 should be monitored regardless of server role. Note that there is a mix of processor, memory, process, networking, and .NET runtime counters that are applicable to all Office Communications Server 2007 servers. We discuss next what performance counters to monitor for specific server roles.

***Table 5 Overall Health Performance Counters***

| Category Name | Counter Name |
|---|---|
| Processor | % Processor Time |
| Memory | Available Bytes |
| Memory | Pages/sec |
| Memory | % Committed Bytes in Use |

*Table 5 Overall Health Performance Counters*

| Category Name | Counter Name |
|---|---|
| Process | % Processor Time |
| Process | Private Bytes |
| Process | Thread Count |
| Physical Disk | %Idle Time |
| Network Interface | Total Bytes/sec. |
| Network Interface | Current Bandwidth |
| TCPv4 | Segments sent/sec. |
| TCPv4 | Segments retransmitted/sec. |
| Calculated Value | % Network Utilization |
| .NET CLR Memory | # Bytes in All Heaps |
| .NET CLR Memory | # GC Handles |
| .NET CLR Memory | % Time in GC |
| LC:SIP - 00 - Networking | SIP - 006 -Connections Refused Due To Server Overload |
| LC:SIP - 00 - Networking | SIP - 007 -Connections Refused Due To Server Overload/Sec. |
| LC:SIP - 00 - Networking | SIP - 029 -Last DNS query time |

To monitor front end server-specific performance counters, use the most pertinent counters shown in Table 6. You may choose to monitor more or less than what is specified in Table 6.

*Table 6 Front-End Server-Specific Performance Counters*

| Category Name | Counter Name |
|---|---|
| LC:SIP - 01 - Peers | SIP - 000 - Connections Active |
| LC:SIP - 01 - Peers | SIP - 018 - Sends Timed-Out |
| LC:SIP - 01 - Peers | SIP - 020 - Average Outgoing Queue Delay |
| The following performance counters provide detail on the type of responses received by the Front-End Server. These responses are collected based on the SIP error categories. | |
| LC:SIP - 04 - Responses | SIP - 038 - Local 400 Responses |
| LC:SIP - 04 - Responses | SIP - 042 - Local 404 Responses |
| LC:SIP - 04 - Responses | SIP - 044 - Local 482 Responses |
| LC:SIP - 04 - Responses | SIP - 046 - Local 483 Responses |
| LC:SIP - 04 - Responses | SIP - 050 - Local 500 Responses |
| LC:SIP - 04 - Responses | SIP - 052 - Local 503 Responses |
| LC:SIP - 04 - Responses | SIP - 054 - Local 504 Responses |

*Table 6 Front-End Server-Specific Performance Counters*

| Category Name | Counter Name |
|---|---|
| The following performance counters provides an indication of the backlog of SIP messages that the Front-End Server has yet to process. If the number of unprocessed SIP messages is consistently high, it provides a good indication that the front end server is under heavy load and additional Front-End Servers need to be added. | |
| LC:SIP - 07 - Load Management | SIP - 000 - Average Holding Time For Incoming Messages |
| LC:SIP - 07 - Load Management | SIP - 004 - Incoming Messages Held Above High Watermark |
| The following performance counters provide insight to database specific connections issues to the SQL back end server. | |
| LC:Usrv - 00 -DBStore | Usrv - 020 - Throttled requests/sec. |
| LC:Usrv - 00 -DBStore | Usrv - 014 - Total Dropped Requests |
| LC:Usrv - 00 -DBStore | Usrv - 017 - Total ODBC Timeout Errors |
| LC:Usrv - 00 -DBStore | Usrv - 018 - Total Severe SQL Errors |
| LC:Usrv - 00 -DBStore | Usrv - 019 - Total Fatal SQL Errors |
| The following performance counters are specific to enhanced presence subscriptions. Subscription requests can have a deep impact of server performance. | |
| LC:Usrv - 04 -Rich presence subscribe SQL calls | Usrv - 000 - RtcBatchSubscribeCategoryList Sproc calls/sec. |
| LC:Usrv - 04 -Rich presence subscribe SQL calls | Usrv - 026 - RtcBatchQueryCategories Sproc calls/sec. |
| LC:Usrv - 04 -Rich presence subscribe SQL calls | Usrv - 031 - Number of requests in the call to RtcBatchQueryCategories |
| LC:Usrv - 05 -Rich presence service SQL calls | Usrv - 000 - RtcPublishMultipleCategories Sproc calls/sec. |
| The following performance counters provide information about active conferences handled by the enterprise pool and should be approximately the same across all front end servers within a pool. | |
| LC:Usrv - 29 - Pool Conference Statistics | Usrv - 001 - Active Conference Count |
| LC:Usrv - 29 - Pool Conference Statistics | Usrv - 002 - Active Participant Count |
| The following performance counters are specific to enterprise voice. They only need to be monitored if VoIP is configured and used by users. | |
| LC:RoutingApps - 00 - UC Routing Applications | RoutingApps - 003 - Errors from UM server |
| LC:RoutingApps - 00 - UC Routing Applications | RoutingApps - 004 - Failed Exchange UM calls |
| LC:RoutingApps - 00 - UC Routing Applications | RoutingApps - 005 - Failed Outbound PSTN calls |
| LC:RoutingApps - 00 - UC Routing Applications | RoutingApps - 014 - Received 5XX from VoIP gateway |
| LC:RoutingApps - 00 - UC Routing Applications | RoutingApps - 016 - Gateway detected to be down |
| LC:RoutingApps - 00 - UC Routing Applications | RoutingApps - 017 - Calls failed due to gateway unavailability |
| LC:RoutingApps - 00 - UC Routing Applications | RoutingApps - 018 - Calls failed due to no matching route |

Although the IM Conferencing Server (IM MCU) service is always collocated with the front end server, Table 7 highlights the suggested performance counters specific to this server role if you want to profile this service.

*Table 7 Performance Counters for IM MCU Service*

| Category Name | Counter Name |
|---|---|
| LC:ImMcu - 00 - IMMCU Conferences | IMMCU - 000 - Active Conferences |
| LC:ImMcu - 00 - IMMCU Conferences | IMMCU - 001 - Connected Users |
| LC:ImMcu - 00 - IMMCU Conferences | IMMCU - 005 - Incoming Messages per sec. |
| LC:ImMcu - 00 - IMMCU Conferences | IMMCU - 007 - Outgoing Messages per sec. |
| LC:ImMcu - 00 - IMMCU Conferences | IMMCU - 013 - Incoming Infos per sec. |
| LC:IMMCU - 02 -MCU Health And Performance | IMMCU - 005 - MCU Health State |
| LC:IMMCU - 02 -MCU Health And Performance | IMMCU - 006 - MCU Draining State |

Table 8 lists the type of performance counters suggested to monitor for the Web Components server role. If this server role is installed on a separate physical server, as in the case of an enterprise pool in an expanded topology, these performance counters target the health of the ASP service running the Web Components.

*Table 8 Performance Counters for Web Components Server*

| Category Name | Counter Name |
|---|---|
| ASP.NET Apps v2.0.50727 | Requests Failed |
| ASP.NET Apps v2.0.50727 | Requests/Sec. |
| ASP.NET Apps v2.0.50727 | Requests In Application Queue |
| LC:DLX - 00 - Distribution List Expansion | DLX - 000 - Valid input requests/sec. |
| LC:DLX - 00 - Distribution List Expansion | DLX - 002 - Average processing time for a valid requests in milliseconds |
| LC:DLX - 00 - Distribution List Expansion | DLX - 015 - Invalid input requests |
| LC:DLX - 00 - Distribution List Expansion | DLX - 026 - Succeeded Address Book File Requests/second |
| LC:DLX - 00 - Distribution List Expansion | DLX - 027 - Average processing time for a succeeded address Book file request in milliseconds |
| LC:DLX - 00 - Distribution List Expansion | DLX - 029 - Failed Address Book File Requests |

The performance counters in Table 9 are suggested to monitor the health of the Audio/Video Conferencing Server service.

*Table 9 Performance Counters for Audio/Video Conferencing Server*

| Category Name | Counter Name |
|---|---|
| AVMCU - 00 Operations | AVMCU - 000 - Number of Conferences |
| AVMCU - 00 Operations | AVMCU - 001 - Number of Users |

*Table 9 Performance Counters for Audio/Video Conferencing Server*

| Category Name | Counter Name |
|---|---|
| LC:AVMCU - 04 -MCU Health And Performance | AVMCU - 005 - MCU Health State |
| LC:AVMCU - 04 -MCU Health And Performance | AVMCU - 006 - MCU Draining State |
| MEDIA - 00 - Operations | MEDIA - 000 - Global health |
| MEDIA - 00 - Operations | MEDIA - 003 - Number of packets dropped by Secure RTP/sec. |
| MEDIA - 01 - Planning | MEDIA - 000 - Number of conferences started |
| MEDIA - 01 - Planning | MEDIA - 001 - Number of audio channels started |
| MEDIA - 01 - Planning | MEDIA - 002 - Number of video channels started |
| MEDIA - 01 - Planning | MEDIA - 004 - Number of conferences with OVERLOADED health |

To monitor the Web Conferencing Server, the performance counters in Table 10 are recommended.

*Table 10 Performance Counters for Web Conferencing Server*

| Category Name | Counter Name |
|---|---|
| LC:DATAMCU - 000 -Conferences | DATAMCU - 000 - Conferences |
| LC:DATAMCU - 000 -Conferences | DATAMCU - 000 - Connected Users |
| LC:DATAMCU - 02 -MCU Health And Performance | DATAMCU - 005 - MCU Health State |
| LC:DATAMCU - 02 -MCU Health And Performance | DATAMCU - 006 - MCU Draining State |

To monitor the health of the SQL instance running on the back end server, the performance counters in Table 11 are recommended.

*Table 11 Performance Counters for SQL Instance on Back End Server*

| Category Name | Counter Name |
|---|---|
| MSSQL$RTC:User Settable | Query |
| MSSQL$RTC:Access Methods | Full Scans/sec. |
| MSSQL$RTC:Access Methods | Page Splits/sec. |
| MSSQL$RTC:Access Methods | Pages Allocated/sec. |
| MSSQL$RTC:Access Methods | Range Scans/sec. |
| MSSQL$RTC:Databases | Active Transactions |
| MSSQL$RTC:Databases | Log File(s) Used Size (KB) |
| MSSQL$RTC:Databases | Log Flush Wait Time |
| MSSQL$RTC:Databases | Transactions/sec. |
| MSSQL$RTC:Latches | Latch Waits/sec. |
| MSSQL$RTC:Latches | Total Latch Wait Time (ms) |

*Table 11 Performance Counters for SQL Instance on Back End Server*

| Category Name | Counter Name |
|---|---|
| MSSQL$RTC:Locks | Average Wait Time (ms) |
| MSSQL$RTC:Locks | Lock Wait Time (ms) |
| MSSQL$RTC:Locks | Number of Deadlocks/sec. |
| MSSQL$RTC:Plan Cache | Cache Hit Ratio |
| MSSQL$RTC:SQL Statistics | Batch Requests/sec. |
| MSSQL$RTC:SQL Statistics | SQL Re-Compilations/sec. |
| MSSQL$RTC:Wait Statistics | Lock waits |
| MSSQL$RTC:Wait Statistics | Log buffer waits |
| MSSQL$RTC:Wait Statistics | Log write waits |

# Solution Validation Testing

Two types of testing were performed against the consolidated deployment model of Office Communications Server 2007 to validate the solution, scalability and failover testing.

Scalability tests were performed to get a sense of the load that a typical small scale deployment can support and failover testing was performed to determine how the application behaves under common failure scenarios.

The physical profile of the servers used in this test environment consisted of:

- Front end 1—1 RU, Dual Core Xeon 3050 @ 2.13 Ghz, 2 GB RAM
- Front end 2—1 RU, Dual Core Xeon 3050 @ 2.13 Ghz, 2 GB RAM
- AD/DNS—1 RU, Dual Core Xeon 3050 @ 2.13 Ghz, 2 GB RAM
- SQL server—2 RU, Quad Core Xeon 5140 @ 2.33 Ghz, 3.252 GB RAM

A summary of these results achieved during this validation testing effort are contained in the following sections.

# Scalability

A number of tests were run against the test bed with increasing numbers of simultaneous users logged into the system executing various functions. The Office Communications Server 2007 consolidated deployment option was tested with two servers and achieved 22,000 concurrent users executing IM session conferencing traffic and presence state traffic.

## Test Results Summary

- Run time = 41 mins
- 22,000 active end points
- Transaction pass rate = 99.9%
- 45 Mbps throughput on ACE
- Server CPU utilization average = 9%

- Server memory usage = 44%
- SQL server CPU utilization = 14%
- SQL server memory usage = 56%

Based on these results it is reasonable to expect that a two server deployment could support up to 30,000 concurrent users and a much larger user population base. This deployment can be scaled up to support even larger numbers of concurrent users and base population by introducing additional front end servers.

# Failover

A few common failure scenarios were tested to assess the resiliency of the Office Communications Server 2007 client and connection replication on the ACE module. The following functions of Office Communications Server 2007 were evaluated under the following failure conditions.

- Features tested:
  - Office Communications Server 2007 client active session
  - Instant messaging conversation
  - Video call
  - Live meeting (Web conference)
- Failure scenarios:
  - Clear active connections on ACE module
  - Server failure
  - ACE failover

The Office Communications Server 2007 client is very resilient and automatically reconnects after failure events given that the back end system is available. All three failure scenarios were executed and the Office Communications Server 2007 client reconnects to servers within seconds under the first failure condition and within 10-15 seconds for the second two. Active instant messaging conversations are also reestablished, but active video as part of an IM conversation is not restored and must be manually restarted.

Peer-to-peer voice calls between client PCs using Office Communications Server 2007 are not affected by failure events due to the nature of the traffic flow which is established directly between the end stations and therefore does not traverse the front end servers. Testing showed that voice calls continue to operate during failover events.

Microsoft Office Live Meeting used for Web and video conferences does reconnect active meetings after failure scenarios, but video must be re-shared by the users.

# Hardware and Software Tested

## Core and Aggregation Switches

Hardware:

- cisco WS-C6509-E (R7000) processor (revision 1.3) with 983008K/65536K bytes of memory.
- Processor board ID SMG1113N59U
- SR71000 CPU at 600Mhz, Implementation 0x504, Rev 1.2, 512KB L2 Cache

Software:

- Cisco Internetwork Operating System Software
- IOS$^{tm}$ s72033_rp Software (s72033_rp-ADVENTERPRISEK9_WAN-M), Version 12.2(18)SXF10, RELEASE SOFTWARE (fc1)

## Access Layer Switches

Hardware:

- cisco WS-C4948-10GE (MPC8540) processor (revision 5) with 262144K bytes of memory.
- Processor board ID FOX112603JY
- MPC8540 CPU at 667Mhz, Fixed Module

Software:

- Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500-ENTSERVICESK9-M), Version 12.2(31)SGA3, RELEASE SOFTWARE (fc1)

## ACE Module

Hardware:

- Product Number: ACE10-6500-K9
- Serial Number: SAD112207M7
- Card Index: 207
- Hardware Rev: 1.4
- Feature Bits: 0000 0001
- Slot No.: 3
- Type: ACE

Software:

- loader: Version 12.2[120]
- system: Version A2(1.0) (latest version of ACE code)
- build: 3.0(0)A2(1.0)
- system image file: [LCP] disk0:c6ace-t1k9-mz.A2_1.bin
- installed license: ACE-08G-LIC ACE-VIRT-250 ACE10-16G-LIC ACE-SSL-20K-K9

## Firewall Services Module

Hardware:

- WS-SVC-FWM-1, 1024 MB RAM, CPU Pentium III 1000 MHz
- Flash SMART CF @ 0xc321, 20MB

Software:

- FWSM Firewall Version 3.1(6) (current Safe Harbor certified version)
- Device Manager Version 5.2(3)F

### Front End Servers

Hardware:

- IBM XSERIES_3250, Xeon® CPU 3050 @ 2.13Ghz, 2 GB RAM

Software:

- Microsoft Windows Server 2003 Enterprise Edition, Service Pack 2

### SQL Server

Hardware:

- Intel® Xeon® CPU 5140 @ 2.33Ghz, 3.25 GB RAM

Software:

- Microsoft Windows Server 2003 Enterprise Edition, Service Pack 2

### Active Directory Server

Hardware:

- Intel® Xeon® CPU 5140 @ 2.33Ghz, 3.25 GB RAM

Software:

- Microsoft Windows Server 2003 Enterprise Edition, Service Pack 2

## Scalability Testing Details

22,000 users—Instant messaging and presence

### Test Configuration

IM settings:

- IM Conferences Per User Per Day = 48
- Max IM Conference Length In Sec. = 300
- Add Participant To IM Conference Per Hour = 60
- Actions Done Per Minute = 2
- Two Party IM Conference Percentage = 90
- IM Send Action Percentage = 8

Presence settings:

- Get Presence Call Per User Per Hour = 25
- Get Presence Target Low = 2
- Get Presence Target High = 10
- Change Presence Per Hour = 6
- Change Calendar State Per User Per Day = 3

## Test Results Summary

- Run time = 41 mins
- 22,000 active end points
- Transaction pass rate = 99.9%
- 45 Mbps throughput on ACE
- Server CPU utilization average = 9%
- Server memory usage = 44%
- SQL Server CPU utilization = 14%
- SQL Server memory usage = 56%

## Test Run Observations

*Figure 14 Perfmon View from Test PC #1*

| | | |
|---|---|---|
| LST: - 00 - General Information | | |
| LST - 000 - Total Time Spent in Minutes | | 41 |
| LST - 001 - Total active endpoints | [ | 10999] |
| LST - 002 - Total failed logon | | 82 |
| LST - 003 - Total logon attempts | | 11130 |
| LST - 004 - Total endpoints disconnected | | 49 |
| LST - 005 - Overall - Pass Rate % | | 99.981 |
| LST - 007 - Transaction - Pass Rate % | | 99.958 |
| LST - 009 - Request/Response - Pass Rate % | | 100.000 |

224635

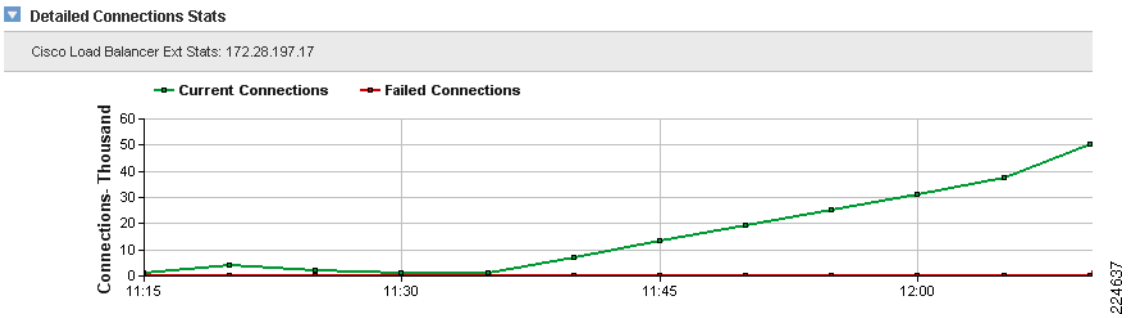
*Figure 15 Perfmon View from Test PC #2*

| | | |
|---|---|---|
| LST: - 00 - General Information | | |
| LST - 000 - Total Time Spent in Minutes | | 41 |
| LST - 001 - Total active endpoints | [ | 10999] |
| LST - 002 - Total failed logon | | 82 |
| LST - 003 - Total logon attempts | | 11130 |
| LST - 004 - Total endpoints disconnected | | 49 |
| LST - 005 - Overall - Pass Rate % | | 99.981 |
| LST - 007 - Transaction - Pass Rate % | | 99.958 |
| LST - 009 - Request/Response - Pass Rate % | | 100.000 |

224636

## ACE Traffic Statistics

*Figure 16 ACE Traffic Statistics*




224637

```
ACE1-DC2/ocs# sh rserver

 rserver              : OCS1, type: HOST
 state                : OPERATIONAL (verified by arp response)
 ---------------------------------
                                                    ----------connections-----------
      real                  weight state        current    total
   ---+--------------------+------+------------+----------+--------------------
   serverfarm: EEPOOL
       10.1.100.20:0         8      OPERATIONAL  10903      11305

 rserver              : OCS2, type: HOST
 state                : OPERATIONAL (verified by arp response)
 ---------------------------------
                                                    ----------connections-----------
      real                  weight state        current    total
   ---+--------------------+------+------------+----------+--------------------
   serverfarm: EEPOOL
       10.1.100.21:0         8      OPERATIONAL  11016      11262


ACE1-DC2/ocs# sh service-policy

Policy-map : OCS-POLICY-MAP
Status     : ACTIVE
----------------------------------------
Interface: vlan 105 110
  service-policy: OCS-POLICY-MAP
    class: EEPOOL-VIP
      loadbalance:
        L7 loadbalance policy: EEPOOL-LB-POLICY
        VIP Route Metric     : 77
        VIP Route Advertise  : DISABLED
        VIP ICMP Reply       : ENABLED
        VIP State: INSERVICE
        curr conns       : 21857     , hit count        : 22669
        dropped conns    : 0
        client pkt count : 32171     , client byte count: 14188155
        server pkt count : 28948     , server byte count: 15979115
        conn-rate-limit      : -         , drop-count : -
        bandwidth-rate-limit : -         , drop-count : -
        Parameter-map(s):
          TCP_IDLE_30min
    class: REAL_SERVERS
      nat:
        nat dynamic 1 vlan 110
        curr conns       : 24        , hit count        : 320
        dropped conns    : 0
        client pkt count : 37134     , client byte count: 16433730
        server pkt count : 28092     , server byte count: 3416107
        conn-rate-limit      : 0         , drop-count : 0

DC2-Agg1#sh svclc mod 4 traffic
ACE module 4:

Specified interface is up line protocol is up (connected)
  Hardware is C6k 10000Mb 802.3, address is 0007.0e0f.2138 (bia 0007.0e0f.2138)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 10Gb/s
  input flow-control is on, output flow-control is unsupported
  Last input never, output never, output hang never
```

```
Last clearing of "show interface" counters 1w4d
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 44933000 bits/sec, 10739 packets/sec
5 minute output rate 45064000 bits/sec, 10798 packets/sec
   44343618 packets input, 21959641830 bytes, 0 no buffer
   Received 3020631 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 input packets with dribble condition detected
   43469636 packets output, 13475563786 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
```

## Server SNMP Statistics

*Figure 17 Top CPU Utilization*

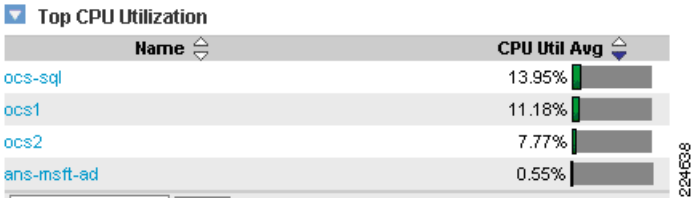
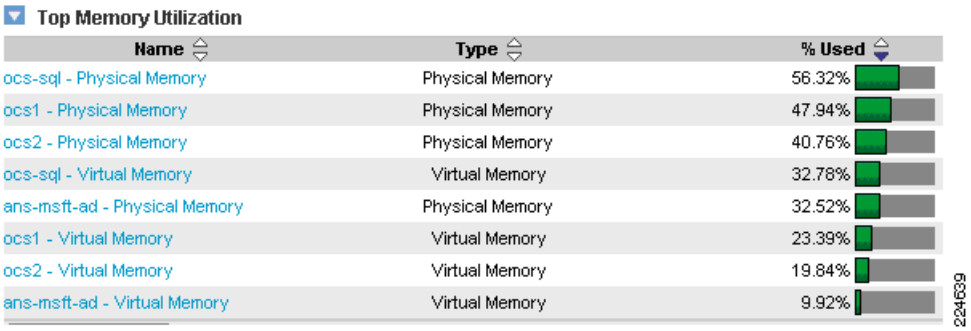



*Figure 18 Top Memory Utilization*




# Device Configurations

## Firewall Services Module—Admin Context

```
FWSM-A# sh run
: Saved
:
FWSM Version 3.1(6) <system>
!
resource acl-partition 12
```

```
hostname FWSM-A
enable password 8Ry2YjIyt7RRXU24 encrypted
!
interface Vlan100
!
interface Vlan105
!
interface Vlan197
!
interface Vlan501
 description LAN Failover Interface
!
interface Vlan502
 description STATE Failover Interface
!
passwd 2KFQnbNIdI.2KYOU encrypted
class default
  limit-resource IPSec 5
  limit-resource Mac-addresses 65535
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource All 0
!

ftp mode passive
pager lines 24
failover
failover lan unit primary
failover lan interface failover Vlan501
failover polltime unit msec 500 holdtime 3
failover polltime interface 3
failover replication http
failover link state Vlan502
failover interface ip failover 192.168.51.1 255.255.255.0 standby 192.168.51.2
failover interface ip state 192.168.52.1 255.255.255.0 standby 192.168.52.2
failover group 1
  preempt
no asdm history enable
arp timeout 14400
console timeout 60

admin-context admin
context admin
  allocate-interface Vlan197
  config-url disk:/admin.cfg
  join-failover-group 1
!

context ocs
  allocate-interface Vlan100
  allocate-interface Vlan105
  config-url disk:/ocs.cfg
  join-failover-group 1
!

prompt hostname context
Cryptochecksum:7f11b8ef15f93a82df4591e34d3f13db
: end
```

# Firewall Services Module—Office Communications Server 2007 Context

```
FWSM-A/ocs# sh run
: Saved
:
FWSM Version 3.1(6) <context>
!
firewall transparent
hostname ocs
names
!
interface Vlan100
 nameif outside
 bridge-group 1
 security-level 0
!
interface Vlan105
 nameif inside
 bridge-group 1
 security-level 100
!
interface BVI1
 ip address 10.1.100.7 255.255.255.0 standby 10.1.100.8
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list BPDU ethertype permit bpdu
access-list outside extended permit ip any any log
access-list inside extended permit ip any any log
access-list OCS-Traffic-Inbound extended permit tcp any host 10.1.100.6 eq 5061
access-list OCS-Traffic-Inbound extended permit tcp any host 10.1.100.6 eq https
access-list OCS-Traffic-Inbound extended permit tcp any host 10.1.100.6 eq 444
access-list OCS-Traffic-Inbound extended permit tcp any 10.1.100.0 255.255.255.0 eq 8057
access-list OCS-Traffic-Inbound extended permit udp any 10.1.100.0 255.255.255.0 range
49152 65535
access-list OCS-Traffic-Inbound extended permit udp any 10.1.100.0 255.255.255.0 eq snmp
access-list OCS-Traffic-Inbound extended permit udp any 10.1.100.0 255.255.255.0 eq 135
access-list OCS-Traffic-Inbound extended permit udp any eq domain 10.1.100.0 255.255.255.0
access-list OCS-Traffic-Inbound extended permit tcp any eq ldap 10.1.100.0 255.255.255.0
access-list OCS-Traffic-Inbound extended permit udp any eq kerberos 10.1.100.0
255.255.255.0
access-list OCS-Traffic-Inbound extended permit udp any eq netbios-ns 10.1.100.0
255.255.255.0
access-list OCS-Traffic-Inbound extended deny ip any any
pager lines 24
logging enable
logging timestamp
logging console informational
logging buffered informational
logging device-id hostname
logging host outside 10.1.50.10
mtu outside 1500
mtu inside 1500
monitor-interface outside
monitor-interface inside
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400
access-group BPDU in interface outside
access-group OCS-Traffic-Inbound in interface outside
access-group BPDU in interface inside
access-group inside in interface inside
route outside 0.0.0.0 0.0.0.0 10.1.100.1 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 60
ssh timeout 60
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect smtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
Cryptochecksum:66f9e6027f130fdd69ade37d5d3778af
: end
```

# ACE Configuration—Admin Context

```
ACE1-DC2/Admin# sh run
Generating configuration....

login timeout 60
hostname ACE1-DC2
boot system image:c6ace-t1k9-mz.A2_1.bin

resource-class Gold
  limit-resource all minimum 10.00 maximum unlimited
  limit-resource conc-connections minimum 10.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited

access-list ANYONE line 10 extended permit ip any any
access-list ANYONE line 20 extended permit icmp any any

class-map type management match-any REMOTE-ACCESS
  description remote access traffic match rule
  10 match protocol telnet any
  20 match protocol ssh any
  30 match protocol icmp any
  31 match protocol https any
  32 match protocol snmp any

policy-map type management first-match REMOTE-MGT
  class REMOTE-ACCESS
```

```
    permit

interface vlan 197
  description To Admin Interface - Lab Management Network
  ip address 172.28.197.15 255.255.255.0
  peer ip address 172.28.197.16 255.255.255.0
  access-group input ANYONE
  service-policy input REMOTE-MGT
  no shutdown

ft interface vlan 500
  ip address 192.168.50.1 255.255.255.252
  peer ip address 192.168.50.2 255.255.255.252
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 500

ft group 1
  peer 1
  no preempt
  priority 200
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 172.28.197.1

context ocs
  description MS Office Communications Server 2007 Testing
  allocate-interface vlan 105-110
  allocate-interface vlan 197
  member Gold

ft group 2
  peer 1
  no preempt
  priority 200
  associate-context ocs
  inservice

ssh key rsa 1024 force

ACE1-DC2/Admin#
```

# ACE Configuration—Office Communications Server 2007 Context

```
ACE1-DC2/ocs# sh run
Generating configuration....


logging enable
logging buffered 7


access-list BPDU-Allow ethertype permit bpdu

access-list ANYONE line 10 extended permit ip any any
access-list ANYONE line 20 extended permit icmp any any
access-list OCS-Traffic-Inbound line 8 extended permit tcp any host 10.1.100.6 eq 5061
access-list OCS-Traffic-Inbound line 16 extended permit tcp any host 10.1.100.6 eq https
```

```
access-list OCS-Traffic-Inbound line 24 extended permit tcp any host 10.1.100.6 eq 444
access-list OCS-Traffic-Inbound line 32 extended permit tcp any 10.1.100.0 255.255.255.0
eq 8057
access-list OCS-Traffic-Inbound line 40 extended permit udp any 10.1.100.0 255.255.255.0
gt 49151
access-list OCS-Traffic-Inbound line 48 extended permit udp any 10.1.100.0 255.255.255.0
eq snmp
access-list OCS-Traffic-Inbound line 56 extended permit udp any 10.1.100.0 255.255.255.0
eq 135
access-list OCS-Traffic-Inbound line 64 extended permit udp any eq domain 10.1.100.0
255.255.255.0
access-list OCS-Traffic-Inbound line 72 extended permit tcp any eq ldap 10.1.100.0
255.255.255.0
access-list OCS-Traffic-Inbound line 80 extended permit udp any eq kerberos 10.1.100.0
255.255.255.0
access-list OCS-Traffic-Inbound line 88 extended permit udp any eq netbios-ns 10.1.100.0
255.255.255.0
access-list OCS-Traffic-Inbound line 128 extended deny ip any any
access-list OCS-Traffic-Outbound line 8 extended permit ip any any


probe icmp PING
  interval 2
  passdetect interval 2
  passdetect count 1
probe tcp SIP-TLS
  port 5061
  interval 10
  passdetect interval 2
  passdetect count 1


parameter-map type connection TCP_IDLE_30min
  set timeout inactivity 1800

rserver host OCS1
  description Front End Server 1
  ip address 10.1.100.20
  inservice
rserver host OCS2
  description Front End Server 2
  ip address 10.1.100.21
  inservice

serverfarm host EEPOOL
  predictor leastconns
  probe PING
  probe SIP-TLS
  rserver OCS1
    inservice
  rserver OCS2
    inservice

sticky ip-netmask 255.255.255.255 address source EEPOOLGP
  timeout 30
  replicate sticky
  serverfarm EEPOOL

class-map match-any EEPOOL-VIP
  2 match virtual-address 10.1.100.6 any
class-map match-all REAL_SERVERS
  2 match source-address 10.1.100.0 255.255.255.0
class-map type management match-any remote-mgt
  201 match protocol snmp any
```

```
  202 match protocol http any
  203 match protocol https any
  204 match protocol icmp any
  205 match protocol ssh any
  206 match protocol telnet any

policy-map type management first-match remote-mgt
  class remote-mgt
    permit

policy-map type loadbalance first-match EEPOOL-LB-POLICY
  class class-default
    sticky-serverfarm EEPOOLGP

policy-map multi-match OCS-POLICY-MAP
  class EEPOOL-VIP
    loadbalance vip inservice
    loadbalance policy EEPOOL-LB-POLICY
    loadbalance vip icmp-reply
    connection advanced-options TCP_IDLE_30min
  class REAL_SERVERS
    nat dynamic 1 vlan 110

interface vlan 105
  description Client-side-vlan
  bridge-group 1
  access-group input BPDU-Allow
  access-group input OCS-Traffic-Inbound
  service-policy input remote-mgt
  service-policy input OCS-POLICY-MAP
  no shutdown
interface vlan 110
  description Server-side-vlan
  bridge-group 1
  access-group input BPDU-Allow
  access-group input OCS-Traffic-Outbound
  nat-pool 1 10.1.100.200 10.1.100.200 netmask 255.255.255.0 pat
  service-policy input OCS-POLICY-MAP
  no shutdown
interface vlan 197
  ip address 172.28.197.17 255.255.255.0
  alias 172.28.197.19 255.255.255.0
  peer ip address 172.28.197.18 255.255.255.0
  access-group input ANYONE
  service-policy input remote-mgt
  no shutdown

interface bvi 1
  ip address 10.1.100.4 255.255.255.0
  peer ip address 10.1.100.5 255.255.255.0
  description OCS-Bridged-vlans
  no shutdown

ip route 0.0.0.0 0.0.0.0 172.28.197.1
ip route 10.1.0.0 255.255.0.0 10.1.100.1
```

# Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)