



WebMux™

Local IP Load Balancing / Traffic Management Appliance

Planning and Deployment Guide for Microsoft® Office Communication Server 2007

Version 1.0

Published November 12, 2007

Copyright

Copyright © 2007 CAI Networks, Inc. All Rights Reserved.

The information contained in this document is the property of CAI Networks, Inc. Neither receipt nor possession hereof confers or transfers any right to reproduce or disclose any part of the contents hereof, without the prior written consent of CAI Networks, Inc. No patent liability is assumed, however, with respect to the use of the information contained herein.

Trademarks

WebMux and MAP are trademarks of CAI Networks, Inc.

Microsoft and Microsoft SQL Server are trademarks of the Microsoft group of companies.

All other product names and logos are trade or service marks of their respective companies.

Disclaimer

The instructions and descriptions contained in this manual were accurate at the time of writing. However, succeeding products and manuals are subject to change without notice. Therefore, CAI Networks, Inc. assumes no liability for damages incurred directly or indirectly from errors, omissions, or discrepancies between the product and this manual.

CAI Networks, Inc.
1715 Wilshire Ave., Suite 719
Santa Ana, CA 92705

www.cainetworks.com

Table Of Contents

Table Of Contents.....	1
About this Guide.....	5
Introduction.....	5
Who This Guide is for.....	5
Terminology.....	5
Legend.....	7
WebMux as Load Balancer for Office Communications Server 2007.....	9
The need for WebMux.....	9
Introducing WebMux.....	9
WebMux Benefits.....	10
Performance and Scalability.....	10
Availability and Reliability.....	10
WebMux Concepts.....	11
Overview.....	11
Functional View.....	12
Physical and Logical Views.....	13
Network View.....	13
Ports.....	18
Farm Configurations.....	19
Static Routes.....	19
Office Communications Server 2007 requirement for WebMux.....	20
Load Balancing and Traffic Management.....	22
Port Affinity / MAP Capability.....	23
SSL/TLS Offloading.....	24
Deploying WebMux with Office Communications Server 2007.....	26
Introduction.....	26
Load Balancer Use in Office Communications Server 2007 Configurations and Topologies.....	26
WebMux Requirement for Office Communications Server 2007 Deployments.....	27
Standard and Enterprise Edition.....	27
Standard Edition.....	28
Enterprise Edition Consolidated Configuration.....	28
Enterprise Edition Expanded Configuration.....	30

Web Components Servers	32
Array of Directors (Array of Standard Edition Servers as a Director).....	32
Edge Topologies	34
Scaled Single-Site Edge Topology	34
Multiple Site with a Remote Site Edge Topology	36
Multiple Site with a Scaled Remote Site Edge Topology.....	38
ISA Servers or other Reverse Proxy Servers	41
Web Farm.....	42
Office Communicator Web Access	43
WebMux Deployment	44
WebMux Configuration	45
Sample WebMux Settings.....	46
Summary	46
Speech Server	47
WebMux Deployment	47
WebMux Configuration	47
Sample WebMux Settings.....	48
Summary	48
Other Office Communications Server 2007 Modules.....	49
Reference Office Communications Server 2007/WebMux Topologies	50
Local Site Deployment.....	50
Remote Site Deployment	52
Scoping WebMux Requirements for Office Communications Server 2007 Deployments	55
Introduction.....	55
Office Communications Server 2007 Load Balancer Requirements	55
Number of WebMuxes Required.....	57
Single Versus Paired WebMux Configuration	58
Determining How Many WebMuxes You Need	58
Choosing Which WebMux Models to Use	63
Installing and Configuring WebMux for Deployment with Office Communications Server 2007	65
Introduction.....	65
Preparing for WebMux Deployment.....	65
Ensure Availability of WebMuxes	66
Ensure Availability and Configuration of Companion Equipment	66
Ensure Sufficient Electrical or UPS Outlets and Capacity	67
Set Office Communications Server 2007 Settings for WebMux.....	67
Determine Labels (optional)	67
Determine Networking Mode (Dispatch Method).....	67
Determine Scheduling Methods	68
Determine VIPs and IP Addresses.....	69
Determine FQDNs	70
Confirm Port Assignments.....	70
Decide on Attack Protection	70

Setting up the Infrastructure for WebMux Deployment	70
Set Server Network Addressing.....	70
Farm Network Addressing.....	71
Set DNS or Hosts File Configurations	71
Set Firewall Rules.....	71
Installing WebMux	71
Rackmount WebMux(es)	72
Connect WebMux(es).....	72
Set WebMux Network Addressing.....	73
Check WebMux Firmware Revision.....	73
Configuring WebMux	73
WebMux Management Console	74
Log into WebMux via the Management Console.....	74
Set WebMux Basic Settings.....	75
Set WebMux Administration Settings.....	75
Enable Attack Protection.....	76
Add Existing or Generate New SSL/TLS Certificates	76
Add Farms.....	77
Add MAP Rules.....	78
Add Servers.....	79
Adjust Service-Level Idle Timeout	80
Step-by-Step Setup	81
WebMux Settings for Office Communications Server 2007 Configurations 95	
Introduction.....	95
Sample WebMux Settings.....	95
WebMux-Level Settings	95
Farm Service-Level Settings.....	97
Farm Configurations.....	97
Ports and Services.....	101
Scheduling Methods	103
Sample Configuration Settings for Internal Network WebMuxes 105	
Introduction.....	105
Enterprise Edition Configurations.....	105
Sample WebMux configuration settings for Enterprise Edition Consolidated and Expanded Configurations	105
Web Components Servers (Enterprise Edition Expanded Configuration)	107
Sample WebMux Settings for Web Components Servers	107
Array of Directors (Array of Standard Edition Servers as a Director).....	108
Sample WebMux Settings for an Array of Directors	108
Sample Configuration Settings for Perimeter Network WebMuxes 111	
Introduction.....	111
Scaled Single-Site Edge Topology.....	111
Sample Inner Perimeter WebMux Settings for Scaled Single-Site Edge Topology	111

Multiple Site with a Remote Site Edge Topology.....	118
Sample WebMux Settings for Multiple Site with a Remote Site Edge Topology (Data Center location).....	118
Multiple Site with a Scaled Remote Site Edge Topology.....	126
Sample WebMux Settings for Multiple Site with a Scaled Remote Site Edge Topology (Data Center location).....	126
Sample WebMux Settings for Multiple Site with a Scaled Remote Site Edge Topology (Remote Site Location)	133
ISA Servers or other Reverse Proxy Servers	138
Sample WebMux Settings for ISA Servers or other Reverse Proxy Servers	138
External Web Farm.....	139
Sample WebMux Settings for an External Web Farm.....	139
Deploying WebMux with Microsoft Office Communicator Web Access (2007 release).....	141
Introduction.....	141
Sample WebMux configuration settings for Communicator Web Access pool.....	141
ISA Servers or other Reverse Proxy Servers	144
Sample WebMux Settings for ISA Servers or other Reverse Proxy Servers	145
Deploying WebMux with Microsoft Office Communications Server 2007 Speech Server.....	147
Introduction.....	147
Sample WebMux configuration settings for Speech Servers	147
Sample WebMux configuration settings for Speech Server Web farm	148
FAQs.....	151
Glossary.....	153
Index.....	165

About this Guide

Introduction

This guide discusses CAI Networks' WebMux™ product in conjunction with Microsoft® Office Communications Server 2007. It:

- Presents WebMux concepts, functionality, and benefits as they relate to Office Communications Server 2007
- Describes how to deploy WebMux in an Office Communications Server 2007 environment, including Communicator Web Access and Speech Server
- Give sample configuration settings for various Office Communications Server 2007 components and modules

This guide attempts to consolidate what you need to know about load balancing Office Communications Server 2007 with WebMux into one document, although in some cases you may need to refer to the Office Communications Server 2007 documentation or WebMux manual.

This guide focuses on load-balancing and traffic-management of Office Communications Server 2007 and presents WebMux concepts from an Office Communications Server 2007 perspective, while bridging some differences between Office Communications Server 2007 and WebMux terminology.

Who This Guide is for

This guide is intended for those who are interested in or have decided to deploy Office Communications Server 2007, and specifically those who intended to or are deploying an Office Communications Server 2007 configuration or topology that requires a "hardware load balancer".

This guide assumes a functional understanding of Office Communications Server 2007 and networking in general. It assumes no knowledge of load balancing or WebMux.

Terminology

This guide assumes you are familiar with Office Communications Server 2007 terminology; where there is conflict or confusion with WebMux terminology, this guide will provide explanations.

As with any product, Office Communications Server 2007 and WebMux have their own terminology, and the two products' terminology for the same thing is not always the

same. Office Communications Server 2007 uses generic terminology in referring to load balancers, and so there are some gaps with some WebMux terminology.

This section will quickly review key terms and try to clear up differences between Office Communications Server 2007 and WebMux terminology.

WebMux terminology is introduced in the succeeding chapters, and a complete glossary can be found in Appendix G that defines Office Communications Server 2007 and WebMux terminology relevant to this guide.

“WebMux”. This is the name of CAI Networks’ load balancer / traffic manager appliance product, and also used to refer to a unit of the product. WebMux can be deployed in a solo configuration (one WebMux) or dual configuration (two WebMuxes in a fault-tolerant configuration). A single WebMux configuration is referred to as *solo WebMux*; a configuration involving two WebMuxes is called *dual WebMux*.

“hardware load balancer”. This is the generic term used by Office Communicator Server 2007 for hardware-based network appliances like WebMux that perform load balancing of multiple servers hosting the same content. Office Communications Server 2007 uses this term to differentiate such load balancers from software-based load balancers like Microsoft WLBS/NLB, which is not supported for Office Communications Server 2007.

“internal load balancer” and “external load balancer”. Office Communications Server 2007 calls for two load balancers for the Edge servers in the perimeter network: one between the Edge servers and the inner firewall (the firewall that isolates the DMZ from the internal network) and one next to the outer firewall (the firewall that isolates the DMZ from the external network/Internet). Office Communications Server 2007 refers to the inner load balancer as the “internal load balancer” and the other as the “external load balancer”. To avoid confusion between load balancers in the internal versus perimeter network, we use the terms *inner perimeter WebMux* and *outer perimeter WebMux* for the WebMux load balancers in the perimeter network.

“internal interface”, “external interface”, and “public interface”. Office Communications Server 2007 refers to Edge Servers that have a different internal and external interface as having both an internal interface and external, or public, interface. The internal interface is used for traffic from the internal network and the external interface is for traffic from the external network (the Internet or a remote Office Communications Server 2007 deployment). These interfaces correlate in a WebMux framework to the inner perimeter WebMux and outer perimeter WebMux (specifically, as will be explained later, to the VIP of the WebMux farm in the inner perimeter WebMux or outer perimeter WebMux of which the particular Edge servers are members).

“array”, “pool”, and “farm”. Office Communications Server 2007 refers to a group of its servers that are logically related as a “pool” except in the case of web servers, where it also uses the term “Web farm” or “webfarm”. Office Communications Server 2007 and its modules also use the terms “array” and “farm” to refer to multiple identical servers. WebMux uses the term *farm* to refer to a group of servers that are logically grouped together for load balancing and traffic management purposes.

“server” and “Server”. Office Communications Server 2007 has software components called *servers* (sometimes capitalized) which are installed on computers that are also

referred to as *servers* (sometimes capitalized). This can be confusing, for example, in the case of some Edge Server topologies where the multiple server roles are both installed (*collocated*) on the same server computer. For WebMux, we refer to any load balanced computer as a *server*. For cases in which it could be ambiguous whether as to whether we are referring to server software, a server role, or a server computer we add words or explanations to clarify.

“virtual server”. WebMux refers to each group of multiple servers having the same content that are members of a WebMux farm, such as Front End Servers and Edge Servers having the same role, as a *virtual server*. Collocated servers in Office Communications Server 2007, such as the collocated Access Edge Server / Web Conferencing Edge Server computers, comprise two virtual servers (one for the Access Edge Server role and one for the Web Conferencing Edge Server role), where each virtual server can be physically represented by one or more computers that hosts software for that role. Each such virtual server can have its own virtual IP address (VIP), which in Office Communications Server 2007 is typically resolved via an A record (address record) configured in a DNS server but which can also be resolved via a hosts file entry.

“Reverse Proxy Server”, “ISA Server”. Office Communications Server 2007 uses HTTP Reverse Proxy Servers, one such model of which is Microsoft Internet Security and Acceleration (ISA) Server 2006. We refer to *ISA Server or other Reverse Proxy Server* to mean an HTTP Reverse Proxy server, which could be ISA Server or some other make.

“protocol” versus “service”. Office Communications Server 2007 uses the term “protocol” to refer to various software protocols (like HTTP and SIP) while we describe these as *services*. We use the term *protocol* to refer to transport protocols like TCP and UDP.

“TCP-level affinity” versus “connection persistence”. In some configurations, Office Communications Server 2007 requires that transactions related to a connection use the same server computer within a farm, rather than being allocated to another server as part of an agnostic load balancing scheme. WebMux calls its ability to direct an active connection’s traffic to the same server as *connection persistence*.

“Local”, “remote”, “central”, sites/locations and “data center”. Office Communications Server 2007 can be deployed in multiple locations which act as federated peers. A location or site with Office Communications Server 2007 deployed is not necessarily local or remote except from your perspective. A centralized Office Communications Server 2007 deployment with remote satellite deployments could be thought of as a hub-and-spoke topology with a central site, but Office Communications Server 2007 is not inherently a hub-and-spoke architecture. In this guide, we use the terms *local* and *remote* in the same way as the Office Communications Server 2007 documentation, which in some cases also distinguishes between *local* and *remote* sites or locations as “data center” and “remote”.

Legend

The information in this guide is based on the following manuals:

- CAI Networks WebMux 8.3.00 manual

- Microsoft® Office Communications Server 2007 Administration Guide, July 2007
- Microsoft® Office Communications Server 2007 Edge Server Deployment Guide, October 2007
- Microsoft® Office Communications Server 2007 Enterprise Edition Deployment Guide, October 2007
- Microsoft® Office Communications Server 2007 Planning Guide, July 2007
- Microsoft® Office Communications Server 2007 Technical Overview, July 2007
- Microsoft® Office Communications Server 2007 Technical Reference, October 2007
- Microsoft® Office Communicator Web Access (2007 release) Planning and Deployment Guide, July 2007
- Microsoft® Office Communications Server 2007 Speech Server documentation (on MSDN), 2007
- Load Balancing Microsoft® Speech Server 2004 Enterprise Edition White Paper, August 2004

WebMux as Load Balancer for Office Communications Server 2007

The need for WebMux

Office Communications Server 2007 offers selected configurations and deployment models to serve customers with demanding requirements for these benefits. Most Office Communications Server 2007 configurations can deploy multiple servers to perform the same role, thereby increasing performance and ensuring that should one server fail another can take over.

Office Communications Server 2007 and WebMux work together to deliver these benefits, within WebMux's framework of ease of use and a set-it-and-forget-it management and operational approach.

Introducing WebMux

WebMux is a server load balancing and traffic management network appliance that is an integral component in a high performance, high availability network architecture.

WebMux allows multiple servers to be deployed for any given server in a network, effectively multiplying its power and capacity. This not only increases performance and scalability, it provides redundancy: in case any server fails – either the server itself or a critical protocol running on the server – it is automatically taken out of service, and other servers automatically take up the work.

WebMux sits between the network clients and servers, or between servers and servers, with all traffic passing through it. WebMux load balances and manages the traffic to the servers best able to handle the work. At the same time, WebMux regularly health checks all configured protocols to determine servers which are unable to handle traffic, and automatically takes unhealthy servers out of service while diverting traffic to healthy servers.

WebMux is a conceptually simple but technologically advanced product that incorporates key networking functionality into a rack-mountable 1U form factor appliance, including Layer 2 through 7 load balancing and traffic management, SSL acceleration, DoS and DDoS attack protection.

WebMux Benefits

Using WebMux with two or more servers as an alternative to a single server provides multiple benefits:

- Performance
- Scalability
- Availability
- Reliability

Performance and Scalability

WebMux achieves both performance and scalability by combining the power of multiple servers performing a given role to create a larger, more powerful virtual server.

Additional servers can be added to increase performance, thereby allowing the solution to scale simply by adding more servers.

SSL/TLS Offloading

Additional performance enhancement can be achieved for certain Office Communications Server 2007 modules by offloading the processor-intensive task of SS/TLS encryption and decryption from Office Communications Server 2007 servers to WebMux.

Depending upon the WebMux model and options ordered, SSL/TLS acceleration can be performed in software or on a dedicated card. (Refer to Table 7 for more information about WebMux models and accessories and the SSL/TLS acceleration capabilities they offer.)

Availability and Reliability

Availability and reliability go hand in hand, since an unreliable solution that goes down has zero availability.

Preventing Unplanned Downtime

WebMux ensures availability via redundancy: both of networked servers and WebMux itself. Should any server be unable to do its job (either because it crashed, or a port or protocol failed), WebMux's comprehensive health checking will detect this and automatically take the dysfunctional server out of service, spreading the workload across the remaining operational servers. Once the failed server is again operational and online, WebMux automatically puts it back into service.

WebMux can be implemented in a redundant active/standby configuration, where a regular bi-directional heartbeat and health checking by the paired WebMuxes determine the other's health. Should the primary WebMux fail, the standby WebMux is automatically put into service, adopting the personality (IP address, etc.) of the primary WebMux.

Operations staff can be notified of failures in real time, and full SNMP logging is provided.

Accommodating Planned Downtime

WebMux's ability to dynamically put servers in and out of service in the event of failure can also be used to take servers offline to perform backups, maintenance, and upgrades. WebMux permits a server to be *quiesced*, whereupon its current connections are permitted to continue but new connections are diverted. Once all current connections have "drained off" the server can be removed from service.

WebMux Concepts

This section covers the main WebMux concepts that you will need to know to successfully deploy it, particularly in an Office Communications Server 2007 environment.

Overview

It is useful to think of WebMux as an unobtrusive black box that load balances and manages traffic to multiple groups of servers, where each group has two or more servers with identical capabilities and content.

For each group of content-alike servers, WebMux presents a *virtual server* to the network, such that the network, the devices on it, and the clients that access it are none the wiser that they are not talking to a single computer. Each virtual server has a virtual IP address (VIP), which can be resolved by via DNS or hosts file. In the case of Office Communications Server 2007, FQDNs are created for the VIPs of the virtual servers and generally resolved by A records configured in DNS.

A single WebMux can manage multiple groups of such like servers (for example a group of web servers and another of FTP servers) and present multiple virtual servers, one for each group. WebMux calls each such logical group of like computers a *farm*. WebMux calls the computers that are members of the farms *servers*.

Each farm is logically comprised of servers that host common data, use the same ports, and could essentially be a single server if not for the desire to meet objectives for performance, scalability, availability, and reliability.

Access to servers via WebMux leaves the allocation of traffic to WebMux's load balancing and traffic management capabilities, with WebMux automatically selecting the best server to service each transaction. Traffic can alternatively be directed to a particular server in a WebMux farm, without going through WebMux, via the server's IP address (instead of the farm's VIP).

To recap these concepts:

- *WebMux* is a network appliance that routes traffic to servers.
- *A farm* is a logical grouping of servers that share common content and ports.

- A *server* is a computer that is a member of one or more farms (and which can also exchange traffic outside of WebMux.)

We will now take a closer look at these concepts from three perspectives: a functional view, a physical view, and a network view.

Functional View

The following is a deeper relationship of farms and servers and how they interrelate with each other and with WebMux.

Farms

Farms serve the purpose of logically grouping servers that can all handle certain traffic. Such groupings are defined by a server's membership in a farm. A server can belong to multiple farms, provided that it is able to serve transactions for all the farms to which it belongs.

(There is also in WebMux the concept of a sub-farm, in which certain servers but not others within the farm can handle certain transactions, but this will not be covered in this guide since the requirement for that does not exist in Office Communications Server 2007.)

Farms define the criteria for load balancing and traffic management within the farm, which ports are used, health checking criteria, and, if SSL/TLS termination is being performed by WebMux for servers in the farm.

Each farm generally has a unique IP address on the network, which is a virtual IP address (VIP). Traffic destined for servers in the farm is addressed to the farm's VIP. It is also permitted to assign the same VIP to multiple farms, but if so the port(s) used for each farm be unique (otherwise, WebMux would not be able to determine which farm to route traffic to).

Farms-to-server relationship

Since any traffic received for a farm must be able to be serviced by any server in the farm (except in the case where subfarms are used), servers within a farm must meet the following criteria:

- They must all have the same content as other servers in the farm. Some servers can have additional content than and unique to other servers, but they must all have the content necessary to handle any traffic that may be directed to them by WebMux by virtue of their membership in a farm
- They must all use the same ports for receiving traffic sent by WebMux and have the same protocols running on those ports

There is no requirement that servers have identical power. WebMux is capable of evenly balancing the load between servers of varying configurations.

WebMux-to-server relationship

The functional relationship between WebMux and the servers for which it manages traffic and load balances is threefold:

- WebMux will route traffic to servers that it determines are best qualified to handle it, based on the configured *scheduling method* for the farm. WebMux's scheduling methods include those that enforce *persistent* connections, whereby transactions related to the same active connections resolve to the same server – a requirement for certain Office Communications Server 2007 components.
- WebMux will monitor the health of specified protocols on each server, based on which protocols have been configured for the farm, and on default or customized health-checking criteria.
- WebMux will stop routing traffic to servers that either it has determined are incapable of handling it, or for which it has been explicitly told to take out of service.

Physical and Logical Views

WebMux is a physical network appliance and servers are physical computers.

Farms are an abstraction of the servers that WebMux manages, and exist to define which servers can handle certain traffic and impose criteria on how traffic among servers that are members of the farm is managed.

Despite the fact that farms are not physical entities, they are the embodiment of the virtual servers presented by WebMux: the VIP used for directing traffic to the servers that are members of a farm is a property of the farm.

Network View

WebMux is connected as a device on the network, and has its own IP address and hostname. In a dual WebMux deployment, the primary and secondary Web are both connected to the network (and each other), and both have unique IP addresses and hostnames.

Networking Mode

WebMux can operate in three different *networking modes*, and it is necessary to choose one of these modes – Transparent (or Bridge mode), NAT (DNAT – Destination Network Address Translation mode), and Out-of-Path (DSR – Direct Server Return mode) – for each WebMux you are deploying in your networks. Each WebMux can only operate in only one configured networking mode.

With both Transparent and NAT mode, traffic passes through WebMux in both directions; that is, both from the network to the servers and back again. These two modes are considered “two-arm” networking modes, since both “arms” of WebMux (one arm servicing inbound traffic and the other servicing return traffic passing through WebMux) are involved.

With Out-of-Path mode, traffic passes through WebMux in one direction only: return traffic from the servers goes directly to the network. This is considered a one-arm networking mode, since only WebMux's inbound arm is used. Out-of-Path mode therefore offers substantial performance advantages to Transparent and NAT mode when there is substantial return traffic.

Microsoft recommends using a two-arm networking mode for load balancing servers in the Enterprise pool, and therefore does not support Out-of-Path mode for deploying WebMux in an Office Communications Server 2007 environment, as it prevents the Office Communications Server 2007 administration tool from being used from outside the local network.

On the other hand, certain Office Communications Server 2007 modules, like Speech Server recommend the use of Out-of-Path mode.

Special attention is required when deploying WebMuxes with mixed networking modes, as the networking mode governs the operation of each WebMux, therefore there could be limitations as to what farms can be collocated within the same WebMux.

NAT Mode

WebMux's NAT mode is an "In-Path" two-arm networking mode that locates the servers being load balanced in one network segment and performs DNAT (Destination Network Address Translation) between the main network and the segment containing the servers. As such, servers are assigned IP addresses that are not part of the main network.

In NAT mode, one of WebMux's arms is connected to the main network via a switch and to the server VLAN via another switch. The main network switch is connected to WebMux's Router LAN port and to the server switch via its Server LAN port.

Incoming network traffic enters WebMux through its Router LAN port, is NATted, and exits to the servers via its Server LAN port. Return traffic enters WebMux through its Server LAN port, is NATted, and exits via its Router LAN port.

An advantage of NAT mode is that it provides the best security for isolating servers from any other part of the network, since they reside in their own VLAN and WebMux can firewall all unconfigured ports. The disadvantage of NAT mode is that it requires that server IP addresses be changed.

Office Communications Server 2007 requires that the Front End Servers in the Enterprise pool be located in a subnet, and WebMux's NAT mode is the best for handling that. If Edge Servers are deployed in a subnet, NAT mode should be used for the WebMuxes in the perimeter network.

Transparent Mode

WebMux's Transparent mode (also called *Bridge* mode) is a two-arm mode in which servers are located on a separate network segment but their IP addresses can be the same as those in the main network. WebMux behaves as an Ethernet bridge between the two segments.

In Transparent mode, WebMux's Router LAN port is connected to a switch that is connected to the main network, and its Server LAN port is connected via a switch to the servers.

In Transparent mode, servers reside "behind" the WebMux but are effectively in the same network as the servers "in front of" the WebMux.

The advantage of Transparent mode is that servers can have external IP addresses, whereas in NAT mode they must have internal IP addresses. The disadvantage of Transparent mode is that if WebMux is deployed in a dual configuration switches and routers to which the WebMuxes are connected must support STP (Spanning Tree Protocol), which older switches that you may already have may not support. If deploying a solo WebMux (without a redundant WebMux to protect against a WebMux failure), STP-capable switches are not required.

Out-of-Path Mode

WebMux's Out-of-Path mode (also called "Direct Server Return" mode) is a one-arm mode in which servers are located in a different subnet and equipped with loopback adapters. Like Transparent mode, servers can have external IP addresses.

Using out-of-path mode can allow substantially more traffic to be handled by WebMux than two-armed networking modes because return traffic from the servers does not need to pass through WebMux, rather it goes directly to the network.

Out-of-Path is not supported for Office Communications Server 2007 because the Office Communications Server 2007 tool used for administrating the Enterprise Servers is unable to pass through WebMux (requiring that direct connections to the Enterprise Servers be made for administration purposes). However, some Office Communications Server 2007 modules, like Speech Server, recommend use of Out-of-Path mode for load balancing.

Table 1: **Comparison of WebMux Networking Modes for use with Office Communications Server 2007**

Mode	Advantages	Disadvantages
Transparent	Fully supported with Office Communications Server 2007	Lower performance for server return traffic compared with Out-of-Path mode, since it needs to pass through WebMux
	External server IP addresses are allowed	If WebMux is deployed in dual mode, switches must be STP-capable
		Lacks port-blocking (firewall) capability
NAT	Fully supported with Office Communications Server 2007	Lower performance for server return traffic compared with Out-of-Path mode, since it needs to pass through WebMux
	Provides the best security for isolating servers from any other part of the network	Server IP addresses must be internal
	Can block ports that are not configured to handle traffic	
Out-of-Path	Higher performance for server return traffic, since it does not need to pass through WebMux	Not officially supported by Office Communications Server 2007, since prevents remote access by Office Communications Server 2007 administration tool
	External server IP addresses are allowed	Requires every load-balanced server be equipped with a loopback adapter
		Lacks port-blocking (firewall) capability
		Cannot be used in combination with SSL/TLS offloading

Network Addressing

Each server has an IP address, which is used by WebMux to route traffic, and which can also be used (as well as hostname) for exchanging traffic outside of WebMux, as network

topology permits. (WebMux also supports servers that have multiple IP addresses assigned, and will route traffic to the same server via one or more IP addresses.)

Without WebMux, traffic is routed directly to a server, either by IP address or hostname (or FQDN resolved to the server’s IP address). With WebMux, traffic is instead routed to a logical *virtual server* that comprises multiple physical servers. Each virtual server exposed by WebMux each has a virtual IP address, or VIP, which is generally unique. (It is possible to have multiple farms with the same VIP, even within a single WebMux, in which case the combination of the VIP and port number for the transaction is used to target the appropriate farm).

WebMux does not hold hostnames for its farm, so to access a farm by FQDN or hostname, an A record needs to be setup in a DNS server to resolve an FQDN to a farm’s VIP, or a hosts file entry needs to resolve a hostname to a farm’s VIP.

Table 2 below shows an example of server addressing with and without WebMux. With WebMux, the servers can still be accessed individually by their IP addresses and hostnames, and collectively by VIP.

Table 2: Addressing Servers with and without WebMux

Without WebMux

Server	IP address	Hostname
Front End Server 1	10.1.0.10	FrontEnd1.corp.contoso.com
Front End Server 2	10.1.0.11	FrontEnd2.corp.contoso.com

With WebMux

Server	IP address	Hostname
All Front End Servers	10.1.0.100 (VIP)	FrontEnds.corp.contoso.com*
Front End Server 1	10.1.0.10	FrontEnd1.corp.contoso.com
Front End Server 2	10.1.0.11	FrontEnd2.corp.contoso.com

* The hostname is resolved by an A Record configured in a DNS server or hosts file entry.

Each WebMux has a IP address and hostname that is unique on the network, but they is not used to direct traffic to the servers the WebMux manages; rather the VIP of a farm configured in WebMux is used. WebMux’s IP address is used to access the WebMux for configuration purposes via WebMux’s browser-based Management Console.

In dual WebMux deployments, in which one WebMux is active (the *primary* WebMux) and the other is a hot standby (*secondary* WebMux), each WebMux has a unique IP address and hostname and both exist on the network. But in the event of failover, the secondary WebMux automatically adopts the primary’s IP address and hostname.

Server Network Addressing

Depending on whether you are deploying WebMux in NAT versus Transparent mode, you may or may not need to take special considerations when assigning IP addresses to Office Communications Server 2007 server computers.

If you are using Transparent mode, you can use whatever IP addresses you want for the Office Communications Server 2007 server computers; but if you are using NAT mode and if the Office Communications Server 2007 servers have external IP addresses assigned they will need to be reassigned with internal IP addresses. If servers are isolated in a subnet behind the WebMux, their IP addresses will need to reflect the subnet in which they reside.

Servers can also exchange traffic on their internal IP addresses, thereby bypassing WebMux's load balancing, assuming that the ports required open.

Farm Network Addressing

Each WebMux farm is must be assigned a virtual IP address (VIP) when it is created. Transactions can be routed to the servers that are members of a farm via the farm's VIP.

Ports

Traffic to servers that are members of WebMux farms access certain ports on the servers, and WebMux carries the traffic to the specified ports, or can reassign the traffic to other ports.

WebMux can load-balance and traffic-manage servers on multiple ports. The methods for configuring WebMux to handle traffic on one port, two ports, or more than two ports differ somewhat.

Port Assignment

When a farm is configured, it is assigned a port, which, by extension, is carried to all servers that are members of the farm. When each server that is a member of the farm is configured, a port is also assigned, which can be either the same port as is assigned for the farm or an additional port, if the server handles traffic on two ports.

In cases in which servers that are members of a farm are handling traffic on more than two ports, a *MAP rule* needs to be defined for each additional port that needs to be handled. MAP rules have the effect of not only defining additional ports for servers within a farm, they also logically bind the ports together such that if the protocol on any port configured for a server fails to respond to WebMux's health check, WebMux will consider the server inoperative and failover to a healthy server within the farm.

To ease configuration of ports for farms, servers, and MAP rules, if the service assigned for a farm or MAP rule has an associated well-known port, WebMux automatically imposes that port for the port number. This port number can be overridden if desired.

Port Number

Farms and MAP rules are configured with a specific port number, or the special combined port “80/443”, which opens those two ports for HTTP and HTTPS traffic.

Servers, on the other hand, can additionally be assigned special port values that have expanded behavior. These special port values and the behavior they cause are:

same	The port assigned to the farm, all MAP rules imposed for the farm, and all servers that are members of the farm are imposed.
0	All ports are assigned, except those that are explicitly assigned with the VIP of the current farm (to other servers or MAP rules within the current farm, or in other farms having the same VIP). “0” should be used when ranges of ports need to be load-balanced and traffic-managed.

Effect of MAP

If MAP rules are configured for a farm, their port numbers are assigned to all servers that are members of the farm.

Port Blocking

In NAT mode, WebMux will by default block inbound traffic on all ports to servers that are members of a farm that are not specifically configured for the farm. In Transparent and Out-of-Path mode, there is no port blocking done: all ports are open. In all networking modes, outbound traffic (from the servers to WebMux) is never blocked.

To disable WebMux’s firewall in NAT mode such that all ports are open for a farm, use the Administration Setup screen of WebMux’s browser-based Management Console to set the ‘forwarding policy’ to “Accept”.

Farm Configurations

A *farm* is a collection of computers that form a virtual server. A VIP is assigned to the farm, which becomes the collective IP address for the servers in the farm: any traffic sent to the farm’s VIP will reach the most appropriate server in the farm, based on the scheduling method configured for the farm.

Static Routes

WebMux allows you to configure a static route to a device. While this is normally not required in Office Communications Server 2007, there are some cases in which it may be required, such as for configuring Office Communications Server 2007 as a SIP peer for Speech Server.

Refer to the WebMux manual for information about configuring static routes.

Office Communications Server 2007 requirement for WebMux

Office Communications Server 2007 requires a hardware load balancer in all of its scalable, fault-tolerant configurations and topologies. Refer to Tables 4 and 5 if you are not sure about whether your intended configuration and/or topology require one or more hardware load balancers and to determine how many WebMuxes you require.

The WebMux deployed in an Office Communications Server 2007 environment is the out-of-the-box product. Office Communications Server 2007 utilizes WebMux's standard features for load balancing and traffic management.

Office Communications Server 2007 relies on four particular WebMux capabilities ensuring proper load balancing and traffic management operations in an Office Communications Server 2007 environment. They are:

- Multifarming (collocated servers)
- Connection persistence (TCP-level affinity)
- Configurable health checking (TCP timeout)
- SSL/TLS offloading (for Communicator Web Access and Speech Server)

These capabilities are key to proper support of Office Communications Server 2007 and are explained below.

Multifarming

Multifarming is the ability to assign a server to multiple farms, or, more specifically, to have a server be a member of more than one farm. While this is not normally required in WebMux deployments, it is an important feature for Office Communications Server 2007.

For some of the Office Communications Server 2007 Edge Server topologies, the Access Edge Server and Web Conferencing Server are collocated on the same computer. At least two such computers, on which both the Access Edge Server and Web Conferencing Server are installed, are deployed in a scaled configuration. A third server pair, hosting the A/V Edge Server, is part of the same topology.

For this topology, Office Communications Server 2007 requires three FQDNs: one for each software server; yet the servers are not all installed on discrete computers. What is necessary is for two logical servers to be created from the two physical servers containing the collocated Access Edge Server and Web Conferencing Server. Office Communications Server 2007 calls for the following:

- Farm A (Access Edge Server farm) has computers 1 and 2 as members
- Farm B (Web Conferencing Server farm) has computers 1 and 2 as members
- Farm C (A/V Edge Server farm) has computers 3 and 4 as members

Or, from the perspective of the computers:

- Computer 1 (Access and Web Conferencing) is a member of farms A and B
- Computer 2 (Access and Web Conferencing) is a member of farms A and B
- Computer 3 (A/V) is a member of farm C

- Computer 4 (A/V) is a member of farm C

WebMux supports this configuration by *multifarming* the computers containing the Access Edge Server and Web Conferencing Edge Server into two different farms (and the A/V Edge Server computers into its own farm). Each farm has its own VIP and, via DNS, its own FQDN.

Within this farm configuration, WebMux applies different health-checking rules to the three different farms, and only considers a server inoperative if any protocol required for a particular farm is down. This means, for example, that if a protocol on server computer 1 or 2 that is required for the Access Edge Server but not the Web Conferencing Server fails, WebMux is able to take the server out of service for the Access Edge Server farm but leave it operational for the Web Conferencing Server farm.

Multifarming Considerations

When a server is a member of more than one farm, its handling by WebMux is independent of other farms. As such, there are some considerations that need to be taken into account relating to the behavior of certain WebMux functionality which affect configuration decisions and operational practices. They are:

Effect on Scheduling Method

Scheduling method is a farm-level setting that affects the servers that are members of the farm. The information WebMux uses for load balancing and traffic management is based on each farm independently – if a server is sent traffic in one farm, that traffic is not considered in another farm’s load balancing and traffic management determinations.

Therefore, for example, the “least connections” scheduling method does not mean the actual least connections for a server but rather its least connections within a particular farm. If a server is a member of multiple farms, the number of connections it has from each of the farm’s perspectives is only the number of connections that it holds for that farm.

For Office Communications Server 2007, this is not much of an issue since the servers that belong to multiple farms have the same presence in the farms. For example, collocated Access Edge / Web Conferencing Edge servers are the exclusive members of the same farms.

Effect on Server Weight

Server *weight* reflects if traffic to that server should be skewed compared with other servers in a farm based on its power relative to other services. A server’s weight is assigned separately for each farm, regardless of its weight in other farms. If using a scheduling method that is weighted for a server that is a member of multiple farms, you can adjust its weight in each farm to cause WebMux to distribute traffic to it evenly, regardless of its membership in other farms.

For example, if you have two farms and each has a dedicated server and both contain a shared server, you can assign a weight to the dedicated servers that is double that of the shared server. This would cause the dedicated servers to be sent twice as much traffic as

the shared server, and thereby the shared server could be evenly load balanced along with the dedicated servers.

Effect on Run State

A server that has a Run State of Active in one farm and Standby in another farm will be passed traffic from the Active farm but not the Standby farm. To deactivate the server, it is necessary to put it in a Standby state in all farms to which it belongs.

Impact on Health Checking

Each farm performs its own health checking of a server based on the service defined for the server's configuration in each farm. If, for example, a server is configured with different ports and services in different farms, all those ports and services will be checked. Should a port or service fail, the farms in which the server has been configured with those ports and service will recognize this (and transactions for those farms will be diverted away from the server).

If a server is configured with the same port/service in multiple farms, it is still necessary for each farm to perform health checks so that the server can be properly be failed over in all farms should the port and/or service fail.

Impact on Server Failover

Should a server fail, the health-checking done by all farms to which it belongs will detect this and traffic for all farms will be diverted around the failed server.

Impact on Quiescing a Server

Quiescing a server in a farm will only stop transactions for that farm. To completely quiesce a server, it is necessary to quiesce it in all farms to which it belongs.

Load Balancing and Traffic Management

Load balancing and traffic management are fundamental WebMux capabilities that are employed in any implementation. For Office Communications Server 2007, some considerations need to be taken to ensure proper distribution of transactions while allowing Office Communications Server 2007 to function properly.

TCP-Level Affinity / Connection Persistence

Office Communications Server 2007 calls for TCP-level affinity when load balancing and managing traffic to the Enterprise pool and Edge Servers, which WebMux achieves by enforcing persistent connections. Office Communications Server 2007 requires for some servers that certain transactions related to a connection resolve to the same server computer, rather than being allocated to another server as part of an agnostic load balancing scheme. Such is sometimes referred to as "sticky" connections.

Persistent Scheduling Methods

WebMux is configured on a farm-by-farm basis to enforce connection persistence or not as a property of the *scheduling method* used for load balancing and traffic management. WebMux offers the following persistent algorithms:

- fastest response, persistent
- least connections, persistent
- weighted least connections, persistent
- round robin, persistent
- weighted round robin, persistent

Non-Persistent Scheduling Methods

For Office Communications Server 2007 components and modules where persistent connections are not required, WebMux offers the following load-balancing and traffic management algorithms:

- least connections
- round robin
- weighted least connections
- weighted round robin
- weighted fastest response
- Layer 7 HTTP URI load directing
- Layer 7 HTTP URI load directing with cookies

Note The Layer 7 scheduling methods above are used for content switching, where traffic routing to particular servers within a farm is dependent on cookies or URIs. This capability is not required in Office Communications Server 2007 since its servers are content agnostic.

Port Affinity / MAP Capability

WebMux takes persistence (TCP-level affinity) a necessary step further for Office Communications Server 2007 via its exclusive MAP™ (Multiple Address Port) capability. MAP creates port affinity, such that user transactions involving multiple ports can all be directed to the same computer, rather than being allocated to different servers within a farm.

So, for example, if a Front End Server receives a successful connection on port 443 and subsequent traffic is sent by the client to port 5060, the subsequent traffic will be directed to the same server as the connection, rather than other servers in the farm.

MAP logical bindings are also utilized for health-assurance purposes: a MAP-enabled farm is configured with multiple ports whose protocols must be healthy in order to consider the server healthy. If any service fails, the server is taken down.

So, for example, if a Front End Server is unable to service traffic on port 5060 and 5061 because there is a problem with the SIP protocol service but it can service traffic on port

443, the server will be taken out of service despite its ability to service traffic on other ports.

SSL/TLS Offloading

WebMux is capable of offloading SSL/TLS encryption and decryption from servers in order to unburden server processor resources, and can incorporate hardware-based SSL/TLS encryption/decryption to more effectively handle higher SSL/TLS transaction volumes. WebMux also offers streamlined SSL/TLS certificate management capabilities as part of its SSL/TLS-related functionality.

Although SSL/TLS offloading is not called for for Office Communications Server 2007's Standard or Enterprise configurations or Edge topologies, SSL/TLS offloading is documented for Communicator Web Access and Speech Server.

Offloading SSL/TLS processing from servers to WebMux has three main benefits:

- Unburdens servers from performing SSL/TLS encryption and decryption
- Accelerates SSL/TLS encryption and decryption via specialized software and, depending on the WebMux model and options, a dedicated SSL/TLS processing card
- Simplifies SSL/TLS certificate management, since certificates reside one place, rather than on multiple servers

The three components of WebMux's SSL/TLS offloading are described below.

SSL/TLS Termination

WebMux is able to terminate incoming SSL/TLS transactions, which involves decrypting the data and sending clear text to the servers, as well as re-encrypting the outbound data from the servers.

WebMux allows you to specify both the port that will receive encrypted traffic as well as the port on the servers to which clear traffic should be sent (generally 443 and 80, respectively)..

SSL/TLS Acceleration

WebMux can perform TLS acceleration so that the encryption and decryption process is done more quickly, either in software or dedicated hardware. SSL/TLS acceleration improves transaction throughput and allows more SSL/TLS transactions to be processed.

Refer to Table 7 for information about WebMux's SSL/TLS capabilities and performance by model.

SSL/TLS Certificate Management

When WebMux is used to offload SSL/TLS processing, SSL/TLS certificates reside and are managed in WebMux rather than the individual servers. This eliminates the need to have multiple identical certificates in various servers, certificates do not need to be duplicated, and it is not necessary to access multiple servers to manage them.

WebMux supports SSL V2, SSL V3, and TLS V1 with 512, 1024, and 2048 byte RSA keys. Each WebMux can accommodate up to 32 certificates, with both active and inactive or reserve keys. Existing certificates can be added into WebMux via copy and paste, or can be requested of proper authorities from within WebMux's Management Console.

Deploying WebMux with Office Communications Server 2007

Introduction

This chapter describes the various configurations and topologies in which Office Communications Server 2007 can be deployed and WebMux's inclusion in them, as well as other WebMux usage in conjunction with Office Communications Server 2007, in the following sequence:

- Standard, Consolidated, and Enterprise Edition
- Array of Standard Edition Servers as a Director (Array of Directors)
- Edge deployment including ISA Server or other Reverse Proxy Server
- Web farms
- Communicator Web Access
- Speech Server
- Other Office Communications Server 2007 modules

Load Balancer Use in Office Communications Server 2007 Configurations and Topologies

Office Communications Server 2007 requires that a hardware load balancer like WebMux be used in all its scalable, highly available, and fault-tolerant configurations and topologies, both at the local site and any remote sites at which scalable, highly available, and fault-tolerant Office Communications Server 2007 configurations and topologies are deployed.

The Office Communications Server 2007 configurations and topologies that are documented to not require a hardware load balancer are the Standard Edition Configuration and Consolidated Edge, Single-Site Edge, and Remote Site Edge Topologies. But even for these configurations and topologies, a load balancer may be required. In addition, other Office Communications Server 2007 modules, Reverse Proxy servers, and web farms can require load balancing where multiple servers are deployed.

The following paragraphs describe the requirement for load balancing for each Office Communications Server 2007 configuration, topology, and various components and modules.

WebMux Requirement for Office Communications Server 2007 Deployments

For the Office Communications Server 2007 deployments discussed in this chapter, we will be using six WebMuxes. The number of WebMuxes required for any particular deployment with Office Communications Server 2007 can vary based on various factors – refer to Chapter 4 for details on scoping WebMux for your Office Communications Server 2007 deployment.

The WebMuxes discussed in this chapter and elsewhere in this guide and their designations are in Table 3 below:

Table 3: WebMux Designators for Office Communications Server 2007 Deployments

WebMux	Functionality with Office Communications Server 2007
front end	Manages internal and external traffic to the Front End Servers for an Enterprise Edition Consolidated or Enterprise Edition Expanded Configuration
epool	Manages internal and external traffic to the Web Components Servers for the Enterprise Edition Expanded Configuration and can manage an Array of Directors and web farm for any configuration
inner perimeter	Manages internal traffic to the Edge Servers
outer perimeter	Manages external traffic to the Edge Servers and ISA Server or other Reverse Proxy Server, and web farm
Communicator Web Access	Manages internal and external traffic to Communicator Web Access servers. (Multiple ISA Servers or other Reverse Proxy Servers used for external Communicator Web Access traffic is managed by the outer perimeter WebMux.)
Speech Server	Manages internal and external traffic to the Speech Servers and, if separate Web Servers are deployed, to them as well

Standard and Enterprise Edition

WebMux can be deployed in local and remote locations with the Office Communications Server 2007 Standard Edition if Directors are used, and is required for both the Enterprise Consolidated and Expanded configurations.

Standard Edition

The Office Communications Server 2007 Standard Edition configuration consists of a single computer that hosts all Office Communications Server 2007 server roles as well as the SQL database. Because there is only one computer, there is no requirement for load balancing and there is therefore no need for WebMux.

In Office Communications Server 2007 Standard Edition deployments with significant external traffic, Microsoft recommends offloading the task of user request authentication from the Standard Edition Server to a separate computer, called a Director. A Director helps insulate the Standard Edition Server from potentially malicious traffic, while relieving it of the overhead of performing authentication, thereby improving security and performance. A Director does not host users but, as a member of an Active Directory domain, has access to Active Directory for purposes of authenticating remote users and routing traffic to the Standard Edition Server.

In the Standard Edition Configuration, a Director is a Standard Edition server that has had most of its server roles (i.e., Web Conferencing, A/V Conferencing, Web Components) and the Address Book Server deactivated.

A single or multiple Directors can be used, but with the Standard Edition Configuration it is not likely that more than one Director would be required. A Standard Edition server with a single Director does not require load balancing and therefore there is no need for WebMux. Should you want to deploy the Standard Edition Configuration with more than one Director, refer to the discussion of Array of Directors later in this chapter.

Enterprise Edition Consolidated Configuration

The Office Communications Server 2007 Enterprise Edition Consolidated Configuration consists of one or more content-identical computers that host all Office Communications Server 2007 server roles and a separate computer hosting an SQL database. (What differentiates it from the Standard Edition is that multiple computers are supported for scalability and fault tolerance, and the database is on a separate computer.)

The computer hosting the database is called the Back End Server and the computers hosting the Office Communications Server 2007 software (Focus, IM Conferencing Server, Web Conferencing Server, Telephony Conferencing Server, A/V Conferencing Server, and IIS Servers) are called Front End Servers.

The Front End Server(s) and any Director(s) that may be deployed are considered Enterprise Servers; along with the Back End Server, they comprise the Enterprise Edition Consolidated Pool. They are all deployed in the internal network at the local site, and in the internal network of each remote site at which this configuration is deployed.

In large deployments with significant external traffic, Microsoft recommends offloading the task of user request authentication from the Enterprise Pool to a separate computer, called a Director. Directors help insulate the Enterprise pool from potentially malicious traffic, while relieving it of the overhead of performing authentication, thereby improving security and performance. A Director does not host users but, as a member of an Active Directory domain, has access to Active Directory for purposes of authenticating remote

users and routing traffic to the Standard Edition Server. If a separate Director or Array of Directors is not deployed, the Enterprise Pool acts as the Director and handles external user authentication.

In the Enterprise Edition Consolidated Configuration, a Director is a Front End server that has had most of its server roles (i.e., Web Conferencing, A/V Conferencing, Web Components) and the Address Book Server deactivated. A single or multiple Directors can be used; more than one Director is called an Array of Directors and requires load balancing by WebMux.

An Enterprise Edition Consolidated Pool with a single Front End server and no Director or a single Director does not require load balancing and there is therefore no need for WebMux. But in the Enterprise Edition Consolidated Configuration there is normally more than one Front End Server and therefore WebMux is normally required.

Note The Back End Server is not load balanced by WebMux, rather a Microsoft SQL Server cluster can optionally be used for the back-end database to provide additional high availability and failover capabilities.

WebMux Deployment

For load balancing by WebMux, the Front End Servers are isolated in their own distinct subnet in the internal network. If Directors are deployed, they are located outside of this distinct subnet.

A solo or dual WebMux configuration is deployed to manage the Front End Servers in the internal network at the local site, and in the internal network of each remote site at which this configuration is deployed. We refer to this WebMux as the *front end WebMux*.

If the Enterprise Edition Consolidated Edition is being deployed with an Array of Directors, a second solo or dual WebMux is deployed to manage the Director servers. We refer to this WebMux as the *epool WebMux*. Refer to the discussion of Array of Directors below for information.

WebMux Configuration

The front end WebMux is configured with one farm, which contains the Front End Server computers. This farm functions as a virtual server and is assigned a VIP, which is resolved by an externally-configured FQDN. The load-balanced servers behind the WebMux can still be addressed by their assigned IP addresses.

The front end WebMux is configured to use NAT mode as its networking mode. The epool WebMux can use NAT or Transparent mode.

WebMux is configured to use a scheduling method for each farm that enforces persistent connections in managing traffic to the servers in order to enforce Office Communications Server 2007's requirement for TCP-level affinity, which means that each connection will "stick" to the server on which it started (rather than have its traffic potentially sent to other servers).

Also, since Office Communications Server 2007 transactions use multiple protocols and operate across multiple ports, WebMux is furthermore configured to enforce port affinity via its MAP capability, which means that for health-checking and failover purposes, if a service on any server that is involved in serving Office Communications Server 2007 transactions fails, the server is taken out of service (rather than allowing transactions that use other services to continue).

Sample WebMux Settings

Refer to Appendix B for detailed sample settings for configuring WebMux for use with Office Communications Server 2007 Enterprise Edition Consolidated Configuration.

Summary

To meet Office Communications Server 2007 requirements for load-balancing the Enterprise Edition Consolidated Configuration, a properly deployed and configured WebMux will:

- Expose multiple servers in the Front End Server pool in a distinct subnet as a single VIP (that can be accessed via a unique FQDN).
- Enforce TCP-level affinity within the Front End Server pool by targeting all Office Communications Server 2007-related traffic for each connection to the same server.
- Enforce port affinity within the Front End Server pool such that in the event of failure of a service that serves Office Communications Server 2007 transactions, the server will be taken out of service and all traffic will be targeted to healthy servers.

Enterprise Edition Expanded Configuration

The Office Communications Server 2007 Enterprise Edition Expanded Configuration consists of one or more content-identical computers hosting the Focus, IM Conferencing Server, and Telephony Conferencing Server, one or more computers each hosting the Web Conferencing Server, A/V Conferencing Server, and Web Components Server, and a separate computer hosting an SQL database. (What differentiates it from the Enterprise Edition Consolidated Configuration is that the Web Conferencing Server, A/V Conferencing Server, and Web Components Server are hosted on separate computers.)

The computer hosting the database is called the Back End Server and the computers hosting the Focus, IM Conferencing Server, and Telephony Conferencing Server are called Front End Servers. The Front End Server(s), Web Conferencing Server(s), A/V Conferencing Server(s), and Web Components Server(s) are considered Enterprise Servers; along with the Back End Server, comprise the Enterprise Edition Expanded Pool. They are all deployed in the internal network.

In an Enterprise Edition Expanded Pool, multiple Front End Servers and Web Components Servers require load balancing and therefore WebMux is required.

Note The conferencing servers and Back End Server are not load balanced by WebMux. The conferencing servers are effectively load balanced by the Conferencing Server Factory, which determines which conferencing server is available to service the request. For the Back End Server, a Microsoft SQL Server cluster can optionally be used to provide additional high availability and failover capabilities.

In large deployments with significant external traffic, Microsoft recommends offloading the task of user request authentication from the Front End Server(s) to a separate computer, called a Director. Directors help insulate the Enterprise pool from potentially malicious traffic, while relieving it of the overhead of performing authentication, thereby improving security and performance. A Director does not host users but, as a member of an Active Directory domain, has access to Active Directory for purposes of authenticating remote users and routing traffic to the Standard Edition Server. If a separate Director or Array of Directors is not deployed, the Enterprise Pool acts as the Director and handles external user authentication.

In the Enterprise Edition Expanded Configuration, a Director is a Front End server that has had most of its roles deactivated. A single or multiple Directors can be used; more than one Director is called an Array of Directors, and requires load balancing by WebMux.

WebMux Deployment

For load balancing by WebMux, the Front End Servers are isolated in their own distinct subnet in the internal network. The Web Components Servers and Directors, if they are deployed, are located outside of this distinct subnet.

A solo or dual WebMux configuration is deployed to manage the Front End Servers in the internal network at the local site, and in the internal network of each remote site at which Office Communications Server 2007 is deployed. We will refer to this WebMux as the *front end WebMux*.

A second solo or dual WebMux is deployed to manage the Web Component Servers and, if an Array of Directors is being deployed, the Director servers as well. We will refer to this WebMux as the *epool WebMux*. Refer to the discussion of Array of Directors below.

WebMux Configuration

The front end WebMux is configured with one farm, which contains the Front End Server computers. For the Enterprise Edition Expanded Configuration, the epool WebMux is configured with a farm for the Web Components Servers. If an Array of Directors is deployed, those servers can reside in an additional farm in the same WebMux (refer to the discussion of Array of Directors below).

Each farm functions as a virtual server and is assigned a VIP, which is resolved by an externally-configured FQDN. The load-balanced servers behind the WebMux can still be addressed by their assigned IP addresses.

The front end WebMux is configured to use NAT mode as its networking mode. The epool WebMux can use NAT or Transparent mode.

Since Office Communications Server 2007 transactions use multiple protocols and operate across multiple ports, WebMux is furthermore configured to enforce port affinity via its MAP capability, which means that for health-checking and failover purposes, if a port or protocol on any server that is involved in serving Office Communications Server 2007 transactions fails, the server is taken out of service (rather than allowing transactions that use other ports and protocols to continue).

Sample WebMux Settings

Refer to Appendix B for detailed sample settings for configuring WebMux for use with Office Communications Server 2007 Enterprise Edition Expanded Configuration.

Summary

To meet Office Communications Server 2007 requirements for load-balancing the Enterprise Edition Expanded Configuration, a properly deployed and configured WebMux will:

- Expose multiple Front End Server computers as a single VIP (that can be accessed via a unique FQDN).
- Expose multiple Web Components Server computers as a single VIP (that can be accessed via a unique FQDN).
- Enforce TCP-level affinity within the Front End Server pool and Web Components Server pool by targeting all Office Communications Server 2007-related traffic for each connection to the same server.
- Enforce port affinity within the Front End Server pool such that in the event of failure of a service that serves Office Communications Server 2007 transactions, the server will be taken out of service and all traffic will be targeted to healthy servers.

Web Components Servers

Web Components Server computers are deployed with the Enterprise Edition Expanded configuration. Refer to Enterprise Edition Expanded Configuration above.

Array of Directors (Array of Standard Edition Servers as a Director)

In Office Communications Server 2007 deployments with significant external traffic, Microsoft recommends offloading the task of user request authentication from the Standard Edition Server in the Standard Edition Configuration or the Enterprise pool in an Enterprise Edition Configurations to a separate computer, called a Director.

A Director helps insulate the Standard Edition Server or Enterprise pool from potentially malicious traffic, while relieving it of the overhead of performing authentication, thereby improving security and performance. A Director does not host users but, as a member of an Active Directory domain, has access to Active Directory for purposes of

authenticating remote users and routing traffic to the Standard Edition Server or Enterprise pool.

A Director is a Standard Edition server that has had most of its server roles (i.e., Web Conferencing, A/V Conferencing, Web Components) and the Address Book Server deactivated. A single or multiple Directors can be used; more than one Director is called Array of Standard Edition Servers as a Director or Array of Directors. The Array of Directors requires load balancing and therefore WebMux is needed. Directors are deployed in the internal network.

WebMux Deployment

To load balance an Array of Directors, a solo or dual WebMux configuration is deployed in the internal network at the local site, and in the internal network of each remote site at which Office Communications Server 2007 is deployed.

The WebMux used to load balance the Front End Servers deployed in a distinct subnet, the front end WebMux, cannot be used for load balancing the Directors. If the Office Communications Server 2007 Enterprise Edition Expanded Configuration is being deployed, the same WebMux that is used for the Web Components Servers, the epool WebMux, can be used for the Array of Directors or a dedicated WebMux can be employed. For the Enterprise Edition Consolidated Configuration, a separate WebMux is required (the epool WebMux) which can load balance other servers in the internal network other than the Front End Servers.

WebMux Configuration

The Array of Directors is configured in its own WebMux farm which functions as a virtual server and is assigned a VIP, which is resolved by an externally-configured FQDN.

Sample WebMux Settings

Refer to Appendix B for detailed sample settings for configuring WebMux for use with an Array of Directors.

Summary

To meet Office Communications Server 2007 requirements for load-balancing an Array of Standard Edition Servers as a Director, a properly deployed and configured WebMux will:

- Expose an Array of Directors as a single VIP (that can be accessed via a unique FQDN).
- Enforce TCP-level affinity within the Director array by targeting all Office Communications Server 2007-related traffic for each connection to the same server within the pool.
- Enforce port affinity within the Director array such that in the event of failure of any service that serves Office Communications Server 2007 transactions, the server will be taken out of service and all traffic targeted to healthy servers.

Edge Topologies

WebMux can be deployed in all Office Communications Server 2007 Edge topologies except the Consolidated Edge Topology. WebMux is required for the Scaled Single-Site Edge Topology, the local site for the Multiple Site with a Remote Site Edge Topology, and both the local and remote sites for the Multiple Site with a Scaled Remote Site Edge Topology.

For all topologies, if more than one ISA Server or other Reverse Proxy Server is deployed, a WebMux is required; but it can be the same WebMux used by the Edge Servers.

The following sections describe the need for, deployment, and configuration of WebMux with Office Communications Server 2007 Edge topologies.

Scaled Single-Site Edge Topology

The Office Communications Server 2007 Single Scaled-Site Edge Topology consists of two or more pairs of computers called Edge Servers. This Office Communications Server 2007 Edge topology has two or more computers with the Access Edge Server and Web Conferencing Edge Server collocated on them, and two or more computers with the A/V Edge Server installed on each. These together are called an Array of Edge Servers.

The Scaled Single-Site Edge Topology also requires one or more HTTP Reverse Proxy Servers, which can be ISA Server or some other make.

The Array of Edge Servers and the HTTP Reverse Proxy Server(s) are deployed in the perimeter network.

WebMux Deployment

Two solo or dual WebMux pairs are deployed in the perimeter network – one to load-balance and traffic-manage the internal interfaces of the Edge servers and the other for the external interfaces. The inner perimeter WebMux load balances internal traffic to the Edge Servers, while the outer perimeter WebMux load balances external traffic.

WebMux Configuration

Different configurations are required for the inner perimeter WebMux and outer perimeter WebMux, since the Web Conferencing Edge Servers are not load balanced on their internal interface, and Office Communications Server 2007 uses different ports for the internal and external Edge Server interfaces.

For the inner perimeter WebMux, the Edge Server computers are logically grouped into two farms: one for the Access Edge Servers and one for the A/V Edge Servers. The collocated Web Conferencing Edge / Access Edge Servers are members of the first farm, while the second farm is comprised by the A/V Edge Servers. (Even though the Web Conferencing Servers are collocated on computers in a WebMux farm, its server role is not configured for load balancing.)

For the outer perimeter WebMux, all three server roles are load balanced and so there are three farms. The computers on which the Access Edge Server and Web Conferencing Edge Server are collocated are logically grouped into two different farms, where both computers are members of both farms. This has the effect of creating one virtual computer for each of the two server types. A third farm contains the A/V Edge Server computers.

The two virtual servers for the inner perimeter WebMux and three virtual servers for the outer perimeter WebMux each have unique VIPs that are resolved by five different FQDNs. Additionally, the load-balanced servers behind the WebMux can still be addressed by their assigned IP addresses. (In the case of the Web Components Servers, FQDNs are created that resolve to the VIPs of those individual servers.)

WebMux is configured to use persistent connections in managing traffic to the servers in order to enforce Office Communications Server 2007's requirement for TCP-level affinity, which means that each connection will "stick" to the server on which it started (rather than have its traffic potentially sent to other servers).

Also, since Office Communications Server 2007 transactions use multiple protocols and operate across multiple ports, WebMux is furthermore configured to enforce port affinity via its MAP capability, which means that for health-checking and failover purposes, if a service on any server that is involved in serving Office Communications Server 2007 transactions fails, the server is taken out of service (rather than allowing traffic that uses other ports).

Sample WebMux Settings

Refer to Appendix C for detailed sample settings for configuring WebMux for use with Office Communications Server 2007's Scaled Single-Site Edge Topology.

Summary

To meet Office Communications Server 2007 requirements for load-balancing the Single Scaled-Site Edge Topology, a properly deployed and configured WebMux will:

- Load-balance and traffic-manage Edge Servers differently on their internal and external interfaces, to separately accommodate traffic from both internal and external users.
- Expose virtual servers for the Access Edge Server and A/V Edge Server roles hosted by multiple dedicated Access Edge Server and A/V Edge Server computers via their internal interfaces as two VIPs (that can be accessed via two unique FQDNs).
- Expose virtual servers for the Access Edge Server, Web Conferencing Server, and A/V Edge Server roles hosted by multiple collocated Access Edge Server / Web Conferencing Edge Server computers and dedicated A/V Edge Server computers via their external interfaces as three VIPs (that can be accessed via three unique FQDNs).

- Enforce TCP-level affinity within each server type by targeting all Office Communications Server 2007-related traffic for each connection to the same server.
- Enforce port affinity within each server type such that in the event of failure of any service used by Office Communications Server 2007, the server will be taken out of service and all Office Communications Server 2007-related traffic targeted to healthy servers.

Multiple Site with a Remote Site Edge Topology

The Office Communications Server 2007 Multiple Site with a Remote Site Edge Topology has both a local and a remote deployment.

At the local site, the Multiple Site with a Remote Site Edge topology is identical to the Single Site-Scaled Edge Topology, comprised of two or more pairs of computers, with the Access Edge Server and Web Conferencing Edge Server collocated on them, and two or more computers with the A/V Edge Server installed on each. These together are called an Array of Edge Servers.

At the remote site, there are two or more Edge Server computers: one or more computers having one or more Web Conferencing Edge servers installed on them, and a dedicated computer hosting the A/V Edge Server. (There is no remote Access Edge Server at the remote site – remote users access the Access Edge Server at the local site.)

The Multiple Site with a Remote Site Edge Topology also requires one or more HTTP Reverse Proxy Servers, which can be ISA Server or some other make.

At both the local and remote site, the Array of Edge Servers and HTTP Reverse Proxy Server(s) are deployed in the perimeter network.

WebMux Deployment

At the local site, two solo or dual WebMux pairs are deployed in the perimeter network – one to load-balance and traffic-manage the internal interfaces of the Edge servers and for the external interfaces. The inner perimeter WebMux load balances external traffic to the Edge servers, while the outer perimeter WebMux load balances external traffic.

The remote site only requires WebMux if there is more than one Web Conferencing Edge Server computer. If so, one WebMux (or pair) is required to load balance the external interfaces of these servers. (A WebMux to load balance the Web Conferencing Edge Servers' internal interface is not required in this configuration since these servers are not load balanced on their internal interface).

WebMux Configuration

For the Multiple Site with a Remote Site Edge Topology, the configuration is different for the local and remote sites.

Local Site

The local site WebMux configuration for the Multiple Site with a Remote Site Edge Topology is the same as for the Single Site-Scaled Edge Topology.

At the local site, different configurations are required for the inner perimeter WebMux and outer perimeter WebMux, since the Web Conferencing Edge Servers are not load balanced on their internal interface, and Office Communications Server 2007 uses different ports for the internal and external Edge Server interfaces.

For the inner perimeter WebMux at the local site, the Edge Server computers are logically grouped into two farms: one for the Access Edge Servers and one for the A/V Edge Servers. The collocated Web Conferencing Edge / Access Edge Servers are members of the first farm, while the second farm is comprised by the A/V Edge Servers. (Even though the Web Conferencing Servers are collocated on computers in a WebMux farm, its server role is not configured for load balancing.)

For the outer perimeter WebMux at the local site, all three server roles are load balanced and so there are three farms. The computers on which the Access Edge Server and Web Conferencing Edge Server are collocated are logically grouped into two different farms, where both computers are members of both farms. This has the effect of creating one virtual computer for each of the two server types. A third farm contains the A/V Edge Server computers.

The two virtual servers for the inner perimeter WebMux and three virtual servers for the outer perimeter WebMux each have unique VIPs that are resolved by five different FQDNs. Additionally, the load-balanced servers behind the WebMux can still be addressed by their assigned IP addresses. (In the case of the Web Components Servers, FQDNs are created that resolve to the VIPs of those individual servers.)

Remote Site

A WebMux is only required at the remote site for the Multiple site with Remote Site Edge topology to load-balance and traffic-manage multiple Web Conferencing Servers if more than one such computer be used to host this role (alternatively, this topology permits multiple server instances to be hosted on a single computer).

In the event of multiple Web Conferencing Server computers, these servers would reside in a single farm in the perimeter at the remote site.

Local and Remote Site

WebMux is configured to use persistent connections in managing traffic to the servers in order to enforce Office Communications Server 2007's requirement for TCP-level affinity, which means that each connection will "stick" to the server on which it started (rather than have its traffic potentially sent to other servers).

Also, since Office Communications Server 2007 transactions use multiple protocols and operate across multiple ports, WebMux is furthermore configured to enforce port affinity via its MAP capability, which means that for health-checking and failover purposes, if a service on any server that is involved in serving Office Communications Server 2007

transactions fails, the server is taken out of service (rather than allowing traffic that uses other ports).

Sample WebMux Settings

Refer to Appendix C for detailed sample settings for configuring WebMux for use with Office Communications Server 2007's Multiple Site with a Remote Site Edge Topology.

Summary

To meet Office Communications Server 2007 requirements for load-balancing the Multiple Site with a Remote Site Edge topology, a properly deployed and configured WebMux will:

- Load-balance and traffic-manage local and remote Edge Servers differently on their internal and external interfaces, to separately accommodate traffic from both internal and external users.
- Expose virtual servers for the Access Edge Server and A/V Edge Server roles for internal users hosted by multiple dedicated Access Edge Server and A/V Edge Server computers at the local site via their internal interfaces as two VIPs (that can be accessed via two unique FQDNs).
- Expose virtual servers for the Access Edge Server, Web Conferencing Server, and A/V Edge Server roles hosted by multiple collocated Access Edge Server / Web Conferencing Edge Server computers and dedicated A/V Edge Server computers at the local site via their external interfaces as three VIPs (that can be accessed via three unique FQDNs).
- If there is more than one Web Conferencing Server computer at the remote site, load-balance the external interfaces of multiple Web Conferencing Server computers and expose them as a virtual server as a VIP (that can be resolved by a unique FQDN).
- Enforce TCP-level affinity within each server type by targeting all Office Communications Server 2007-related traffic for each connection to the same server.
- Enforce port affinity within each server type such that in the event of failure of any service used by Office Communications Server 2007, the server will be taken out of service and all Office Communications Server 2007-related traffic targeted to healthy servers.

Multiple Site with a Scaled Remote Site Edge Topology

The Office Communications Server 2007 Multiple Site with a Remote Site Edge Topology has both a local and a remote deployment.

At the local site, the Multiple Site with a Scaled Remote Site Edge Topology is identical to the Single Site-Scaled Edge Topology and Multiple Site with a Remote Site Edge Topology, comprised of two or more pairs of computers, with the Access Edge Server and Web Conferencing Edge Server collocated on them, and two or more computers with

the A/V Edge Server installed on each. These together are called an Array of Edge Servers.

At the remote site, there are two or more pairs of computers: two having the Web Conferencing Edge servers installed on them and the other hosting the A/V Edge Server. (There is no remote Access Edge Server – remote users access the Access Edge Server at the local site.)

The Multiple Site with a Scaled Remote Site Edge Topology also requires one or more HTTP Reverse Proxy Servers, which can be ISA Server or some other make.

At both the local and remote site, the Array of Edge Servers and HTTP Reverse Proxy Server(s) are deployed in the perimeter network.

WebMux Deployment

At both the local and remote site, two solo or dual WebMux pairs are deployed in the perimeter network – one to load-balance and traffic-manage the internal interface of the Edge servers and one for the external interface. The inner perimeter WebMux load balances internal traffic to the Edge servers, while the outer perimeter WebMux load balances external traffic.

WebMux Configuration

For the Multiple Site with a Remote Site Edge Topology, the configuration is different for the local and remote sites.

Local Site

The local site configuration for the Multiple Site with a Scaled Remote Site Edge Topology is the same as for the Single Site-Scaled Edge Topology and Multiple Site with a Remote Site Edge Topology. The remote site configuration for the Multiple Site with a Scaled Remote Site Edge Topology is different than the non-scaled topology in that multiple A/V Edge Servers as well as multiple Web Conferencing Servers can be deployed.

At the local site, different configurations are required for the inner perimeter WebMux and outer perimeter WebMux, since the Web Conferencing Edge Servers are not load balanced on their internal interface, and Office Communications Server 2007 uses different ports for the internal and external Edge Server interfaces.

For the inner perimeter WebMux at the local site, the Edge Server computers are logically grouped into two farms: one for the Access Edge Servers and one for the A/V Edge Servers. The collocated Web Conferencing Edge / Access Edge Servers are members of the first farm, while the second farm is comprised by the A/V Edge Servers. (Even though the Web Conferencing Servers are collocated on computers in a WebMux farm, its server role is not configured for load balancing.)

For the outer perimeter WebMux at the local site, all three server roles are load balanced and so there are three farms. The computers on which the Access Edge Server and Web Conferencing Edge Server are collocated are logically grouped into two different farms,

where both computers are members of both farms. This has the effect of creating one virtual computer for each of the two server types. A third farm contains the A/V Edge Server computers.

The two virtual servers for the inner perimeter WebMux and three virtual servers for the outer perimeter WebMux each have unique VIPs that are resolved by five different FQDNs. Additionally, the load-balanced servers behind the WebMux can still be addressed by their assigned IP addresses. (In the case of the Web Components Servers, FQDNs are created that resolve to the VIPs of those individual servers.)

Remote Site

the remote site configuration for the Multiple Site with a Scaled Remote Site Edge Topology is different than the non-scaled topology in that multiple A/V Edge Servers as well as multiple Web Conferencing Servers can be deployed.

Unlike the local site topology, the topology for the remote site excludes the Access Edge Servers, since they are not present in the remote topology (remote users instead access the Access Edge Servers at the local site).

The remote site inner perimeter WebMux has only one farm – for the A/V Edge Servers – with its own VIP and FQDN. (Web Conferencing Edge Servers are not load balanced on their internal interface, rather, Office Communications Server 2007 accesses them individually via FQDNs based on the server VIPs.)

The remote site outer perimeter WebMux has two farms: one for the Web Conferencing Servers and one for the A/V Edge Servers. Each farm has its own VIP and FQDN, for the two server roles.

Local and Remote Site

WebMux is configured to use persistent connections in managing traffic to the servers in order to enforce Office Communications Server 2007's requirement for TCP-level affinity, which means that each connection will “stick” to the server on which it started (rather than have its traffic potentially sent to other servers).

Also, since Office Communications Server 2007 transactions use multiple protocols and operate across multiple ports, WebMux is furthermore configured to enforce port affinity via its MAP capability, which means that for health-checking and failover purposes, if a service on any server that is involved in serving Office Communications Server 2007 transactions fails, the server is taken out of service (rather than allowing traffic that uses other ports).

Sample WebMux Settings

Refer to Appendix C for detailed sample settings for configuring WebMux for use with Office Communications Server 2007's Multiple Site with a Scaled Remote Site Edge Topology.

Summary

To meet Office Communications Server 2007 requirements for load-balancing the Multiple Site with a Scaled Remote Site Edge topology, a properly deployed and configured WebMux will:

- Load-balance and traffic-manage local and remote Edge Servers differently on their internal and external interfaces, to separately accommodate traffic from both internal and external users.
- Expose virtual servers for the Access Edge Server and A/V Edge Server roles for internal users hosted by multiple dedicated Access Edge Server and A/V Edge Server computers at the local site via their internal interfaces as two VIPs (that can be accessed via two unique FQDNs).
- Expose virtual servers for the Access Edge Server, Web Conferencing Server, and A/V Edge Server roles hosted by multiple collocated Access Edge Server / Web Conferencing Edge Server computers and dedicated A/V Edge Server computers at the local site via their external interfaces as three VIPs (that can be accessed via three unique FQDNs).
- Expose virtual servers for the A/V Edge Server and Web Conferencing Edge Server roles hosted by multiple dedicated A/V Edge Server computers and Web Conferencing Edge Server computers at the remote site via their external interfaces as two VIPs (that can be accessed via two unique FQDNs).
- Enforce TCP-level affinity within each server type by targeting all Office Communications Server 2007-related traffic for each connection to the same server.
- Enforce port affinity within each server type such that in the event of failure of any service used by Office Communications Server 2007, the server will be taken out of service and all Office Communications Server 2007-related traffic targeted to healthy servers.

ISA Servers or other Reverse Proxy Servers

Office Communications Server 2007 requires the use of HTTP Reverse Proxy Servers in the perimeter network, which can be ISA Servers or other makes of reverse proxies. If you deploy multiple reverse proxies, which is recommended for high availability, they require load balancing.

In using WebMux to load-balance multiple Reverse Proxy Servers, the benefits are not restricted to Office Communications Server 2007 users: all traffic to your Reverse Proxy servers can be load balanced by WebMux, and you have the benefits of load balancing, scalability, failover, etc.

WebMux Deployment

You can either deploy a dedicated WebMux to load balance Reverse Proxy Servers, whether ISA Server or another type of Reverse Proxy server, or use the outer perimeter WebMux for that purpose.

WebMux Configuration

Regardless of whether you use a dedicated or shared WebMux to load balance your reverse proxies, you will place them in their own WebMux farm.

In configuring WebMux settings for the farm and its member servers, you can choose any of WebMux's scheduling methods for your web farm to properly distribute a mix of Office Communications Server 2007 and non-Office Communications Server 2007 traffic.

If your Reverse Proxy Servers will be receiving SSL- or TLS-encrypted traffic, you can use WebMux's SSL/TLS offloading capabilities to terminate the traffic so that clear text is sent to the Reverse Proxy servers, thereby unburdening them from the tasks of encryption and decryption. WebMux's SSL/TLS encryption and decryption can be done in hardware using dedicated processors to accomplish the tasks more quickly.

Sample WebMux Settings

Refer to Appendix C for detailed sample settings for configuring WebMux for use with ISA Server or other Reverse Proxy Server.

Summary

To meet Office Communications Server 2007 requirements for load-balancing Multiple ISA Servers or other Reverse Proxy Servers, a properly deployed and configured WebMux will:

- Expose a virtual server for Multiple ISA Servers or other Reverse Proxy Servers at the local or remote site via their external interfaces as a single VIP (that can be accessed via a unique FQDN).
- Enforce TCP-level affinity within each server type by targeting all Office Communications Server 2007-related traffic for each connection to the same server.
- Enforce port affinity within each server type such that in the event of failure of a protocol or port that serves Office Communications Server 2007 transactions, the server will be taken out of service and all Office Communications Server 2007-related traffic targeted to healthy servers.

Web Farm

WebMux is ideally suited to balance the servers that comprise your web farm. You can either use a dedicated WebMux for this purpose, or leverage your investment in other WebMuxes used for Office Communications Server 2007 to load-balance your web farm.

In using WebMux to load-balance your web farm, the benefits are not restricted to Office Communications Server 2007 users: all traffic to whatever web farms you have can be load balanced by WebMux, and you have the benefits of load balancing, scalability, failover, etc.

WebMux Deployment

If your web farm resides in your internal network, you can either deploy a dedicated WebMux to load-balance it, or use the epool WebMux (the WebMux(es) that is/are used for the Web Components Servers and/or Array of Directors).

If your web farm resides in the same perimeter network where Office Communications Server 2007's Edge servers reside, you can either deploy a dedicated WebMux to load balance them, or use the outer perimeter WebMux (which handles external traffic to the Edge Servers) for that purpose.

WebMux Configuration

Regardless of whether you use a dedicated or shared WebMux to load balance your web farm, the web servers will reside in a single WebMux farm.

In configuring WebMux settings for the farm and its servers, you can choose any of WebMux's scheduling methods for your web farm to properly distribute the traffic, you can utilize WebMux's SSL/TLS offloading functionality if you have web servers that perform secure transactions, and you can target transactions to particular servers using WebMux's content-switching capabilities.

Sample WebMux Settings

Refer to Appendix C for detailed sample settings for configuring WebMux for use with an Office Communications Server 2007 web farm.

Summary

To meet Office Communications Server 2007 requirements for load-balancing multiple web servers that comprise a web farm, a properly deployed and configured WebMux will:

- Expose a virtual server for multiple web servers in the internal or perimeter network at the local or remote site via their external interfaces as a single VIP (that can be accessed via a unique FQDN).
- Enforce TCP-level affinity within each server type by targeting all Office Communications Server 2007-related traffic for each connection to the same server.
- Enforce port affinity within each server type such that in the event of failure of a protocol or port that serves Office Communications Server 2007 transactions, the server will be taken out of service and all Office Communications Server 2007-related traffic targeted to healthy servers.

Office Communicator Web Access

Microsoft Office Communicator Web Access facilitates web-based access to Office Communications Server 2007 functionality. Its main servers reside in the internal network, while the ISA Server or other Reverse Proxy Server(s) used by external users reside(s) in the perimeter network.

In deploying Communicator Web Access, Microsoft recommends physically separating internal user traffic from external user traffic by using one or more dedicated servers each for internal and external users. Alternately a single server can be used for both internal and external users.

WebMux is required if multiple separate servers are used for internal and external users. It can also be used to provide failure protection where a single server each is used for internal and external users by deploying an additional server as a shared internal and external user server to facilitate fault-tolerance for both the single internal and external server.

WebMux's SSL/TLS termination feature can be used to offload SSL/TLS encryption and decryption from external user Communicator Web Access servers. If there will be high volumes of Communicator Web Access transactions, you may consider using a WebMux configuration that additionally provides SSL/TLS acceleration, to perform the encryption and decryption on a dedicated CAI-RSA card.

WebMux Deployment

One or two solo or dual WebMux configurations are deployed in the internal network at the local site and in the internal network of each remote site at which Communicator Web Access is deployed. A separate WebMux, deployed in the perimeter network, load balances the ISA Server or other Reverse Proxy Server.

Possible WebMux topologies for a multiple-server Communicator Web Access deployment are:

- Two WebMuxes or pairs in the internal network for the internal and external user server array, and a separate WebMux or pair in the perimeter network for the ISA Server or other Reverse Proxy Server.
- One WebMux or pair in the internal network for both the internal and external user server arrays, and a separate WebMux or pair in the perimeter network for the ISA Server or other Reverse Proxy Server.

Alternatively:

- For the WebMux(es) required in the internal network, the epool WebMux (the WebMux(es) that is/are used for the Web Components Servers and/or Array of Directors) can be used, either exclusively or in combination with a dedicated WebMux or pair for Communicator Web Access.
- For the WebMux(es) in the perimeter network for load balancing Multiple ISA Servers or other Reverse Proxy Servers, the outer perimeter WebMux (which is used for the external interfaces of the Edge Servers) can be used.

For performance reasons, if high volumes of external user traffic will be experienced, you may want to use a WebMux model that offers SSL acceleration. Refer to Table 7 for information about WebMux's SSL/TLS performance characteristics and options.

WebMux Configuration

In deploying WebMux with Communicator Web Access, regardless of how many and which WebMuxes are used, internal user servers, external user servers, and ISA Server or other Reverse Proxy Server all reside in separate farms.

In the internal network:

- If you are deploying a dedicated WebMux or pair each for the internal and external server arrays, each WebMux or pair will have one farm each.
- If you are deploying a single WebMux or pair for both the internal and external server arrays, the WebMux or pair will have two farms.
- If you are using the same WebMux for Communicator Web Access as for the Web Components Servers (in the Office Communications Server 2007 Enterprise Edition Expanded Configuration) and/or Array of Directors, two additional farms will be added to the epool WebMux or pair.

In the perimeter network:

- If you are deploying a dedicated WebMux or pair for the ISA Servers or other Reverse Proxy Servers, it will have one farm.
- If you are using the same WebMux for Communicator Web Access as for the Edge Servers, one additional farm will be added to the outer perimeter WebMux or pair.

In the case in which a shared server is deployed as a hot standby with a dedicated server each for internal and external users, two farms are still required, where the shared server is a member of both farms.

Differentiating Internal and External User Server Farms

Regardless of the WebMux deployment topology, Communicator Web Access requires a method to target internal and external users to the appropriate farm. The two farms can be differentiated for Communicator Web Access either by assigning a different VIP (and FQDN) for each farm or using the same VIP but a different port number (and requiring users to specify the appropriate port number or, for external users, by having the firewall reassign the port number).

For example, if you want to assign the same VIP for both farms, you could assign port 444 for the internal user farm and port 443 for the external farm and require internal users to specify the port number (for example, via <https://cwaVIP.contoso.com:444>). Or, you could assign port 443 for the internal user farm and port 444 for the external user farm and configure your firewall to accept requests on the default SSL/TLS port 443 but redirect them to port 444 so that they reach the external user servers.

If you are deploying a shared server for both internal and external users alongside a dedicated server for each, either each Communicator Web Access instance would use a different port or two IP addresses would be assigned to the shared server.

Networking Mode

When deploying WebMux with Communicator Web Access, it is recommended that either NAT or Transparent mode be used.

Scheduling Method

When deploying WebMux with Communicator Web Access, the scheduling method used for all farms must be one that imposes persistent connections to enforce Communicator Web Access's requirement for TCP-level affinity, which means that each connection will "stick" to the server on which it started (rather than have its traffic potentially sent to other servers).

SSL/TLS Offloading

You can configure WebMux to offload SSL/TLS encryption and decryption tasks from the Communicator Web Access servers. To do that, you will need to configure the certificates that would normally be resident in the Communicator Web Access servers to instead be held in WebMux, and configure the Communicator Web Access server array farms to perform SSL/TLS termination.

If the WebMux model you are using is equipped with an SSL/TLS termination card, or if you have ordered that as an option, WebMux will also accelerate the SSL/TLS encryption and decryption by performing them in hardware.

Sample WebMux Settings

Refer to Appendix D for detailed sample settings for configuring WebMux for use with Communicator Web Access.

Summary

To meet Office Communications Server 2007 requirements for load-balancing Communicator Web Access, a properly deployed and configured WebMux will:

- Expose separate server arrays for internal and external users as two virtual servers (each of which can have a unique FQDN).
- Allow both virtual servers to have the same VIP but use different port numbers, different VIPs but with same port number, or different VIPs and port numbers.
- Enforce TCP-level affinity within the server array by targeting all Office Communications Server 2007-related traffic for each connection to the same server.
- Enforce port affinity within the server array such that in the event of failure of a protocol or port that serves Office Communications Server 2007 transactions, the server will be taken out of service and all Office Communications Server 2007-related traffic targeted to healthy servers.
- Optionally (depending on WebMux configuration) terminate SSL/TLS transactions such that clear text is sent to the Communicator Web Access servers.

- Optionally (depending on WebMux model) accelerate SSL/TLS transactions to increase performance.

Speech Server

Microsoft Office Communications Server 2007 Speech Server can be deployed on a single server computer or using multiple servers (“clones”). It requires an IIS web server, which can be collocated with the other Speech Server components on Speech Server computers or on separate Web Server computers with IIS hosting VXML and SALT pages.

The Small Enterprise and Large Enterprise Speech Server topologies, which use multiple servers, require WebMux, while the Single Server (“all in one”) Topology does not.

If you have configured Speech Server and its SIP peers in your deployment to use Mutual Transport Layer Security (TLS) to authenticate the endpoints and encrypt the transport channel, you can use WebMux’s SSL/TLS termination feature to offload TLS encryption and decryption from Speech Servers. If there will be high volumes of Speech Server transactions, you may consider using a WebMux configuration that additionally provides TLS acceleration, to perform the encryption and decryption on a dedicated CAI-RSA card.

WebMux Deployment

One or two solo or dual WebMux configurations are deployed in the internal network at the local site and in the internal network of each remote site at which Speech Server is deployed.

Possible WebMux topologies for a Small Enterprise Topology or Large Enterprise Topology are:

- One WebMux (or pair) in the internal network for the Speech Servers, if the web servers are installed on the Speech Server computers
- One WebMux (or pair) in the internal network for both the Speech Servers and Web servers.
- Two WebMuxes (or pairs) in the internal network – one each for the Speech Servers and Web servers.

Alternatively:

- The epool WebMux (the WebMux(es) that is/are used for the Web Components Servers and/or Array of Directors) can be used, either exclusively or in combination with a dedicated WebMux (or pair) for Speech Server.

WebMux Configuration

In deploying Speech Server with WebMux, either one or two farms are required in one or two WebMuxes (or pairs):

- If you are deploying Speech Servers that have the web server installed on them, the WebMux will have one farm
- If you are deploying separate Speech Servers and Web Servers with one WebMux, the WebMux will have two farms
- If you are deploying separate Speech Servers and Web Servers with two WebMuxes (or pairs), each WebMux will have one farm
- If you are using the same WebMux for Speech Server as for the Web Components Servers (in the Office Communications Server 2007 Enterprise Edition Expanded Configuration) and/or Array of Directors, one or two additional farms will be added to the epool WebMux

Networking Mode

As the Speech Servers need to connect directly with the SIP peers, it is recommended that WebMux's Out-of-Path networking mode be used for the Speech Servers.

Scheduling Method

When deploying WebMux with Speech Server, it is recommended for the Speech Server farm to use (unweighted, non-persistent) round robin, as other scheduling methods may lead to undesirable results when service states change, when services are too busy, or when connectivity issues arise.

If the Web Servers are being deployed as separate computers, its farm can use any scheduling method.

TLS Offloading

You can configure WebMux to offload TLS encryption and decryption tasks from the Speech Servers. To do that, you will need to configure the certificates that would normally be resident in the Speech Servers to instead be held in WebMux, and configure the Speech Server farms to perform TLS termination.

If the WebMux model you are using is equipped with a CAI-RSA card, or if you have ordered that as an option, WebMux will also accelerate the TLS encryption and decryption by performing those operations in hardware.

Sample WebMux Settings

Refer to Appendix E for detailed sample settings for configuring WebMux for use with Speech Server.

Summary

To meet Office Communications Server 2007 requirements for load-balancing a Small Enterprise Topology or Large Enterprise Topology of Speech Server, a properly deployed and configured WebMux will:

- For deployments in which the web server is installed on the Speech Server computers, expose multiple Speech Servers as a virtual server having its own VIP (which can be accessed via a unique FQDN).
- For deployments in which the web server is installed on separate Web Server computers, expose multiple Speech Servers and Web Servers as two virtual servers, each having its own VIP (which can be accessed via two unique FQDNs).
- Optionally (depending on WebMux configuration) terminate TLS transactions such that clear text is sent to the Speech Servers.
- Optionally (depending on WebMux model) accelerate TLS transactions to increase performance.

Other Office Communications Server 2007 Modules

In addition to the Office Communications Server 2007 components and modules documented above, load balancing may be required for other Office Communications Server 2007 components. This may include:

- Mediation Servers
- Conferencing Servers
- CTI Server (RCC Gateway)
- Third-party offerings

Documentation of these and other modules is beyond the scope of this guide.

In general, however, if more than one identical server is used for a particular function, those servers require load balancing. If only one server is required, consider the consequences of the failure of that server or a required protocol for that software. If you cannot afford the downtime of that service, or if performance and/or capacity is an issue, consider adding one or more additional servers and load balancing them.

WebMux Deployment

If the server is deployed in the internal network and can reside in the same network as the Office Communications Server 2007 servers (not the Front End Server pool, which are in a discrete subnet), they can be load-balanced by the same WebMux being used to manage the Web Components Servers (for the Enterprise Edition Expanded Configuration and/or Array of Directors), the epool WebMux.

If the server is deployed in the perimeter network, it can be load-balanced by either or both the inner and outer perimeter WebMuxes.

You can alternatively deploy a dedicated WebMux for one or more additional servers should you desire, but this may not be a requirement.

WebMux Configuration

Each pool of like servers needs to be configured in their own WebMux farm, so that they form a virtual server representing the same content. In some cases – such as in the case where software is collocated on multiple servers – more than one farm may be required.

The WebMux scheduling method, whether connection persistence is required, whether port affinity via MAP capability is required, whether content switching is needed, and whether SSL/TLS offloading is appropriate depend on the particular solution being deployed.

Reference Office Communications Server 2007/WebMux Topologies

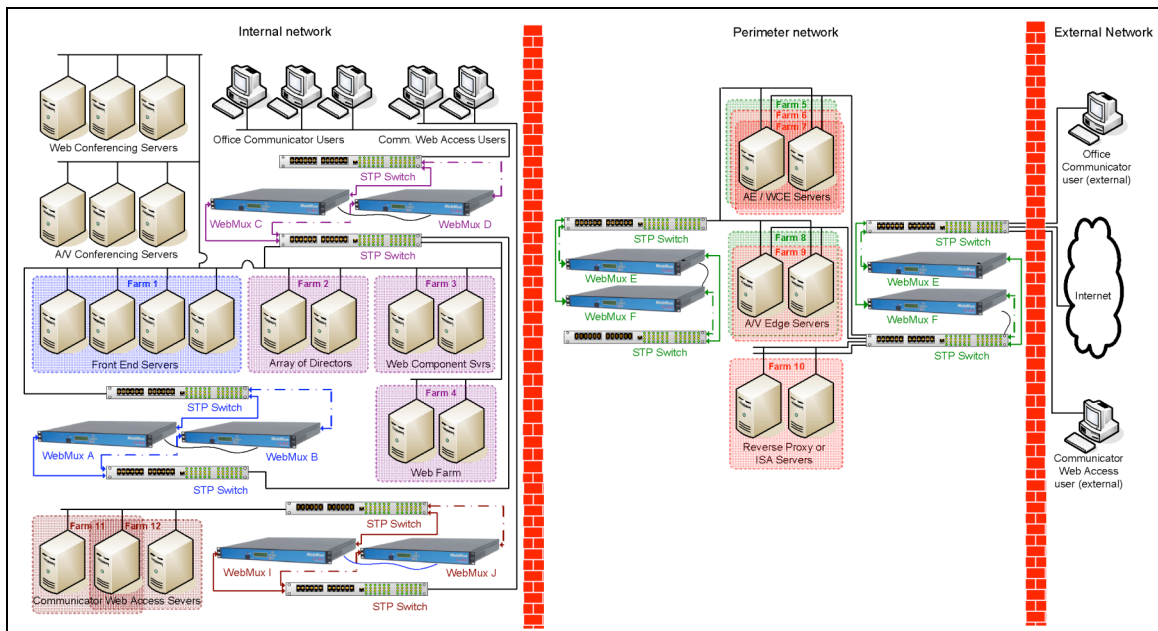
Following are reference architecture diagrams showing WebMux deployed in the context of an Office Communications Server 2007 deployment.

Local Site Deployment

Figure 1 shows a sample local site WebMux deployment in an Office Communications Server 2007 Enterprise Edition Expanded Configuration with a Scaled Multi-Server Edge Topology and Office Communicator Web Access, which involves multiple servers in multiple farms.

It uses five pairs of WebMuxes: three in the local internal network and two in the local perimeter network.

Figure 1: Local Site Deployment Topology



Error! Bookmark not defined.

In the above diagram of a fault-tolerant, high availability local site configuration comprising the Office Communications Server 2007 Enterprise Edition Extended Configuration with an Array of Directors and a Scaled Edge Topology, as well as Communicator Web Access:

- A pair of WebMuxes (blue) is deployed in dual mode to load balance the Front End Server pool (Farm 1).
- An additional pair of WebMuxes (purple) is deployed in dual mode to load balance the Web Components Servers (Farm 2), an Array of Directors (Farm 3), and a web farm (Farm 4). The conferencing servers do not require load balancing – they are part of the Enterprise pool but not members of any WebMux farm.
- An additional WebMux pair (brown) is deployed in dual mode to load balance the server pool for Communicator Web Access. This pool contains three identically configured servers, with one server dedicated to internal users, one to external users, and the third is a shared hot standby server which is automatically brought online only if either of the other two servers fails. Two WebMux farms (Farms 11 and 12) are used to present two different VIPs, with the shared server belonging to both farms.
- Two pairs of WebMuxes are deployed in dual mode for the perimeter network to load-balance the Edge Server Array: one pair to load balance the external traffic to the Edge Servers (red) and one to balance the traffic from the internal network (green). The outer perimeter WebMux is also used to load-balance a pool of Reverse Proxy Servers.
- The collocated Access Edge Servers and Web Conferencing Edge Servers are both members of WebMux farms (Farms 6 and 7) in the outer perimeter WebMux to form a virtual server for external traffic for each server role, each having its own VIP. The A/V Edge servers reside in their own farm (Farm 8) on the outer perimeter WebMux, having its own VIP.
- The collocated Access Edge Servers and Web Conferencing Servers are members of a single farm (Farm 5) in the inner perimeter WebMux. This WebMux is configured to only load balance Access Edge traffic, since the Web Conferencing Edge Servers do not require load balancing on their internal interfaces. The A/V Edge Servers reside in their own farm in the inner perimeter WebMux (Farm 8).
- The Reverse Proxy Servers form their own farm (Farm 10) in only the outer perimeter WebMux, and are addressable via an external VIP.
- All WebMuxes are configured to use a two-arm networking mode, which causes traffic to flow via WebMux in both directions (both inbound traffic to the servers and outbound traffic from the servers), as illustrated by arrowheads.
- Traffic flows through the primary WebMux of the pair via switches (solid line); the secondary WebMuxes are connected to the switches and network (broken lines) and serve as hot standbys should a primary WebMux fail.

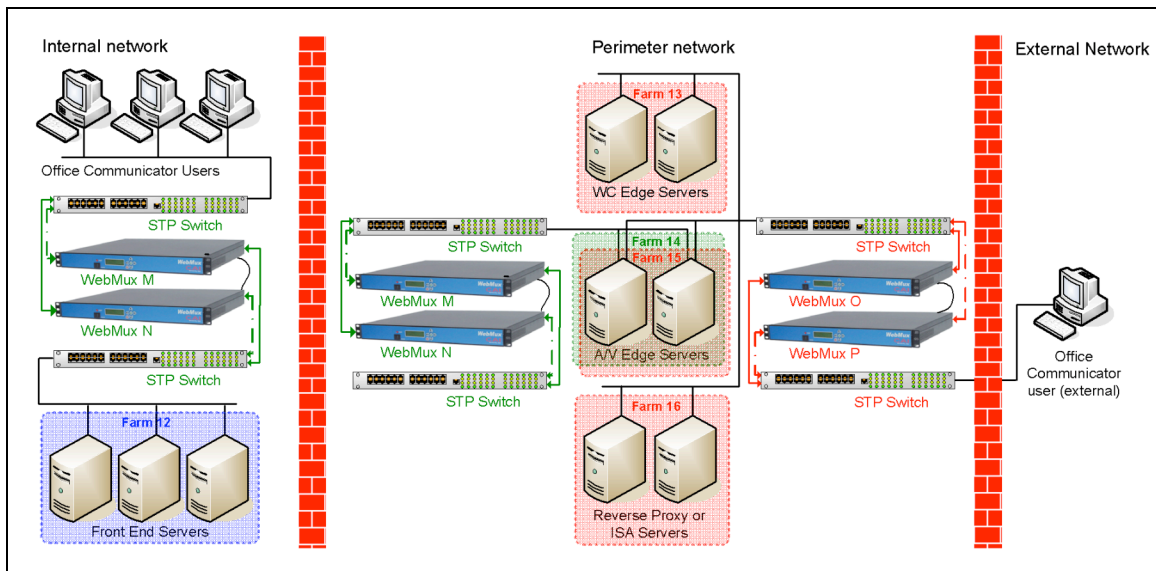
If WebMux fault tolerance and overall performance requirements are more modest, the required load balancing and traffic management can be accomplished with a single WebMux for the internal network and two WebMuxes for the perimeter network.

Remote Site Deployment

Figure 2 shows a remote site deployment of Office Communications Server 2007 Enterprise Edition Consolidated Configuration with a Multiple Site Edge topology and a Scaled Remote Site Edge. It uses four pairs of WebMuxes: two in the local internal network and two in the local perimeter network.

It uses three pairs of WebMuxes: one for the remote internal network, and two for the remote perimeter network.

Figure 2: Remote Site Deployment Topology



In the above diagram of a fault-tolerant, high availability remote site configuration comprising the Office Communications Server 2007 Enterprise Edition Consolidated Configuration and a Scaled Edge Topology:

- A pair of WebMuxes (blue) is deployed in dual mode to load balance Front End Server pool (Farm 1).
- A pair of WebMuxes (green) is deployed in dual mode in the perimeter network to load-balance the internal interfaces of the A/V Edge Server array (Farm 14).
- An additional pair of WebMuxes (red) is deployed in dual mode in the perimeter network to load-balance the external interfaces of the Web Conferencing Edge Server array (Farm 13) and the A/V Edge Server array (Farm 15), as well as the Reverse Proxy servers (Farm 16).

- The Web Conferencing Edge Servers and A/V Edge Servers form two farms (Farms 13 and 15), with each role having its own VIP on their external interfaces. The A/V Edge Servers also have an internal farm (Farm 14) with its own VIP.
- The Reverse Proxy Servers form their own farm (Farm 16), and are addressable via an external VIP.
- All WebMuxes are configured to use a two-arm networking mode, which causes traffic to flow via WebMux in both directions (both inbound traffic to the servers and outbound traffic from the servers), as illustrated by arrowheads.
- Traffic flows through the primary WebMux of the pair via switches (solid line); the secondary WebMuxes are connected to the switches and network (broken lines) and serve as hot standbys should a primary WebMux fail. Because the dual WebMuxes are deployed in Transparent networking mode, the interconnecting switches must support STP protocol (not required in solo WebMux deployment).

If WebMux fault tolerance and overall performance requirements are more modest, the required load balancing and traffic management can be accomplished with one WebMux each for the internal and perimeter network.

Scoping WebMux Requirements for Office Communications Server 2007 Deployments

Introduction

This chapter covers which Office Communications Server 2007 deployments you will need WebMux for, and how many. For some Office Communications Server 2007 deployments, you will need more than one WebMux.

This chapter will help you determine how many WebMuxes you need for your Office Communications Server 2007 deployment, and understand which WebMux models might be most appropriate.

Office Communications Server 2007 Load Balancer Requirements

Office Communications Server 2007 can be deployed in several different configurations and topologies, not all of which require the use of a hardware load balancer, while some configurations and topologies require multiple load balancers.

Office Communications Server 2007 offers substantial flexibility in its deployment models, with a number of configurations and topologies. Configurations can include multiple Directors, the Enterprise Extended configuration can include multiple Web Components Servers, and Edge configurations include one or more ISA Server or other Reverse Proxy Server.

In general, any configuration in which more than one computer running any type of server software requires load balancing and traffic management by a hardware load balancer like WebMux. Within Office Communications Server 2007, at least one WebMux is required in the following cases:

- Any Enterprise Edition configuration
- Any deployment with an Array of Directors
- Any Scaled Edge topology
- Any local Edge topology that supports a Remote Site Edge deployment
- Any configuration or topology with more than one Reverse Proxy Server
- A Communicator Web Access deployment with a server array
- Any Small Enterprise or Large Enterprise topology

Table 4 below illustrates for each Office Communications Server 2007 configuration and topology whether a load balancer is required. If you are deploying multiple configurations and topologies, you will need more than WebMux, as described in the section that follows the tables.

Table 4: Load Balancer Requirements for Various Office Communication Server 2007 Configurations and Topologies

Standard Edition or Enterprise Edition Configuration

Configuration	Requirement for WebMux
Standard Edition	Does not require WebMux except when deployed with an Array of Directors
Enterprise Edition Consolidated Configuration	Requires WebMux except when only one Front End Server is deployed
Enterprise Edition Expanded Configuration	Requires WebMux except when only one Front End Server is deployed

Edge Topologies

Topology	Requirement for WebMux
Consolidated Edge Topology	Does not require WebMux
Single-Site Edge Topology	Does not require WebMux
Scaled Single-Site Edge Topology	Requires WebMux
Multiple Site with a Remote Site Edge Topology	Requires WebMux for the local site, and the remote site if multiple Web Conferencing Edge Servers are deployed
Multiple Site with a Scaled Remote Site Edge Topology	Requires WebMux for the local site and each remote site

Web Farm

Configuration	Requirement for WebMux
Single web server	Does not require WebMux
Multiple web servers	Requires WebMux

ISA Server or other Reverse Proxy Server

Configuration	Requirement for WebMux
Reverse Proxy collocated on another server	Does not require WebMux
Single ISA Server or other Reverse Proxy Server	Does not require WebMux
Multiple ISA Servers or other Reverse Proxy Servers	Requires WebMux

Communicator Web Access

Configuration	Requirement for WebMux
One server for both internal and external users	Does not require WebMux
Separate single servers for internal and external users	Does not require WebMux unless a shared third server is deployed for fault tolerance
Multiple servers for internal and/or external users	Requires WebMux
Multiple ISA Servers or other Reverse Proxy Servers	Requires WebMux

Speech Server

Configuration	Requirement for WebMux
Single-server (“all-in-one”) topology	Does not require WebMux
Small Enterprise Topology	Requires WebMux
Large Enterprise Topology	Requires WebMux

Number of WebMuxes Required

You will need to determine how many WebMuxes you require for your Office Communications Server 2007 implementation. Such choices relate to questions of:

- Which configurations and topologies will be deployed at the central location?
- What other Office Communications Server 2007 modules will be deployed and what load balancing requirements do they have?
- How many remote locations (if any) will be deployed?
- What are your user and traffic volumes?

- What is the skew of internal versus external users?
- What are the uptime requirements for the core hosting?
- What are the uptime requirements for the edge deployment?
- What are the uptime requirements for each remote deployment?

Single Versus Paired WebMux Configuration

Just as you need to determine which Office Communications Server 2007 configurations and topologies to deploy based somewhat on reliability concerns, you will need to decide which WebMux deployments require a fault-tolerant configuration.

In a paired configuration, one WebMux is active and the other is passive.

Determining How Many WebMuxes You Need

Determining how many WebMuxes you need can be a bit complicated, since there are a number of considerations, so we'll start out with a quick Office Communications Server 2007 topology overview and rule of thumb for WebMux determinations.

Rough Calculation

Office Communications Server 2007 puts its Standard or Enterprise servers in the internal network. Generally, the Standard Edition does not require a WebMux, the Enterprise Edition Consolidated Configuration requires one WebMux, and the Enterprise Edition Consolidated Configuration requires two WebMuxes in the internal network.

You will also need to deploy an Edge topology in the perimeter network to host your internal users. This generally requires two WebMuxes unless your volumes are low or you do not require fault tolerance for the remote site, in which case one WebMux or no WebMux is required.

If you are the local site for one or more remote locations that will deploy Office Communications Server 2007, each remote site will require a Edge deployment as well as a Standard or Enterprise Edition deployment, which will require no WebMux if volumes are low, or two WebMuxes if volumes are moderate, or three WebMuxes if volumes are high (or more if volumes are very high).

For any WebMuxes that you want to deploy in a fault-tolerant dual configuration, double the count.

Precise Calculation

As shown in Table 5 below, there are a number of factors that determine how many WebMuxes you will require. It is good to keep two points in mind:

Firstly, any function that is performed only by one server will not be available should that server fail or crash. If it is a critical function for the Office Communications Server 2007 operation you desire, it should be replicated and load balanced.

Secondly, although there are Office Communications Server 2007 configurations and topologies that do not require a load balancer, those deployments may be coupled with multiple companion servers that do require load balancing. For example:

- Directors (Standard Edition Server as a Director) are effectively companions to Standard or Enterprise servers and require their own computer. More than one Director (an Array of Directors) requires a load balancer.
- Reverse Proxy Servers are effectively companions to Edge Servers and require their own load balancer. More than one Reverse Proxy requires a load balancer.
- If you are making a web farm accessible to Office Communications Server 2007 users, you will want to load balance it. More than one web server requires a load balancer.

So although these configurations may be unlikely, a Standard Edition Configuration (which requires no load balancer) with two Directors requires a load balancer; and likewise a Single-Site Edge Topology (which requires no load balancer) with two Reverse Proxy Servers requires a load balancer.

Table 5 below illustrates how many WebMuxes you could require for each site and network.

Table 5: Number of WebMuxes Required for Various Office Communication Server 2007 Configurations and Topologies

Local Internal Network

Configuration	Solo WebMux	Dual WebMux
Standard Edition Configuration with 0 or 1 Director	0	-
Standard Edition Configuration with an Array of Directors	1	2
Enterprise Edition Consolidated Configuration with 1 Front End Server and without an Array of Directors	0	-
Enterprise Edition Consolidated Configuration with 2 or more Front End Servers and without Array of Directors	1	2
Enterprise Edition Consolidated Configuration with 2 or more Front End Server and with an Array of Directors	2	4
Enterprise Edition Expanded Configuration with 1 of each server type	0	-
Enterprise Edition Expanded Configuration with 1 Front End Server and an Array of Directors	1	2
Enterprise Edition Expanded Configuration with 2 or more Front End Servers (with or without an Array of Directors)	2	4
Single web server	0	-
Web farm	+0 or +1*	+0 or +2*
Communicator Web Access server array with 2 or more servers	+0-+2**	+0-+4**
Speech Server farm with collocated web server	+0-+1***	+0-+2***
Speech Server farm and Web Server farm	+0-+2***	+0-+4***

* The web farm can either be load-balanced by the epool WebMux, which load balances the Web Components Servers (for the Office Communications Server 2007 Enterprise Edition Expanded Configuration) and/or Array of Directors, or it can have its own WebMux

** Multiple Communicator Web Access servers can be load-balanced by the epool WebMux or they can have their own WebMux(es): either one each for the internal user server array and external user server array, or one WebMux for both arrays

*** Speech Server can be load-balanced by the epool WebMux or it can have its own WebMux(es): either one each for the Speech Server farm and Web server farm, or one WebMux for both farms, or one WebMux for a farm of Speech Servers that also host the web servers

Local Perimeter Network

Topology	Solo WebMux	Dual WebMux
Consolidated Edge Topology or Single-Site Edge Topology with 1 ISA Server or other Reverse Proxy Server	0	-
Consolidated Edge Topology or Single-Site Edge Topology with 2 or more ISA Servers or other Reverse Proxy Servers	1	2
Scaled Single-Site Edge Topology, Multiple Site with Remote Site Edge Topology, or Multiple Site with Scaled Remote Site Edge Topology with 1 ISA Server or other Reverse Proxy Server	2	4
Scaled Single-Site Edge Topology, Multiple Site with Remote Site Edge Topology, or Multiple Site with Scaled Remote Site Edge Topology with 2 or more ISA Servers or other Reverse Proxy Servers	3	6
Communicator Web Access with 2 or more ISA Servers or other Reverse Proxy Servers	1*	2*

* Multiple ISA Servers or other Reverse Proxy Servers for Communicator Web Access can either be load-balanced by the same WebMux that load balances the external interface of the Edge Servers, the outer perimeter WebMux, or they can have their own WebMux

Remote Internal Network (per site)

Same as Local Internal Network

Remote Perimeter Network (per site)

Topology	Solo WebMux	Dual WebMux
Remote Site Edge Topology with 1 Web Conferencing Edge Server computer and 1 ISA Server or other Reverse Proxy Server	0	-
Remote Site Edge Topology with 2 or more Web Conferencing Edge Server computers or ISA Server or other Reverse Proxy Server	1	2
Scaled Remote Site Edge Topology	2	4
Communicator Web Access with 2 or more ISA Servers or other Reverse Proxy Servers (if Communicator Web Access is installed at remote site)	1*	2*

* The Communicator Web Access ISA Server or other Reverse Proxy Server can either be load-balanced by the same WebMux that load balances the external interface of the Edge Servers (the outer perimeter WebMux) or they can have their own WebMux

For a single-site Enterprise Edition deployment with a solo WebMux managing both the Enterprise pool and the web farm that has local and instrumented external Windows users but no remote sites and no Web-based access by external users, a minimum of three WebMuxes is required:

- One for the Enterprise Edition deployment
- Two for the Edge deployment

A remote site deployment for the above could be implemented without a WebMux if volumes are low.

For a high volume, maximum-performance, fully fault-tolerant Enterprise Edition Extended Configuration implementation with one scaled remote site and use of Communicator Web Access and Speech Server at the local site, a maximum of 24 WebMuxes is required:

- Two for the Front End Servers at the local site
- Two for the Web Conferencing Edge Servers and Array of Directors at the local site
- Two for the web farm at the local site
- Four for the Edge deployment at the local site
- Two for the Enterprise Edition Consolidated Edition deployment at the remote site
- Four for the Edge deployment at the remote site
- Four for the Communicator Web Access deployment at the local site
- Four for the Speech Server deployment at the local site

Note Office Communications Server 2007 modules not detailed in this guide may require their own WebMux or pair of WebMuxes if deployed with more than one server.

Choosing Which WebMux Models to Use

In addition to determining how many WebMuxes you require for your Office Communications Server 2007 implementation, you will need to choose which WebMux models to use. Such choices relate to:

- How many concurrent connections will Office Communications Server 2007 need to handle
- How many transactions per second will Office Communications Server 2007 need to handle
- What throughput rates are required
- What network connection speeds are required

Additionally, if you are deploying Communicator Web Access, you have the option of offloading its SSL/TLS processing from its server computers to WebMux. If you want to offload SSL/TLS processing to WebMux, you will want to determine:

- How many RSA terminations per second you need to support
- What is the maximum number of SSL connections you need to support
- Do you need to equip your WebMux with an optional SSL acceleration card and, if so, which model

There are currently three WebMux models available, which differ primarily based on how much traffic they can handle, at what throughput rates, and how many SSL/TLS transactions they can handle and at what throughput rates. Performance and capacity characteristics of the three WebMux models are shown in the Table 6; SSL/TLS offloading characteristics are shown in Table 7.

Table 6: WebMux Performance Characteristics

Characteristic	481S	591SG	680PG**
Maximum concurrent connections*	1,440,000	2,880,000	5,760,000
Maximum transactions per second	15,000	50,000	200,000
Maximum throughput per second	200 MBits	1 GBits	4 GBits
Maximum Internet link speed	2 X T3	1.5 X OC-12	1.5 X OC-12

* The metrics shown are for NAT and Transparent networking mode. Out-of-path mode offers higher throughput.

** To achieve the performance numbers shown, switches deployed with WebMux must support LACP protocol.

Table 7: **WebMux SSL/TLS Offloading Characteristics**

Characteristic	481S	591SG	680PG
Maximum 1024-bit RSA terminations per second (round trip)	120	250, 1200**, 2400***	2000, 3000***
Maximum SSL connections	10,000	30,000	50,000

** With CAI-RSA3500 option card

*** With CAI-RSA7000 option card

WebMux does not impose limitations as to the number of farms and servers any WebMux can handle, nor does it impose site or user licensing limits. Decisions about capacity for WebMux can be based strictly on traffic flow.

Also, in a paired WebMux configuration there is not a requirement that the secondary WebMux be the same model as the primary WebMux. Therefore, you can save costs by deploying a less expensive WebMux model as the secondary (and thereby experience lesser performance and capacity should the primary WebMux be taken out for service) if that meets your performance objectives.

Installing and Configuring WebMux for Deployment with Office Communications Server 2007

Introduction

You need to consider WebMux deployment in the context of your Office Communications Server 2007 deployment. The Office Communications Server 2007 documentation gives details and recommendations about load balancer deployment; this section augments that information and relates it to the WebMux product.

Deploying WebMux as part of an Office Communications Server 2007 implementation involves the following activities, covered in this chapter:

- Preparing for WebMux deployment. This includes deciding which WebMux models and how many, ensuring prerequisites are met, ensuring that companion hardware is available, establishing your deployment process, choosing which networking topology, and determining information that will be required for configuration.
- Setting up the infrastructure for WebMux deployment. This includes configuring DNS, firewalls, routers, and in some cases servers.
- Installing WebMux. This requires setup in the data center and network, and potentially at remote locations, of one or more WebMuxes. This includes installing WebMux in the rack, powering it, and connecting it to the network.
- Configuring WebMux. This includes setting the IP address of each WebMux (for those WebMuxes that were not factory preconfigured) and the configuration settings for each.
- Testing WebMux. This includes performing test transactions to ensure correct behavior and, if desired, crashing servers, etc. to ensure failover is working.

Preparing for WebMux Deployment

Preparing for WebMux deployment in an Office Communications Server 2007 environment includes:

- Ensuring that the proper WebMuxes are available at the each site that requires them

- Ensuring that the appropriate companion equipment (routers, switches) is available
- Making sure there are enough electrical or UPS outlets for all the new equipment and that they have sufficient capacity
- Deciding which networking mode each WebMux should operate in. For WebMuxes operating in NAT mode, determine whether WebMux's firewall needs to be disabled
- Determining which scheduling methods are most suitable for allocating traffic in each WebMux farm. If you are using a WEIGHTED scheduling method, you will also need to determine what weights to use for each server computer
- Determining what VIP to use each WebMux, farm, and server, as well as VIPs for MAP rules
- Determining what FQDNs to configure in DNS (or hosts files) to resolve to the VIPs for the WebMux farms
- Confirming port assignments for each WebMux farm and managed servers
- Determining what weights may need to be assigned to servers within WebMux configurations to compensate for server performance differences
- Determining which farms will offload SSL/TLS termination from servers to WebMux and the certificates for those
- Determining the TCP connection timeout to impose for each WebMux, and the retry interval to impose for each service in each WebMux
- Deciding whether WebMuxes need to be enabled for protection against DoS, DDoS, and other attacks and the configurations for those
- Determining who should be notified of WebMux events and by what method

Ensure Availability of WebMuxes

Make sure you have the correct number and models of WebMux for your deployment.

Dual-configuration deployments require two WebMuxes for each instance; they can be of different models but they need to be running at the same firmware revision.

Office Communications Server 2007 remote sites require the WebMux(es) to be deployed at the remote locations.

Ensure Availability and Configuration of Companion Equipment

Depending on the deployment model, you may require additional switches, routers, hubs, and/or cables to connect your WebMux(es) to your network(s).

Review the information in this guide and in the WebMux manual to ensure that you have everything you need.

Note If you are deploying a dual WebMux configuration in Transparent mode, the switches that connect WebMux to the network must support STP (Spanning Tree Protocol), and the protocol must be enabled and the switches properly configured. If you are deploying WebMux in solo mode, STP support is not required.

Note If you are deploying WebMux model 680PG, in order to take advantage of WebMux's trunking feature to achieve full bandwidth utilization potential, the switches that connect WebMux to the network must support LACP protocol, and the protocol must be enabled and the switches properly configured to aggregate the appropriate ports properly.

Ensure Sufficient Electrical or UPS Outlets and Capacity

Each WebMux will need its own power point, as will any additional switches, routers, and/or hubs you are using to support the WebMux configuration. WebMux has a universal power supply and is shipped with a power cable with a type B (USA grounded) plug.

Set Office Communications Server 2007 Settings for WebMux

Office Communications Server 2007 servers may require configuration settings related to WebMux, as documented in the product documentation.

Generally, what is required for Office Communications Server 2007 to access its servers via WebMux is to set the FQDNs required by Office Communications Server 2007 to WebMux farm VIPs.

Note It is an Office Communications Server 2007 requirement that for each Enterprise server running the Web Components Server, you must configure IIS to allow loopback for the FQDN that resolves to the VIP of the WebMux farm that contains the server. If this is not done, Office Communications Server 2007's validation wizard will fail. Once the validation wizard has completed, the FQDN setting can be removed. Refer to Appendix D of the Microsoft® Office Communications Server 2007 Enterprise Edition Deployment Guide for more information.

Determine Labels (optional)

WebMux permits labels to optionally be specified for farm, server, and MAP rules. Except for content-based traffic management (which Office Communications Server 2007 does not use), labels are for display purposes only.

Determine Networking Mode (Dispatch Method)

WebMux can operate in three networking modes: NAT, Out-of-Path, and Transparent.

The networking modes Office Communications Server 2007 supports for load balancing are NAT and Transparent. The preferred networking mode is Transparent, since it allows

the servers to be configured with external IP addresses, but this mode requires STP-compatible routers and switches be used, which you may not have available.

For some Office Communications Server 2007 modules, like Speech Server, Out-of-Path mode is recommended.

You will need to set WebMux's networking mode as part of its initial setup, and you may require additional or different networking equipment depending on the networking mode chosen, so best to reach this decision early.

Refer to the sections above and to the WebMux manual for a discussion about and examples of NAT versus Transparent mode.

Note Each WebMux can operate in only one networking mode at a time, so Office Communications Server 2007 modules that require one networking mode cannot be managed by the same WebMux as those that require a different networking mode.

Determine Scheduling Methods

WebMux's scheduling method determines what algorithm WebMux will use when load balancing and traffic managing servers within a farm.

Some Office Communications Server 2007 modules need to have persistent connections enforced to meet a requirement for TCP-level affinity. WebMux offers scheduling methods that enforce persistent connections.

If you are using computers of different models or which have different inherent performance characteristics, you will want to consider using a weighted variant of these scheduling methods to compensate for differences in server power.

The recommended scheduling method to use for each WebMux farm in an Office Communications Server 2007 deployment is shown in the sample settings in Appendixes B through E.

Server Weights

When using a weighted scheduling method, you will need to assign as weight for each server computer, which is used when choosing for each farm how to skew the amount of traffic that is sent to a server based on its power to service transactions.

By default a weight of 1 is assigned; a weight value of 2 means twice as much traffic will be sent. (A weight of 0 does not mean weight is not being imposed; rather it means the server should not accept traffic.)

Table 8 below shows the effect of server weights.

Table 8: **Example of Server Weight Effect**

Server	Weight	Requests
Server 1	1	25%
Server 2	1	25%
Server 3	2	50%
Server 4	0	0% (down)

Determine VIPs and IP Addresses

There are four IP addresses that come into play when configuring WebMux, two of which are real IP addresses and two of which are VIPs.

WebMux IP Addresses

Every WebMux is a real device on the network which needs to have a real IP address, which is used primarily for WebMux access for management purposes.

If WebMux is deployed in dual mode, each WebMux is assigned its own real IP address. (In the unlikely event of a WebMux failover, the secondary WebMux automatically adopts the IP address of the primary WebMux, but for them to co-exist on the network during normal conditions they require unique IP addresses.)

Farm IP Addresses

Each farm is a virtual server on the network and is assigned a VIP. The farm's VIP effectively takes the place of a server IP address: whereas without WebMux traffic could be routed to a server by its IP address, routing traffic to a WebMux farm's VIP causes it to route to one of the servers that is a member of the farm.

The VIP does not to be unique within the WebMux: multiple farms can have the same VIP, as WebMux routes traffic based on the combination of VIP and port number. If multiple farms in a WebMux have identical VIPs, WebMux will choose the farm that is configured with the port to which the traffic is directed (whether the port was set for the farm, a MAP rule, or a server configuration). For this reason, the combination of VIP and port needs to be unique within each WebMux.

MAP Rule IP Addresses

Each MAP rule within a farm requires a VIP. These do not need to be unique, but the combination of its VIP and port value needs to be unique within the WebMux.

Server IP Addresses

The IP address for each real server computer that is a member of a WebMux farm must be specified in WebMux.

If WebMux's networking mode is NAT, the servers being load balanced need to be on a separate network segment than the computers outside the WebMux and therefore their IP addresses (and default gateway settings) may need to be changed.

Server IP addresses should be Internet non-routable so that the source address from the Internet does not conflict with the IP address on the LAN in which the server is networked.

Determine FQDNs

Office Communications Server 2007 accesses the servers that are members of WebMux farms by FQDN. This requires that a DNS A Record or hosts file entry is created for each WebMux farm.

Confirm Port Assignments

You will need to assign a main port for each farm and, for some farms, additional ports, via MAP rules.

If at any point you decide to reassign any ports on any servers that are being load balanced and traffic managed by WebMux, you will need to adjust WebMux settings accordingly.

Decide on Attack Protection

For WebMuxes in the perimeter network and others that could receive outside traffic, and/or to safeguard against infected computers internally, you will want to consider enabling WebMux's protection from DoS, DDoS, and other attacks.

Refer to the WebMux manual for more information.

Setting up the Infrastructure for WebMux Deployment

Setting up the required network infrastructure for WebMux deployment in an Office Communications Server 2007 environment includes:

- Set server IP addressing, as required by the chosen networking mode
- Necessary DNS configurations (for FQDNs)
- Necessary firewall configurations
- Necessary Active Directory configurations

Set Server Network Addressing

Depending on which networking mode you are deploying WebMux in, you may or may not need to take special considerations when assigning IP addresses to Office Communications Server 2007 server computers.

If you are using Transparent mode, you can use whatever IP addresses you want for the Office Communications Server 2007 server computers.

If you are using NAT mode and if the Office Communications Server 2007 servers have external IP addresses assigned they will need to be reassigned with internal IP addresses on the LAN where they are connected (behind the WebMux) and also their default gateway settings will need to be changed to point to the server LAN's gateway device.

If you are using Out-of-Path mode and the server is a member of a farm enabled for SSL/TLS termination, you will need to set the server's default gateway to point to the LAN gateway IP address configured in the WebMux. You will also need to attach and configure a loopback adapter to every server being load-balanced by WebMux.

Refer to the discussion about Networking Mode in this section and also to the WebMux manual.

Farm Network Addressing

Each WebMux farm must be assigned an IP address – a virtual IP address, or VIP – when it is created. Transactions can be routed to the servers that belong to the farm by the farm's VIP (and via an FQDN that resolves to the VIP, configured in a DNS server or hosts file).

Set DNS or Hosts File Configurations

Whereas servers can have host names, WebMux farms do not; therefore, it is necessary to use either DNS A records or hosts file entries to equate an FQDN or host name with a WebMux farm. Such DNS or hosts file configuration needs to resolve a unique FQDN to the VIP of a WebMux farm.

Set Firewall Rules

If there is a firewall between WebMux and an Internet router, firewall rules must be defined for to allow both WebMux and each farm to communicate with the Internet on all ports.

For WebMux, the IP address is its assigned IP address (done at WebMux installation time); for each farm, the IP address is the farm's VIP (done at farm creation time).

Firewall rules must also be set for Office Communications Server 2007 servers. Refer to the Office Communications Server 2007 manuals for information about firewall settings for an Office Communications Server 2007 deployment.

Installing WebMux

WebMux is designed to be installed in a rack and connected to power, networks, and devices in the same manner as other network devices. It is made network accessible by setting its IP address, which for WebMux models 481S and 591SG is done via a keypad and for model 680PG is done via a serial interface connection.

Note WebMux can be factory preconfigured, with its networking parameters already set, as a free option when ordering.

Installing WebMux into your data center includes:

- Putting it in the rack
- Connecting it to the network and, if installing in a dual configuration, connect the two WebMuxes together
- Setting its IP address
- Checking the firmware revision

Rackmount WebMux(es)

WebMux has a standard 1U rack-mountable chassis. Put one or both WebMuxes in the rack.

Connect WebMux(es)

WebMux needs to be connected to both the network in front of and behind it via appropriate switches. If you are deploying WebMux in a dual configuration, you will also need to connect both WebMuxes to the network as well as together.

Connect to Network

Depending on the WebMux model you have, there will be one or more Ethernet ports for Router LAN and Server LAN. These ports are not interchangeable.

For WebMux models 481S and 591SG, the Router LAN port is the leftmost RJ45 socket on the back of the WebMux and the Server LAN port is the rightmost RJ45 socket. For WebMux model 680PG, “LAN 1” to “LAN 4” on the front of WebMux are Router LAN ports, while “LAN 5” to “LAN 7” are Server LAN ports.

If you are deploying WebMux model 680PG with LACP-capable switches to maximize bandwidth potential via WebMux’s trunking capability, ensure that LACP is enabled on the switches and that the switches are properly configured.

Connect Two WebMuxes in Dual Configuration

If you are deploying WebMux in a dual configuration, connect them both to the network, as described above.

Also connect them together via the BACKUP WEBMUX port, either via a crossover cable or a regular cable with a hub.

For WebMux model 680PG, the Backup LAN port is “LAN 8” on the front of the WebMux.

If you are deploying WebMux in dual configuration with Transparent networking mode via STP-capable switches, ensure that STP is enabled on the switches and that the switches are properly configured.

Set WebMux Network Addressing

Depending on which model WebMux you have, you either set WebMux's IP address, netmask, and gateway via the keypad or via a serial connection.

If you are configuring a pair of WebMuxes, you will need to set a different IP address for each one. (Should the primary WebMux failover to the secondary due to a fault while in operation, the secondary WebMux will automatically adopt the IP address and other properties of the primary. But for initial configuration, and for both WebMuxes to actively co-exist on the network, each needs its own unique IP address.)

Refer to the WebMux manual for more information.

Check WebMux Firmware Revision

Depending on which model WebMux you have, WebMux's firmware revision number was either displayed in the front-panel LCD or you will need to browse to `http://WebMux_ip_address:24t/cgi-bin/rec` for IPV4 or `http://[WebMux_ip_address]:24/cgi-bin/rec` for IPV6 and use WebMux's Management Console to display it. Refer to the WebMux manual for more information.

Ensure the firmware release is version 8.2.07 or later. If the WebMux firmware release is not current, contact CAI Networks technical support to get an update.

If you are implementing WebMux in a dual configuration, both WebMuxes must be on the same firmware release.

Configuring WebMux

Once you have a WebMux set up and accessible by its browser-based Management Console, you are ready to start configuring it.

Each WebMux must be configured independently except for in the case of a dual configuration, where the primary WebMux's settings are automatically propagated to the secondary. Except for the dual case, WebMuxes do not talk to and are not dependent on each other, so there is no need to configure them all at the same time.

WebMux configuration tasks include:

- Configuring the basic and administrative settings, notification, logging, and other settings for each WebMux
- Configuring the farms, their servers, and MAP rules for each WebMux
- Changing "TCP idle timeout" as required
- Changing "Reset stranded TCP connection" as required

Before you start configuring WebMux, make sure you:

- Have browser-based access to WebMux's Management Console and the know the login username and password
- Know what farms you will be creating

- Have VIPs to assign to each farm
- Know which servers will be members of each farm and their relative weights (if the WebMux scheduling method you are using uses weights)
- Know what MAP rules will be created for each farm
- Know which health-checking algorithms need to be adjusted and the settings for those
- Know which WebMuxes need DoS and DDoS attack protection and the settings for those
- Know the email address to send WebMux notifications to
- Will use SNMP logging or not and, if so, details of the syslog server

WebMux Management Console

WebMux configuration is done via WebMux’s browser-based Management Console.

Here is what the Main Console for finished setup for the Front End Servers in the front end WebMux looks like Figure 3.

Figure 3: WebMux Main Management Console configured for Enterprise pool

WebMux™ High Availability Solution
 built-in scalability webservers loadbalancer
 CAI Networks, Inc Nov 6 15:35:04 2007 up since Nov 6 15:21:10 2007 Help

frontend.contoso.com cpu: 0%, mem: 7%
 IP 10.0.0.50 MAC 00:e0:81:76:5a:93 IP 10.1.0.50 MAC 00:e0:81:76:5a:92

	type	service	IP address	port	status	conn	conn/s	pkt/s		
☐ 1.	LC (P) farm	tcp	OCS_FE	10.0.0.100	5060	5 servers	ALIVE	0	0	0
2.		tcp_nohc	OCS_FE_MAP_2	10.0.0.100	135					
3.		https	OCS_FE_MAP_3	10.0.0.100	443					
4.		tcp_nohc	OCS_FE_MAP_4	10.0.0.100	444					
5.		tcp	OCS_FE_MAP_1	10.0.0.100	5061					
6.	server		OCS_FE_SRV_1	10.1.0.10	same	weight 1	ALIVE	0	0	0
7.	server		OCS_FE_SRV_2	10.1.0.11	same	weight 1	ALIVE	0	0	0
8.	server		OCS_FE_SRV_3	10.1.0.12	same	weight 1	ALIVE	0	0	0
9.	server		OCS_FE_SRV_4	10.1.0.13	same	weight 1	ALIVE	0	0	0
10.	server		OCS_FE_SRV_5	10.1.0.14	same	weight 1	ALIVE STANDBY	0	0	0
grand totals:								0	0	0

© 1997-2007 CAI Networks. All rights reserved.

In the above example, line 1 is the farm entry, lines 2 through 5 are MAP rule entries, and lines 6 through 10 are server entries. The farm has four active servers and one hot standby server.

Log into WebMux via the Management Console

Browse to `http://WebMux_ip_address:24/cgi-bin/login` for IPv4 or `http://[WebMux_ip_address]:24/cgi-bin/login` for IPv6 and login as “superuser” with the

factory default password of “superuser” (or whatever you may have changed the password to previously).

Change the password for security purposes and log back in.

Set WebMux Basic Settings

WebMux’s basic settings include WebMux’s name and IP address on the network, WebMux’s networking mode, and whether the WebMux deployment is solo or dual.

Depending upon which WebMux model you are configuring, you may have entered some of the basic settings via the front panel keypad and you can add additional settings via WebMux’s browser-based Management Consoler at http://WebMux_ip_address:24/cgi-bin/rec for IPv4 or [http://\[WebMux_ip_address\]:24/cgi-bin/rec](http://[WebMux_ip_address]:24/cgi-bin/rec) for IPv6.

Refer to the WebMux manual for more information.

WebMux Host and Domain Name

In the basic settings, you will configure a host and domain name for each WebMux. Note that those, and WebMux’s IP address, are not relevant to the Office Communications Server 2007 configuration: the IP addresses and FQDNs that Office Communications Server 2007 will be using are set when configuring farms in WebMux.

If you are configuring a pair of WebMuxes in a dual configuration, you do not need to configure the secondary WebMux – the configuration settings from the primary WebMux will propagate to the secondary.

Networking Mode

The “dispatch method” setting determines which networking mode WebMux will operate in. Office Communications Server 2007 supports NAT and Transparent mode, while for other Office Communications Server 2007 modules, like Speech Server, Out-of-Path mode is recommended.

Refer to the above and to the WebMux manual for a discussion on networking modes.

Set WebMux Administration Settings

WebMux’s Administration settings include who to email and/or page when problems arise, syslog settings, and timeout adjustments. To get to WebMux’s Administration screen, login to WebMux via http://WebMux_ip_address:24/cgi-bin/login for IPv4 or [http://\[WebMux_ip_address\]:24/cgi-bin/login](http://[WebMux_ip_address]:24/cgi-bin/login) for IPv6 and hit the “Setup” button.

Refer to the WebMux manual for more information.

Server LAN Gateway IP Address

If you are deploying WebMux in NAT or Out-of-Path networking mode, you will need to configure a Server LAN Gateway IP Address in WebMux that points to the device

(firewall, router, etc.) that is acting as the gateway for the LAN on which the Office Communications Server 2007 servers are connected.

Adjust Stranded TCP Connection Reset setting

WebMux is capable of resetting stranded TCP connections as an option. WebMux's default may need to be overridden for certain Office Communications Server 2007 modules.

To change this setting WebMux-wide, use the "reset stranded TCP connections" setting in WebMux's Administration screen.

Refer to the WebMux manual for information about that.

Enable Attack Protection

For WebMuxes that face externally (such as the outer perimeter WebMux), it is recommended that you enable WebMux's attack protection feature, which is capable of blocking DoS and DDoS attacks.

You may also wish to enable attack protection for WebMux(es) in your internal network if you think that exploits may penetrate your network defenses.

Use the Security Settings screen in the WebMux's Management Console to set attack protection for WebMuxes that receive external traffic. You can get to the Security Settings screen by browsing to `http://WebMux_ip_address:24/cgi-bin/sec` for IPv4 or `http://[WebMux_ip_address]:24/cgi-bin/sec` for IPv6 and login as "superuser" with the factory default password of "superuser" (or whatever you may have changed the password to previously).

Refer to the WebMux manual for information about attack protection if desired, as well as the Step-by-Step instructions at the end of this chapter.

Add Existing or Generate New SSL/TLS Certificates

If you are using WebMux to offload SSL/TLS processing from servers, the SSL/TLS certificate(s) that would otherwise reside in the servers need(s) to be held in WebMux.

If you already have certificates generated for SSL for Communicator Web Access, you can add them via cut and paste into WebMux's Add Keys screen.

If you do not already have certificates and would like to generate them (via CSR), you can do that from within WebMux's Management Console. Refer to the WebMux manual for more information.

You can add SSL and TLS certificates into WebMux via the Add Keys screen of the WebMux Management Console. To assign certificates to farms, use the Add Server or Change Server screen and select the already-present certificate from the listbox.

Add Farms

Adding farms into WebMux is done with the Add Farms screen in WebMux's Management Console. The settings for adding farms are:

IP address	The virtual IP address assigned for the farm. (The VIP is resolved by an FQDN configured in DNS or hosts file.)
label	An optional value for display purpose only. Suggested Label values are in Appendices B through E but you can assign any value you choose.
port number	<p>The main port for the farm. If there is a well-known port for the chosen Service, its port number is automatically filled.</p> <p>If WebMux will be terminating SSL/TLS traffic for this farm, specify the appropriate clear-traffic port rather than an encrypted traffic port (e.g., 80 rather than 443 for HTTP traffic).</p> <p>Refer to Table 12 for the ports used by Office Communications Server 2007 for each component and module, and to Appendices B through E for sample MAP rule settings for various Office Communications Server 2007 configurations and topologies.</p> <hr/> <p>Note If you need to assign multiple ports for a farm, for servers that handle traffic on multiple ports, you will need to assign one port as the farm's port and create MAP rules for the additional ports.</p> <hr/>
service	<p>The main service (protocol) for the farm, chosen from a listbox.</p> <p>Refer to Table 10 for the services recommended for each Office Communications Server 2007 component and module, and to Appendices B through E for sample farm settings for various Office Communications Server 2007 configurations and topologies.</p>
scheduling method	<p>The scheduling method is the algorithm used by WebMux to determine how traffic is load-balanced and traffic-managed among the servers in the farm.</p> <p>Refer to Table 13 for the scheduling methods recommended for each Office Communications Server 2007 component and module, and to Appendices B through E for sample scheduling method settings for various Office Communications Server 2007 configurations and topologies.</p>

SSL termination	To have WebMux terminate SSL/TLS traffic for this farm, select the already-configured key that should be used; otherwise select “(none)” from the listbox.
SSL port	If SSL/TLS termination is being performed by WebMux on behalf of servers in this farm, this is the port that will receive encrypted traffic. (The clear-traffic port to which traffic will be sent to the servers is specified in the Port field.)
Block non-SSL access to the farm	If WebMux is performing SSL/TLS termination for this farm, this option if set to ‘YES’ causes WebMux to block incoming traffic that is not encrypted.
Tag SSL-terminated HTTP requests	If WebMux is performing SSL/TLS termination for this farm, this option if set to ‘YES’ causes WebMux to add a specific MIME header to identify HTTP versus HTTPS transactions.

Refer to the WebMux manual for more information about and examples of creating farms. Refer to Appendix B and C for information about what farms need to be created for various Office Communications Server 2007 configurations.

Add MAP Rules

Adding MAP rules for a farm is done with the “add IP address/ports” screen in WebMux’s Management Console. The settings for adding MAP rules are:

IP address	A value that when combined with the specified Port is unique within the WebMux. (Normally using the farm’s VIP is fine.)
label	An optional value for display purpose only. Suggested Label values are in Appendices B through E but you can assign any value you choose.
port number	The port for the MAP rule. This is treated as an additional port that will be load-balanced and traffic-managed for servers that are members of the farm. If a range of ports requires load balancing, specify “0” to cause WebMux to load-balance and traffic-manage all ports for the farm which were not explicitly specified. Refer to Table 12 for the ports used by Office Communications Server 2007 for each component and module, and to Appendices B through E for sample MAP rule settings for various Office Communications Server 2007 configurations and topologies.
service	The service (protocol) for the MAP rule, chosen from a listbox.

Refer to Table 12 for the services used by Office Communications Server 2007 for each component and module, and to Appendices B through E for sample MAP rule settings for various Office Communications Server 2007 configurations and topologies.

SSL termination	If WebMux should terminate SSL/TLS traffic for the port specified for the MAP rule you are adding, select the certificate that should be used; otherwise, select '(none)' from the listbox. If you selected a value other than '(none)' complete the next prompts and ensure you have setup the necessary SSL/TLS configurations.
SSL port	If SSL/TLS termination is being performed for the port specified for the MAP rule you are adding, specify the port will receive encrypted traffic. (The clear-traffic port to which traffic will be sent to the servers is specified in the Port field.)
Block non-SSL access to the farm	If WebMux is performing SSL/TLS termination for this farm, this option if set to 'YES' causes WebMux to block incoming traffic that is not encrypted.
Tag SSL-terminated HTTP requests	If WebMux is performing SSL/TLS termination for this farm, this option if set to 'YES' causes WebMux to add a specific MIME header to identify HTTP versus HTTPS transactions.

Refer to the WebMux menu for more information about and examples of adding MAP rules. Refer to Appendices B through E for information about what MAP rules need to be created for various Office Communications Server 2007 configurations, topologies, and modules.

Add Servers

Adding servers as members of a farm is done with the "add servers" screen in WebMux's Management Console. The settings for adding servers are:

IP address	The real IP address of the server computer.
label	An optional value for display purpose only. Suggested Label values are in Appendices B through E but you can assign any value you choose.
port number	If port redirection is required, specify the port number on the server to which traffic should be redirected; otherwise, specify "same".
weight	Specify a value between 1 and 100 based on server power. This value is only used if you have chosen a weighted scheduling method for the farm.
run state	Choose from the listbox whether you want the server to be in active or a hot standby.

Note: There is no requirement that servers be members of only one farm. In Office Communications Server 2007, there are cases in which servers are members of multiple farms.

Refer to the WebMux manual for more information about and examples of adding MAP rules. Refer to Appendices B through E for information about what MAP rules need to be created for various Office Communications Server 2007 configurations, topologies, and modules.

Adjust Service-Level Idle Timeout

The TCP idle timeout is the interval that WebMux will wait before retrying a failed protocol on a server.

WebMux's factory default TCP idle timeout needs to be overridden for some Office Communications Server 2007 components and modules, as shown in Table 10. The TCP ideal timeout is a property of WebMux's health checking performed for each service (protocol).

Health checking settings are adjustable by service (protocol) for each WebMux, and all servers that are members of farms configured for a WebMux are governed by a common set of health checking settings.

To adjust the TCP idle timeout retry interval for a service for a WebMux, from the WebMux's Main Management Console, click on the service and you can adjust its TCP idle timeout.

Refer to the WebMux manual for more information about this feature.

Step-by-Step Setup

This is a summary step-by-step setup guide for WebMux in an Office Communications Server 2007 environment. Each WebMux must be configured independently. Discussion about the steps below can be found above.

All the steps below are not required for all WebMux configurations, as some features are required for some types of deployments and others not. Steps are shown in the proper sequence, with comments therein that describe in what scenarios certain steps are required.

Rack Mount WebMuxes

This step is necessary for every WebMux that will be deployed at any site. If WebMux is being deployed in dual mode, this step is required for both the primary and secondary WebMux.

1. Rack mount WebMux and connect it to the network. If WebMux is being deployed in dual mode, connect the two WebMuxes together.

Set WebMux's Networking Attributes

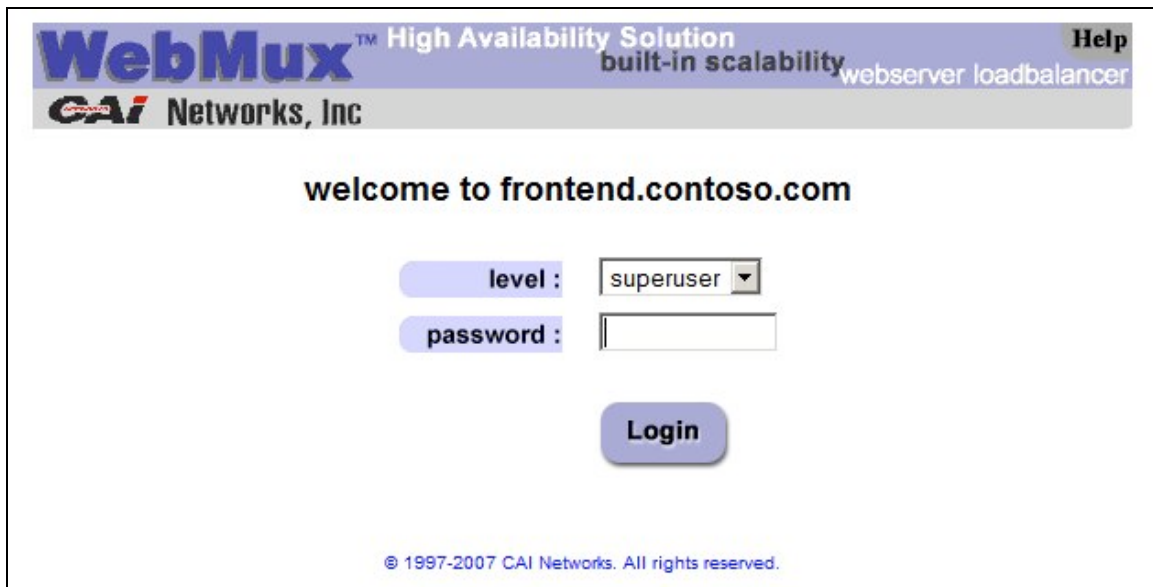
This step is necessary for every WebMux that will be deployed at any site. If WebMux is being deployed in dual mode, this step is required for both the primary and secondary WebMux.

2. If you are deploying WebMux model 481S or 591SG, set WebMux's hostname, networking mode, and IP addresses and netmasks for the Router LAN, Server LAN, Server LAN Gateway, and external gateway via the front panel keypad and LCD. If you are deploying WebMux model 680PG, connect it to a PC via a console cable to set those values.

Set WebMux Administrative Settings

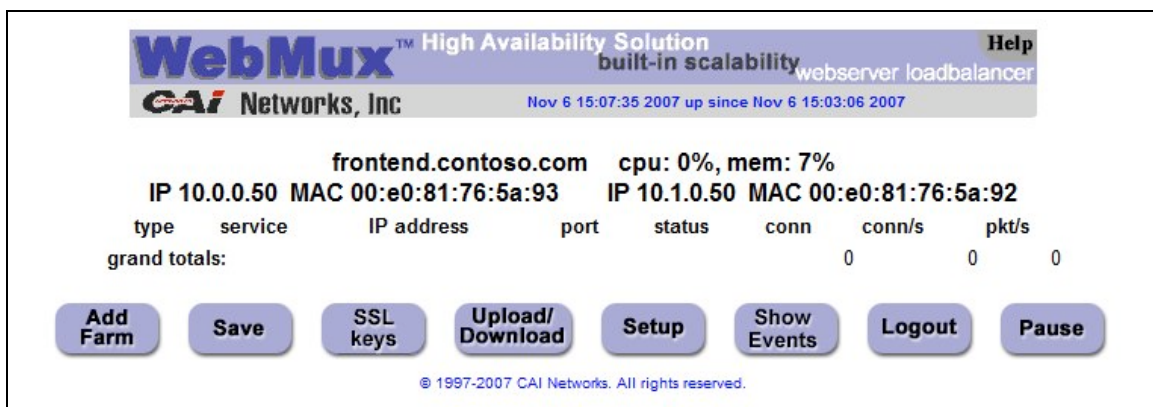
This step is required for every primary WebMux.

3. Invoke WebMux's Main Management Console by browsing to `http://WebMux_ip_address:24/cgi-bin/login` for IPv4 or `http://[WebMux_ip_address]:24/cgi-bin/login` for IPv6. The login screen will be displayed:



The screenshot shows the WebMux login interface. At the top, there is a header with the WebMux logo, the text "High Availability Solution built-in scalability", and "webserver loadbalancer". Below the header, it says "welcome to frontend.contoso.com". There are two input fields: "level" with a dropdown menu set to "superuser" and "password" with an empty text box. A "Login" button is centered below the fields. At the bottom, there is a copyright notice: "© 1997-2007 CAI Networks. All rights reserved."

- a. Select a login level of 'superuser' and specify the factory password of "superuser". The Main Management Console will be displayed, reflecting WebMux's basic settings:



The screenshot shows the WebMux Main Management Console. At the top, there is a header with the WebMux logo, the text "High Availability Solution built-in scalability", and "webserver loadbalancer". Below the header, it says "Nov 6 15:07:35 2007 up since Nov 6 15:03:06 2007". The main content area displays system information: "frontend.contoso.com cpu: 0%, mem: 7%", "IP 10.0.0.50 MAC 00:e0:81:76:5a:93", and "IP 10.1.0.50 MAC 00:e0:81:76:5a:92". Below this, there is a table with columns: "type", "service", "IP address", "port", "status", "conn", "conn/s", and "pkt/s". The "grand totals" row shows "0" for "conn", "0" for "conn/s", and "0" for "pkt/s". At the bottom, there are several buttons: "Add Farm", "Save", "SSL keys", "Upload/Download", "Setup", "Show Events", "Logout", and "Pause". At the very bottom, there is a copyright notice: "© 1997-2007 CAI Networks. All rights reserved."

- b. Click on the 'Setup' button to set the Administration settings for this WebMux. The Administration Settings screen will be displayed:

Please enter information below. Use ":" as divider for multiple entries, except use "." as divider for IPv6 addresses. Multiple entries are not allowed for the server gateway, control ports, mail server, or warning threshold. The items with * take effect on next restart.

allowed remote host IPs	<input type="text"/>
allowed remote host IPv6 IPs	<input type="text"/>
* TACACS+ server configuration	<input type="text"/>
dialout prefix (blank if none)	<input type="text"/>
pager phone numbers	<input type="text"/>
email server IP address for notification	10.0.0.15
email addresses for notification	ITops@contoso.com
UDP syslog server IP address for notification	10.1.0.199
* server gateway IP address	0.0.0.0
* WebMux http control port	24
* WebMux https control port	35
* WebMux SNMP UDP port	161
* WebMux diagnostic ports	77:87
connection warning threshold	0
* least significant bits in client IP address to ignore for persistent connections	0 (specific IP address) ▾
ICMP packet input policy	accept ▾
* forwarding policy	deny ▾
* front network verification	TCP connection ▾
front network verification address	<input type="text"/>
send gratuitous ARP replies for farms	yes ▾
* persistence timeout	20 min ▾
connection timeout	20 min ▾
URL for custom service check	/cgi-bin/custom
UDP NTP time server IP address	164.67.62.194
reset stranded TCP connections	yes ▾

Reboot **Shut Down** **Change Password** **Change Pin** **Set Clock** **Confirm** **Cancel**

© 1997-2007 CAI Networks. All rights reserved.

To make changes:


- c. Set the settings as desired.
- d. Hit the 'Confirm' button to confirm the settings.

In the above example, we are specifying that notifications should be emailed via an email server at 10.0.0.15 to ITops@contoso.com and that syslog entries should be sent to a syslog server at 10.1.0.199. We are also setting the default connection timeout for all sessions connecting through this WebMux to servers being load-balanced and traffic-managed by this WebMux to 20 minutes.

Setup SSL/TLS Certificates

This step is required if any of the servers this WebMux will load-balance and traffic-manage will offload SSL/TLS processing to WebMux. For Office Communications Server 2007, this is limited to the Communicator Web Access and Speech Server.

4. If this WebMux will perform SSL/TLS offloading for any farm, you will need to set up whatever keys and certificates are required for all such farms. From the Main Console, click on the 'SSL keys' button to get to the "SSL termination management" screen:



The screenshot shows the WebMux interface for SSL termination management. At the top, there is a header with the WebMux logo, the text "High Availability Solution built-in scalability", and a "Help" button. Below the header, the title "SSL termination management" is centered. A instruction "Click on its link to manage a key." is displayed. A table lists 11 keys, each with a link to manage it, a count of farms (all 0), and a status "(key and certificate unset)".

key	farms	
key 1	0	(key and certificate unset)
key 2	0	(key and certificate unset)
key 3	0	(key and certificate unset)
key 4	0	(key and certificate unset)
key 5	0	(key and certificate unset)
key 6	0	(key and certificate unset)
key 7	0	(key and certificate unset)
key 8	0	(key and certificate unset)
key 9	0	(key and certificate unset)
key 10	0	(key and certificate unset)
key 11	0	(key and certificate unset)

key 24	0	(key and certificate unset)
key 25	0	(key and certificate unset)
key 26	0	(key and certificate unset)
key 27	0	(key and certificate unset)
key 28	0	(key and certificate unset)
key 29	0	(key and certificate unset)
key 30	0	(key and certificate unset)
key 31	0	(key and certificate unset)
key 32	0	(key and certificate unset)

Or choose encryption protocols allowed.

encryption protocols

SSLv2, SSLv3, TLSv1

Confirm

Cancel

© 1997-2007 CAI Networks. All rights reserved.

To set up a new SSL or TLS key:

- a. Click on an unset key to set a key and certificate for it.

You will be taken to the 'SSL key management' screen for the key you have chosen:

WebMux™ High Availability Solution
built-in scalabilityHelp
webserver loadbalancer
CAI Networks, Inc

SSL key 1 management

This key and certificate chain are not currently used for SSL termination. You may change this key or certificate chain using the dropdown menus. You may either let WebMux generate a new key or paste in a new private key. You may paste in a new certificate chain. If you wish to let WebMux generate a new private key, please select the key length from the dropdown menu. When the WebMux generates a new key for you, it will also generate a matching certificate request (not an actual certificate). Please be prepared to fill in the necessary information for such a request.

You may not use a new key until you have pasted in a matching signed certificate chain. You may paste a new certificate chain any time before the key is put into use.

Some certification authorities issue a certificate chain consisting of a single certificate. Some certification authorities issue a chain consisting of multiple certificates. Often the certificate chain consists of a server certificate and an intermediate certificate. In this case the server certificate should come first, and then the intermediate certificate. (The root certificate for the certification authority itself need not be included.)

private key: Oct 03, 2005 21:18:58 GMT

```
cwaVIP.contoso.com 1024-bit private key
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDPqN6uvzVgI9eOiZtYIMMjd2nnt8TqukqUxqvYmdj+5jfn7Axj
lOnyiHgt+uflNqz6ifCdx8jZuEIIB5uhPuCLoO4xYNI15WinaNIgzjXAdzOPliqB
```

certificate: Oct 03, 2005 21:19:42 GMT

```
cwaVIP.contoso.com 1024-bit certificate
-----BEGIN CERTIFICATE-----
MIIDaDCCAtGgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBhTELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbgG1mb3JuaWEeEjAQBgNVBAcTCVNhbnRhIEFuYTEbMBkGA1UE
```

© 1997-2007 CAI Networks. All rights reserved.

- b. Paste a value for the key into the 'private key' box.
- c. Select 'use new key pasted in' from the private key listbox.
- d. Paste a value for the certificate into the 'certificate' box.
- e. Select 'use new key pasted in' from the certificate listbox.
- f. Hit the "Confirm" button to save the certificate settings.


In the above example, we are setting up a TLS key and certificate for Communicator Web Access by pasting in a 1024-bit TLS key and certificate having a subject name of "cwaVIP.contoso.com" (WebMux automatically determines the certificate type and size.)

5. Repeat step 7 for all keys/certificates required for the all farms in this WebMux.
6. Hit the "Save" button from the Main Console to make the keys and certificates you have just created are durable.

Add Farm


This step is required for all WebMux deployments.

7. Hit the 'Add Farm' button from the Main Console to set up the first farm for this WebMux. This will take you to the 'add farm' screen:



High Availability Solution
 built-in scalability

Help
 webserver loadbalancer


CAI Networks, Inc

add farm

The services tcp, udp and ip (both of tcp and udp) are generic. Bad server detection is less rigorous for such services. A blank port number (default) means to use the default well-known port for the specified service. For the generic services, a port number of 0, *, or all denotes the wild specification of all ports. The wild port specification is not allowed for other services.

IP address	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="100"/>
label	<input type="text" value="OCS_FE"/>	port number	<input type="text" value="5060"/>	
service	<input type="text" value="generic (TCP)"/>			
scheduling method	<input type="text" value="least connections - persistent"/>			
SSL termination	<input type="text" value="(none)"/>	SSL port	<input type="text"/>	
block non-SSL access to farm	<input type="text" value="NO"/>			
tag SSL-terminated HTTP requests	<input type="text" value="NO"/>			

© 1997-2007 CAI Networks. All rights reserved.

To set up a new farm:

- a. Specify the values for the prompts:
- b. Hit the 'Confirm' button to create the farm.

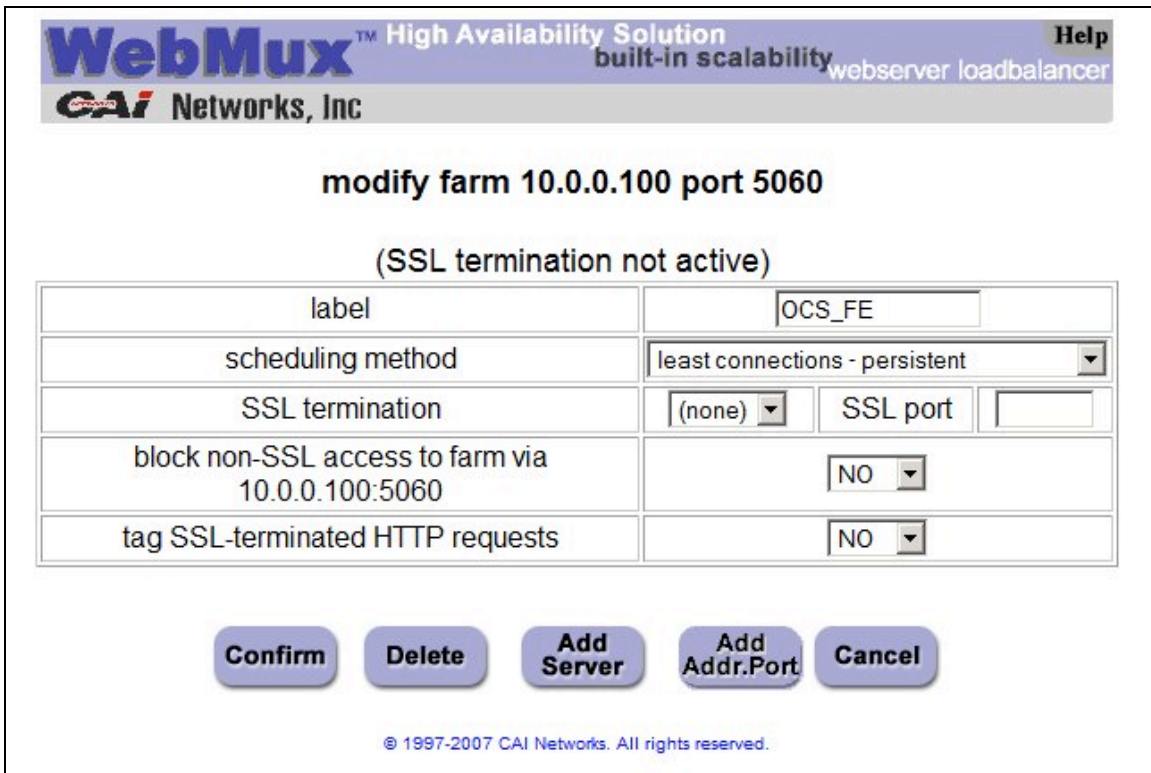
In the above example, we are setting up a Front End Server farm for an Enterprise Consolidated deployment with a virtual server address of 10.0.0.100 and a label of "OCS_FE", and we are choosing a service of 'generic (TCP)', specifying that it should use port 5060, and choosing a scheduling method of 'least connections, persistent'. Because WebMux will not be performing SSL/TLS termination for the servers in this farm, we are leaving the default of '(none)' for that function. (If we were setting up a farm for Communicator Web Access or Speech server, we could instead choose the appropriate SSL/TLS certificate to use for encryption and decryption, and we would also specify a port appropriate for unencrypted traffic, e.g. 80 instead of 443).

You will automatically be taken back to the main screen.

Add MAP Rules

This step is required for all WebMux farms for which the servers communicate on multiple ports.

8. The servers in this farm communicate on multiple ports, and the health of the protocols that run on all those ports should be considered en masse to determine whether a server is capable of handling traffic. For this, we need to create MAP rules to identify the various ports. From the main screen, click VIP on the farm you are setting up to go to the 'modify farm' screen:



WebMux™ High Availability Solution **Help**
CAI Networks, Inc. built-in scalability webservers loadbalancer



modify farm 10.0.0.100 port 5060
(SSL termination not active)

label	OCS_FE
scheduling method	least connections - persistent
SSL termination	(none) SSL port
block non-SSL access to farm via 10.0.0.100:5060	NO
tag SSL-terminated HTTP requests	NO

Confirm **Delete** **Add Server** **Add Addr.Port** **Cancel**

© 1997-2007 CAI Networks. All rights reserved.

From the 'modify farm' screen, click on the 'Add Addr.Port' button to get to the 'add IP address/port' screen to set up the first MAP rule for this farm:

 High Availability Solution built-in scalability webserver loadbalancer				Help
				
add IP address/port farm: 10.0.0.100:5060				
IP address	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="100"/>
label	<input type="text" value="OCS_FE_MAP_1"/>		port number	<input type="text" value="5061"/>
service	<input type="text" value="generic (TCP)"/>			
SSL termination	<input type="text" value="(none)"/>		SSL port	<input type="text"/>
block non-SSL access to farm	<input type="text" value="NO"/>			
tag SSL-terminated HTTP requests	<input type="text" value="NO"/>			
<input type="button" value="Confirm"/> <input type="button" value="Cancel"/>				
<small>© 1997-2007 CAI Networks. All rights reserved.</small>				

To add a MAP rule for the current farm:

- a. Specify the values for the prompts.
- b. Hit the ‘Confirm’ button to save the MAP rule.

In the above example, we are configuring a MAP rule labeled “OCS_FE_MAP_1” to add port 5061 to the server configurations in this farm using a service of ‘generic (TCP)’. (The settings for the other fields in this screen are the same as for its farm.)

9. Repeat step 12 to create additional MAP rules for the farm, as required.

Add Servers

This step is required for all WebMux farms.

10. We now need to add servers to the farm. From the ‘modify farm’ screen, click on the ‘Add Server’ button to get to the ‘add server’ screen.

WebMux™ High Availability Solution				Help
built-in scalability				webserver loadbalancer
CAI Networks, Inc				
add server				
farm: 10.0.0.100:5060				
IP address	10	1	0	10
label	OCS_FE_SRV_1		port number	same
weight				1
run state				ACTIVE

Confirm **Cancel**

© 1997-2007 CAI Networks. All rights reserved.

To set up the first server that is a member of this farm:

- a. Specify the values for the prompts.
- b. Hit the ‘Confirm’ button to save the server settings.

In the above example, we are configuring a Front End Server computer to be a member of this farm that has an IP address of 10.1.0.10, we are assigning a label of “OCS_FE_SRV_1” to it, specifying that it should use the same ports defined for the farm, and that it should be brought up in an active state.

Test the Farm

This step is recommended for all new farms, once the first server that is a member of the farm has been set up.

11. It is recommended that you now test the farm you have created before adding more servers to it. To do so, you can simply ping the farm’s VIP and ensure that the server that has been configured as a member of the farm responds, or you may wish to perform more extensive tests.

Add Additional Servers to the Farm

This step is required for each additional server that will be a member of the current farm.

12. Repeat step 14 for additional servers that are members of the current farm.
13. Hit the ‘Save’ button from the Main Console to make the farm, MAP rule, and server configurations you have just created durable.

Add Additional Farms to the WebMux

This step is required for each additional farm this WebMux will have.

14. Repeat steps 10 through 17 for each farm for this WebMux.

Set TCP Idle Timeout Retry Interval

This step is required only for Office Communications Server 2007 components for which WebMux's default TCP idle timeout retry interval is not sufficient, such as Speech Servers.

15. Set the TCP idle timeout retry interval for selected services for this WebMux by clicking on the service in the Main Console. This will go to the "modify service timeout" screen:

WebMux™ High Availability Solution
built-in scalability webserver loadbalancer
CAI Networks, Inc

modify service timeout

changing health check timeout for servers in all farms which use the service tcp ...

Please enter the number of seconds to wait for a server's response. To omit checking servers using this service altogether, enter 0.

You are using the factory default for all services. The factory timeout for the service tcp is 5 seconds.

new timeout for tcp service

Confirm **Cancel**

© 1997-2007 CAI Networks. All rights reserved.

To change the TCP timeout for the selected service:

- a. Specify the desired value in seconds.
- b. Click the 'Confirm' button.

In the above example, we are setting a retry interval of 30 seconds for the "generic (TCP)" service.

16. Repeat step 17 for other services for this WebMux for which the default retry interval is not appropriate for all the servers in all the farms in this WebMux using that service.

17. Hit the 'Save' button from the Main Console to make the settings you have just made durable.

Enable Attack Protection

This is an optional step that is recommended for WebMuxes that receive traffic from the Internet and servers that may have been comprised with malware. It enables WebMux's attack protection, which helps fend off DDoS attacks.

18. To enable attack protection for this WebMux and specify its settings, browse to http://WebMux_ip_address:24/cgi-bin/sec for IPv4 or [http://\[WebMux_ip_address\]:24/cgi-bin/sec](http://[WebMux_ip_address]:24/cgi-bin/sec) for IPv6. This will bring up the 'security settings' screen:



The screenshot shows the 'security settings for frontend.constoso.com' page. At the top, there is a header for 'WebMux High Availability Solution' with 'built-in scalability' and 'webservice loadbalancer' below it, and a 'Help' link. The CAI Networks, Inc. logo is also present. The main content area contains the following fields and instructions:

- Instructions: "Please enter information below. Use ':' as divider for multiple entries in whitelist, Multiple entries are not allowed for attack threshold."
- Field: "TCP connection attack threshold" with a text input containing the value "3".
- Field: "client whitelist for TCP attacks" with an empty text input.
- Field: "duration to block attackers" with a dropdown menu currently set to "2 hr".
- Buttons: "Confirm" and "Cancel".
- Footer: "© 1997-2007 CAI Networks. All rights reserved."

To enable attack protection to be enabled for the WebMux:

- a. Set the settings as desired.
- b. Hit the "Confirm" button.

In the above example, we are setting an attack threshold of 3 and a blocking duration of 2 hours.

19. Hit the 'Save' button to make the settings you have just made durable.

Backup WebMux Configuration

This step is recommended for each WebMux once it has been fully configured. Should the WebMux crash, or should you need to go back to an older configuration, the saved configuration can be restored within the WebMux.

20. When you have finished making all the settings for this WebMux, back up its configuration settings by hitting the 'Upload/Download' button from the Main Console to go to the 'upload/download' screen:

WebMux™ High Availability Solution **Help**
CAI Networks, Inc. built-in scalability webserver loadbalancer

upload/download

The exact download method is browser-dependent. A left click should display the configuration on screen for cut and paste. A right click should bring up a menu allowing saving the contents directly by choosing, say, "Save Link As" or "Save Target". Please be sure to use the correct file. For example do not attempt to save only the farm configuration, and use that file to restore all settings. After a file has been successfully downloaded, please push Cancel button below if you are finished.

Download farm/server information from WebMux: [Click here](#) to download farm and server configuration.

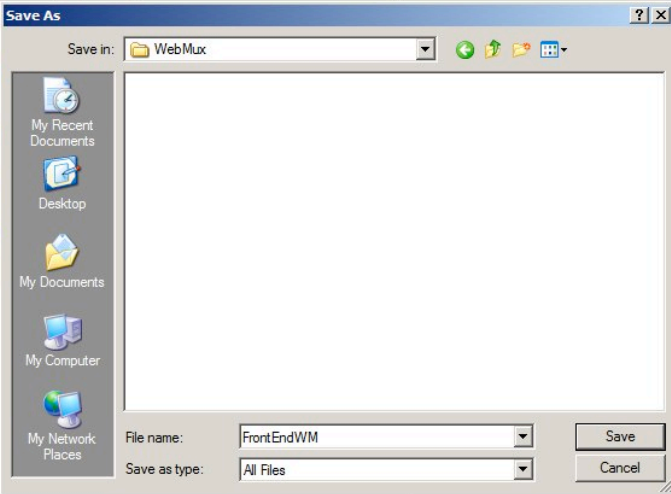
Upload farm/server configuration to WebMux: Use this form to upload farm/server configuration. New farm/server configuration goes into effect immediately.

Download all settings from WebMux: [Click here](#) to download all settings.

Upload all settings to WebMux: Use this form to upload all settings. Upload all settings do not go into effect until next reboot.

© 1997-2007 CAI Networks, Inc.

Done



To back up the current settings to your PC:

- a. Click on the second 'Click here' link on the screen
- b. Choose 'File->Save As' from the browser menu to save the configuration as a text file
- c. Name the file as desired and save it

In the above example, we are downloading the full current configuration for this WebMux to a file called "FrontEndWM".

WebMux Settings for Office Communications Server 2007 Configurations

Introduction

This appendix contains sample and recommended configuration settings for WebMux deployed with Office Communications Server 2007.

As described previously, WebMux configuration settings are comprised of:

- WebMux-level settings
- Service-level settings for each farm
- Settings for each farm
- Settings for the
- MAP rules for each farm (if any)
- Settings for the servers that are members of each farm

Tables 8 through 10 show recommended settings for various Office Communications Server 2007 deployments

In this Appendix, we are assuming that for all Office Communications Server 2007 components and modules that five WebMuxes (or pairs) are being deployed: one for the Enterprise pool, two for the Edge Servers, and one each for Communicator Web Access and Speech Server (if those modules are being deployed). You may deploy more or less WebMuxes to suit your own requirements, in which case you will need to map the configurations in this Appendix to your own environment.

Sample WebMux Settings

Sample WebMux settings for farms, MAP rules, and servers for various Office Communications Server 2007 configurations and topologies are documented in Appendices B through E.

WebMux-Level Settings

Table 9 shows the recommended WebMux-level settings for WebMuxes used in Office Communications Server 2007 deployments:

Table 9: **WebMux-Level Settings**

WebMux	Network	Networking Mode	TCP timeout	Reset timeouts	Attack protection
front end	Internal	NAT	30 minutes*	Yes	No
epool	Internal	NAT	30 minutes*	Yes	No
inner perimeter	Perimeter	NAT or Transparent	30 minutes*	Yes	Yes
outer perimeter	Perimeter	NAT or Transparent	30 minutes*	Yes	Yes
Communicator Web Access	Internal	NAT or Transparent	92 seconds**	Yes	No
Speech Server	Internal	Out-of-Path	20 minutes	Yes	No

** This setting should have a maximum value greater than or equal to the minimum of the REGISTER refresh or SIP Keep-Alive interval configured in Office Communication Server 2007.

** This setting should be at least twice the maximum client polling interval.

Farm Service-Level Settings

Table 10 shows the recommended service-level settings for different WebMuxes in an Office Communications Server 2007 environment.

Table 10: Farm Service-Level Settings

WebMux	Service	TCP retry interval
enterprise	generic no health check (TCP)	n/a
	generic (TCP)	Factory default
	HTTPS - secure hypertext transfer protocol (TCP)	Factory default
inner perimeter	generic (TCP)	Factory default
	generic (TCP)	Factory default
	HTTPS - secure hypertext transfer protocol (TCP)	Factory default
outer perimeter	generic no health check (TCP)	n/a
	generic (TCP)	Factory default
	HTTPS - secure hypertext transfer protocol (TCP)	Factory default
Communicator Web Access	generic (TCP/UDP)	30 seconds*
	HTTP - hypertext transfer protocol (TCP)	30 seconds*
	HTTPS - secure hypertext transfer protocol (TCP)	30 seconds*
Speech Server	generic (TCP/UDP)	Factory default
	HTTP - hypertext transfer protocol (TCP)	Factory default
	HTTPS - secure hypertext transfer protocol (TCP)	Factory default

* If you are using a separate WebMux for ISA Server or other Reverse Proxy Server for Communicator Web Access, use a value of 30 seconds.

Farm Configurations

Table 11 shows various Office Communications Server 2007 configurations and topologies and the recommended farms for each, and what servers are members of the farms.

Table 11: Farm Configurations

Front End WebMux

Configuration/Topology	Farm	Servers
Enterprise Edition Consolidated Configuration	1	Front End Servers pool
Enterprise Edition Expanded Configuration	1	Front End Servers pool

Epool WebMux

Configuration/Topology	Farm	Servers
Standard Edition or Enterprise Edition Consolidated Configuration with an Array of Directors	1	Array of Directors
Enterprise Edition Expanded Configuration without an Array of Directors and 2 or more Web Components Servers	1	Web Components Servers
Enterprise Edition Expanded Configuration with an Array of Directors and 2 or more Web Components Servers	1	Web Components Servers
	2	Array of Directors

Inner Perimeter WebMux – Local Site

Configuration/Topology	Farm	Servers
Scaled Single-Site Edge Topology, Multiple Site with Remote Site Edge, or Multiple Site with Scaled Remote Site Edge Topology	1	Access Edge Servers
	2	A/V Edge Servers

Outer Perimeter WebMux – Local Site

Configuration/Topology	Farm	Servers
Scaled Single-Site Edge Topology or Multiple Site (with a Remote Site Edge or Scaled Remote Site Edge) Topology with 0 or 1 ISA Server or other Reverse Proxy Server	1	Access Edge Servers
	2	Web Conferencing Edge Servers
	3	A/V Edge Servers

Outer Perimeter WebMux – Local Site (continued)

Configuration/Topology	Farm	Servers
Scaled Single-Site Edge Topology or Multiple Site (with a Remote Site Edge or Scaled Remote Site Edge) Topology with 2 or more ISA Servers or other Reverse Proxy Servers	1	Access Edge Servers
	2	Web Conferencing Edge Servers
	3	A/V Edge Servers
	4	ISA Server or other Reverse Proxy Server

Inner Perimeter WebMux – Remote Site

Configuration/Topology	Farm	Servers
Scaled Remote Site Edge Topology	1	A/V Edge Servers

Outer Perimeter WebMux – Remote Site

Configuration/Topology	Farm	Servers
Remote Site Edge Topology with 2 or more Web Conferencing Edge Server computers and 0 or 1 ISA Server or other Reverse Proxy Server	1	Web Conferencing Edge Servers
Remote Site Edge Topology with 1 Web Conferencing Edge Server computer and 2 or more ISA Servers or other Reverse Proxy Servers	1	ISA Server or other Reverse Proxy Server
Remote Site Edge Topology with 2 or more Web Conferencing Edge Server computers and 2 or more ISA Servers or other Reverse Proxy Servers	1	Web Conferencing Edge Servers
	2	ISA Servers or other Reverse Proxy Servers
Scaled Remote Site Edge Topology with 0 or 1 ISA Server or other Reverse Proxy Server	1	A/V Edge Servers
	2	Web Conferencing Edge Servers
Scaled Remote Site Edge Topology with 2 or more ISA Servers or other Reverse Proxy Servers	1	A/V Edge Servers
	2	Web Conferencing Edge Servers
	3	ISA Servers or other Reverse Proxy Servers

Front End WebMux – Remote Site

Same as local site front end WebMux.

Epool WebMux – Remote Site

Same as the local site epool WebMux.

Communicator Web Access WebMux

Configuration/Topology	Farm	Servers
Separate servers for internal and external users, with 1 server for internal users, 2 or more servers for external users, and 1 ISA Server or other Reverse Proxy Server	1	Internal user server array
Separate server arrays for internal and external users, with 2 or more servers for internal users, 1 server for external users, and 1 ISA Server or other Reverse Proxy Server	1	External user server array
Separate server arrays for internal and external users, with 2 or more servers for internal users, 2 or more server for external users, and 1 ISA Server or other Reverse Proxy Server	1	Internal user server array
	2	External user server array
Separate server arrays for internal and external users, with 2 or more servers for internal users, 2 or more servers for external users, and 2 or more ISA Servers or other Reverse Proxy Servers	1	Internal user server array
	2	External user server array
	3	ISA Servers or other Reverse Proxy Servers
Single server for internal users, single server for external users, a shared server as a hot standby, and 1 ISA Server or other Reverse Proxy Server	1	Internal user server and shared server
	2	External user server and shared server
Single server for internal users, a single server for external users, a shared server as a hot standby, and 2 or more ISA Servers or other Reverse Proxy Servers	1	Internal user server and shared server
	2	External user server and shared server
	3	ISA Servers or other Reverse Proxy Servers

Speech Server WebMux

Topology	Farm	Servers
Small Enterprise Topology or Large Enterprise Topology with web servers installed on Speech Servers	1	Speech Server farm
Small Enterprise Topology or Large Enterprise Topology with separate Web Servers	1	Speech Server farm
	2	Web server farm

Ports and Services

Table 12 shows the recommended ports and related services for WebMux farms for Office Communications Server 2007 deployments.

Table 12: Ports and Services

Farm	Port	Service
Web Components Servers	443	HTTPS - secure hypertext transfer protocol (TCP)
Front End Servers	135	generic no health check (TCP)*
	443	generic no health check (TCP)*
	444	generic no health check (TCP)*
	5060	generic (TCP)
	5061	generic (TCP)
Web Components Servers	443	HTTPS - secure hypertext transfer protocol (TCP)
Array of Directors	135	generic no health check (TCP)*
	443	generic no health check (TCP)*
	444	generic no health check (TCP)*
	5060	generic (TCP)
	5061	generic (TCP)

Table 12: Ports and Services (continued)

Farm	Port	Service
Access Edge Servers	443	HTTPS - secure hypertext transfer protocol (TCP)
	5061	generic (TCP)
Web Conferencing Edge Servers	443	HTTPS - secure hypertext transfer protocol (TCP)
	8057	generic (TCP)
A/V Edge Servers	443	HTTPS - secure hypertext transfer protocol (TCP)
	3478	generic (UDP)
	5062	generic (TCP)
	0**	generic (TCP/UDP)
ISA Servers or other Reverse Proxy Servers	443	HTTPS - secure hypertext transfer protocol (TCP)
External Web farm	443	HTTPS - secure hypertext transfer protocol (TCP)
Communicator Web Access servers	80 or 443	HTTP - hypertext transfer protocol (TCP) or HTTPS - secure hypertext transfer protocol (TCP)
	0**	generic (TCP/UDP)
Communicator Web Access ISA Servers or other Reverse Proxy Servers	443	HTTPS - secure hypertext transfer protocol (TCP)
Speech Server Speech Servers	80 or 443	HTTP - hypertext transfer protocol (TCP) or HTTPS - secure hypertext transfer protocol (TCP)
	0**	generic (TCP/UDP)
Speech Server Web servers	80 or 443	HTTP - hypertext transfer protocol (TCP) or HTTPS - secure hypertext transfer protocol (TCP)

- * The services for these ports are configured with no health checking because Office Communications Server 2007 does not maintain activity on them and therefore health-checking these ports would cause WebMux to incorrectly determine that the server was inoperative.
- ** These farms handle traffic over a range of dynamically-allocated ports. Port 0 instructs WebMux to load balance and traffic manage any port that may be accessed for the farm.

Scheduling Methods

Table 13 shows the recommended scheduling methods to configure for WebMux farms for Office Communications Server 2007 deployments.

Table 13: **Scheduling Methods**

Farm	Label	Scheduling Method
Front End Servers	OCS_FE	weighted least connections, persistent
Web Components Servers	OCS_WCS	weighted least connections, persistent
Array of Directors	OCS_DA	weighted least connections, persistent
Access Edge Servers (external users)	OCS_E_AE	weighted least connections, persistent
Access Edge Servers (internal users)	OCS_I_AE	weighted least connections, persistent
Web Conferencing Edge Servers (external users)	OCS_E_WCE	weighted least connections, persistent
A/V Edge Servers (external users)	OCS_E_AVE	weighted least connections, persistent
A/V Edge Servers (internal users)	OCS_I_AVE	weighted least connections, persistent
ISA Servers or other Reverse Proxy Servers	RP	weighted least connections
External Web farm	WebFarm	weighted least connections, persistent
Communicator Web Access servers (internal users)	CWA_INT	weighted least connections, persistent
Communicator Web Access servers (external users)	CWA_EXT	weighted least connections, persistent
Communicator Web Access ISA Servers or other Reverse Proxy Servers	RP	weighted least connections
Speech Server Speech Servers	SS_SS	round robin
Speech Server Web Servers	SS_WS	weighted round robin

Sample Configuration Settings for Internal Network WebMuxes

Introduction

This appendix details the internal network deployments for which Office Communications Server 2007 requires the use of a hardware load balancer:

- Enterprise Edition Consolidated Configuration
- Enterprise Edition Expanded Configuration
- Multiple Web Components Servers (for Enterprise Edition Expanded Configuration)
- Array of Directors (Array of Standard Edition Servers as a Director) for Standard Edition or Enterprise Edition

Enterprise Edition Configurations

The Enterprise Edition Consolidated Configuration and Enterprise Edition Expanded Configuration are similar from a WebMux perspective in that their Front End Servers in the Enterprise pool comprise a single WebMux farm.

Both the Consolidated and Expanded configurations can optionally have a single Director or Array of Directors (Array of Standard Edition Servers as a Director); if the latter, they are members of a WebMux farm.

The Enterprise Edition Expanded Configuration additionally has a pool of Web Components Servers that comprise their own farm.

Sample WebMux configuration settings for Enterprise Edition Consolidated and Expanded Configurations

The following tables show the sample WebMux settings for the Front End Servers in an Enterprise pool for either the Office Communications Server 2007 Enterprise Edition Consolidated Configuration or Enterprise Edition Expanded Configuration

Farm configuration**Enterprise Edition – Front End Servers**

Setting	Value
IP Address	VIP associated with the Front End Server FQDN
Label	“OCS_FE”
Port number	“5060”
Service	generic (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

MAP rules**Enterprise Edition – Front End Servers**

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_FE_MAP_1”
Port number	“5061”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Service	generic no health check (TCP)
Label	“OCS_FE_MAP_2”
Port number	“135”
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_FE_MAP_3”
Port number	“443”
Service	generic no health check (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_FE_MAP_4”
Port number	“444”
Service	generic no health check (TCP)
SSL/TLS Termination?	(none)

Server configuration

Enterprise Edition – Front End Servers

Setting	Value
IP Address	Internal IP address of Front End Server computer <i>n</i>
Label	“OCS_FE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional Front End Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Web Components Servers (Enterprise Edition Expanded Configuration)

Sample WebMux Settings for Web Components Servers

The following tables show the sample WebMux settings for multiple Web Components Servers (servers running IIS) in the Enterprise Edition Expanded Configuration.

Farm configuration Enterprise Edition: Expanded – Web Components Servers

Setting	Value
IP Address	VIP associated with the FQDN of the Web Components Servers
Label	“OCS_WCS”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Server configuration Enterprise Edition: Expanded – Web Components Servers

Setting	Value
IP Address	Internal IP address of Web Components Server <i>n</i>
Label	“OCS_WCS_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)

To add additional Web Components Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Array of Directors (Array of Standard Edition Servers as a Director)

Sample WebMux Settings for an Array of Directors

The following tables show the sample WebMux settings for multiple Director server computers deployed with the Standard or Enterprise Configuration deployment.

Farm configuration**Array of Directors**

Setting	Value
IP Address	VIP associated with FQDN of the Array of Directors
Label	“OCS_DA”
Port number	“5060”
Service	generic (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

MAP rules**Array of Directors**

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_DA_MAP_1”
Port number	“5061”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_DA_MAP_2”
Port number	“135”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_DA_MAP_3”
Port number	“443”
Service	generic no health check (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_DA_MAP_4”
Port number	“444”
Service	generic no health check (TCP)
SSL/TLS Termination?	(none)

Server configuration

Array of Directors

Setting	Value
IP Address	Internal IP address of Director computer <i>n</i>
Label	“OCS_DA_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional Director server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Sample Configuration Settings for Perimeter Network WebMuxes

Introduction

This appendix details the local and remote perimeter network deployments for which Office Communications Server 2007 requires the use of a hardware load balancer:

- Scaled Single-Site Edge Topology
- Multiple Site with a Remote Site Edge Topology (data center side only)
- Multiple Site with a Scaled Remote Site Edge Topology (both data center and remote sites)
- Multiple ISA Servers or other Reverse Proxy Servers

Scaled Single-Site Edge Topology

Sample Inner Perimeter WebMux Settings for Scaled Single-Site Edge Topology

The following tables show the sample WebMux settings for the Office Communications Server 2007 Scaled Single-Site Edge Topology.

Inner Perimeter WebMux

Farm #1 farm configuration

Scaled Single-Site Edge Topology

Setting	Value
IP Address	VIP associated with FQDN of Access Edge Server role
Label	“OCS_I_AE”
Port number	“5061”
Service	generic (TCP)
Scheduling Method	weighted least connections, persistent

Farm #1 server configuration**Scaled Single-Site Edge Topology**

Setting	Value
IP Address	Internal IP address of collocated Access Edge Server / Web Components Server computer <i>n</i>
Label	“OCS_AE-WCE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional collocated Access Edge Server / Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Inner Perimeter WebMux**Farm #2 farm configuration****Scaled Single-Site Edge Topology**

Setting	Value
IP Address	VIP associated with FQDN of A/V Edge Server role
Label	“OCS_I_AVE”
Port number	“443”
Service	generic (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #2 MAP rules**Scaled Single-Site Edge Topology**

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_I_AVE_MAP_1”
Port number	“3478”
Service	generic (UDP)"
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_I_AVE_MAP_2”
Port number	“5062”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_I_AVE_MAP_3”
Port number	“0”
Service	generic (TCP/UDP)
SSL/TLS Termination?	(none)

Farm #2 server configuration**Scaled Single-Site Edge Topology**

Setting	Value
IP Address	Internal IP address of A/V Edge Server computer <i>n</i>
Label	“OCS_AVE_SRV_” <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional A/V Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Outer Perimeter WebMux**Farm #1 farm configuration****Scaled Single-Site Edge Topology**

Setting	Value
IP Address	VIP associated with FQDN of Access Edge Server role
Label	“OCS_E_AE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent

Farm #1 MAP configuration**Scaled Single-Site Edge Topology**

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_E_AE-MAP_1”
Port number	“5061”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Farm #1 server configuration**Scaled Single-Site Edge Topology**

Setting	Value
IP Address	Internal IP address of collocated Access Edge Server / Web Conferencing Edge Server computer <i>n</i>
Label	“OCS_AE-WCE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)

To add additional collocated Access Edge Server / Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Note that you will also need to add the new computer into Farm #2, with identical settings.

Outer Perimeter WebMux**Farm #2 farm configuration****Scaled Single-Site Edge Topology**

Setting	Value
IP Address	VIP associated with FQDN of Web Conferencing Edge Server role
Label	“OCS_E_WCE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #2 MAP rules**Scaled Single-Site Edge Topology**

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_WCE_MAP_1”
Port number	“8057”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Farm #2 server configuration**Scaled Single-Site Edge Topology**

Setting	Value
IP Address	Internal IP address of collocated Access Edge Server / Web Conferencing Edge Server computer <i>n</i>
Label	“OCS_AE-WCE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run State	Choose the state that the server should be in when WebMux starts

To add additional collocated Access Edge Server / Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Note that you will also need to add the new computer into Farm #1, with identical settings.

Outer Perimeter WebMux

Farm #3 farm configuration

Scaled Single-Site Edge Topology

Setting	Value
IP Address	VIP associated with FQDN of A/V Edge Server role
Label	“OCS_E_AVE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #3 MAP rules

Scaled Single-Site Edge Topology

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_E_AVE_MAP_1”
Port number	“3478”
Service	generic (UDP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_E_AVE_MAP_2”
Port number	“0”
Service	generic (TCP/UDP)
SSL/TLS Termination?	(none)

Farm #3 server configuration**Scaled Single-Site Edge Topology**

Setting	Value
IP Address	Internal IP address of A/V Edge Server computer <i>n</i>
Label	“OCS_AVE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional A/V Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Multiple Site with a Remote Site Edge Topology**Sample WebMux Settings for Multiple Site with a Remote Site Edge Topology (Data Center location)**

The following tables show the sample WebMux settings for the Office Communications Server 2007 Remote Site Edge Topology.

Local Site Inner Perimeter WebMux**Farm #1 farm configuration****Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	VIP associated with FQDN of Access Edge Server role
Label	“OCS_I_AE”
Port number	“5061”
Service	generic (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #1 server configuration**Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	Internal IP address of first collocated data center Access Edge Server / Web Conferencing Edge Server computer
Label	“OCS_AE-WCE_SRV_n”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional collocated Access Edge Server / Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Note that you will also need to add the new computer into Farm #2, with identical settings.

Local Site Inner Perimeter WebMux**Farm #2 farm configuration****Remote-Site Edge Topology – Local Site**

Setting	Value
IP Address	VIP associated with FQDN of data center A/V Edge Server role
Label	“OCS_I_AVE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #2 MAP rules**Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_I_AVE_MAP_1”
Port number	“5062”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_I_AVE_MAP_2”
Port number	“3478”
Service	generic (UDP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_I_AVE_MAP_3”
Port number	“0”
Service	generic (TCP/UDP)
SSL/TLS Termination?	(none)

Farm #2 server configuration**Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	Internal IP address of data center A/V Edge Server computer <i>n</i>
Label	“OCS_AVE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional A/V Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Local Site Outer Perimeter WebMux**Farm #1 farm configuration****Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	VIP associated with FQDN of Access Edge Server (role, not computer)
Label	“OCS_E_AE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #1 MAP rule**Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_E_AE_MAP_n”
Port number	“5061”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Farm #1 server configuration**Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	Internal IP address of collocated data center Access Edge Server / Web Conferencing Edge Server computer <i>n</i>
Label	“OCS_AE-WCE_SRV_n”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional collocated Access Edge Server / Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Note that you will also need to add the new computer into Farm #2, with identical settings.

Local Site Outer Perimeter WebMux

Farm #2 farm configuration

Remote Site Edge Topology – Local Site

Setting	Value
IP Address	VIP associated with FQDN of data center Web Conferencing Server role
Label	“OCS_E_WCE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #2 MAP rules

Remote Site Edge Topology – Local Site

Setting	Value
IP address	The VIP of the current farm
Label	“OCS_E_WCE_MAP_1”
Port number	“8057”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Farm #2 server configuration

Remote Site Edge Topology – Local Site

Setting	Value
IP Address	Internal IP address of collocated data center Access Edge Server / Web Conferencing Edge Server computer <i>n</i>
Label	“OCS_AE-WCE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional collocated Access Edge Server / Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*,

“same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Note that you will also need to add the new computer into Farm #1, with identical settings.

Local Site Outer Perimeter WebMux

Farm #3 farm configuration

Remote Site Edge Topology – Local Site

Setting	Value
IP Address	VIP associated with FQDN of data center A/V Edge Server role
Label	“OCS_E_AVE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #3 MAP rules

Remote Site Edge Topology – Local Site

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_E_AVE_MAP_1”
Port number	“3478”
Service	generic (UDP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_E_AVE_MAP_2”
Port number	“0”
Service	generic (TCP/UDP)
SSL/TLS Termination?	(none)

Farm #3 server configuration**Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	Internal IP address of data center A/V Edge Server computer <i>n</i>
Label	“OCS_AVE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run State	Choose the state that the server should be in when WebMux starts

To add additional A/V Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Remote Site Inner Perimeter WebMux**Farm configuration****Remote Site Edge Topology – Remote Site**

Setting	Value
IP Address	VIP associated with FQDN of remote site Web Conferencing Edge Server role
Label	“OCS_E_WCE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Server configuration**Remote Site Edge Topology – Remote Site**

Setting	Value
IP Address	Internal IP address of remote site Web Conferencing Edge Server computer <i>n</i>
Label	“OCS_WCE_SRV_” <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Multiple Site with a Scaled Remote Site Edge Topology

Sample WebMux Settings for Multiple Site with a Scaled Remote Site Edge Topology (Data Center location)

The following tables show the sample WebMux settings for the Office Communications Server 2007 Scaled Remote Site Edge Topology deployment at the local site.

Local Site Inner Perimeter WebMux

Farm #1 farm configuration**Scaled Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	VIP associated with FQDN of Access Edge Server (role, not computer)
Label	“OCS_I_AE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #1 MAP rules**Scaled Remote Site Edge Topology – Local site**

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_AE_MAP_1”
Port number	“5061”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Farm #1 server configuration**Scaled Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	Internal IP address of collocated data center Access Edge Server / Web Conferencing Edge Server computer <i>n</i>
Label	“OCS_AE-WCE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional collocated Access Edge Server / Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Note that you will also need to add the new computer into Farm #2, with identical settings.

Local Inner Perimeter WebMux

Farm #2 farm configuration

Scaled Remote-Site Edge Topology – Local Site

Setting	Value
IP Address	VIP associated with FQDN of data center A/V Edge Server (role, not computer)
Label	“OCS_AVE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #2 MAP rules

Scaled Remote Site Edge Topology – Local Site

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_AVE_MAP_1”
Port number	“5062”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_AVE_MAP_2”
Port number	“3478”
Service	generic (UDP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_AVE_MAP_3”
Port number	“0”
Service	generic (TCP/UDP)
SSL/TLS Termination?	(none)

Farm #2 server configuration**Scaled Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	Internal IP address of data center A/V Edge Server computer <i>n</i>
Label	“OCS_AVE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional A/V Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Local Site Outer Perimeter WebMux**Farm #1 farm configuration****Scaled Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	VIP associated with FQDN of Access Edge Server (role, not computer)
Label	“OCS_AE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #1 MAP rules**Scaled Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_AE_MAP_1”
Port number	“5061”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Farm #1 server configuration**Scaled Remote Site Edge Topology – Local Site**

Setting	Value
IP Address	Internal IP address of collocated data center Access Edge Server / Web Conferencing Edge Server computer <i>n</i>
Label	“OCS_AE-WCE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional collocated Access Edge Server / Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Note that you will also need to add the new computer into Farm #2, with identical settings.

Local Site Outer Perimeter WebMux

Farm #2 farm configuration

Scaled Remote Site Edge Topology – Local Site

Setting	Value
IP Address	VIP associated with FQDN of data center Web Conferencing Edge Server (role, not computer)
Label	“OCS_WCE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #2 MAP rules

Scaled Remote Site Edge Topology – Local Site

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_WCE_MAP_1”
Port number	8057
Service	“generic (TCP)”
SSL/TLS Termination?	(none)

Farm #2 server configuration

Scaled Remote Site Edge Topology – Local Site

Setting	Value
IP Address	Internal IP address of data center collocated Access Edge Server / Web Conferencing Edge Server computer <i>n</i>
Label	“OCS_AE-WCE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional collocated Access Edge Server / Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*,

“same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Note that you will also need to add the new computer into Farm #1, with identical settings.

Local Site Outer Perimeter WebMux

Farm #3 farm configuration

Scaled Remote Site Edge Topology – Local Site

Setting	Value
IP Address	VIP associated with FQDN of data center A/V Edge Server (role, not computer)
Label	“OCS_AVE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #3 MAP rules

Scaled Remote Site Edge Topology – Local Site

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_AVE_MAP_1”
Port number	“5062”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_AVE_MAP_2”
Port number	“3478”
Service	generic (UDP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_AVE_MAP_3”
Port number	“0”
Service	generic (TCP/UDP)
SSL/TLS Termination?	(none)

Farm #3 server configuration

Scaled Remote Site Edge Topology – Local Site

Setting	Value
IP Address	Internal IP address of data center A/V Edge Server computer <i>n</i>
Label	“OCS_AVE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional A/V Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Sample WebMux Settings for Multiple Site with a Scaled Remote Site Edge Topology (Remote Site Location)

The following tables show the sample WebMux settings for the Scaled Remote Site Edge Topology deployment at the remote site.

Remote Site Inner Perimeter WebMux

Farm configuration

Scaled Remote Site Edge Topology – Remote Site

Setting	Value
IP Address	VIP associated with FQDN of remote site A/V Edge Server role
Label	“OCS_I_AVE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

MAP rules

Scaled Remote Site Edge Topology – Remote Site

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_I_AVE_MAP_1”
Port number	“5062”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_I_AVE_MAP_2”
Port number	“3478”
Service	generic (UDP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_I_AVE_MAP_3”
Port number	“0”
Service	generic (TCP/UDP)
SSL/TLS Termination?	(none)

Server configuration

Scaled Remote Site Edge Topology – Remote Site

Setting	Value
IP Address	Internal IP address of remote site A/V Edge Server computer <i>n</i>
Label	“OCS_AVE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional A/V Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Remote Site Outer Perimeter WebMux

Farm #1 farm configuration

Scaled Remote Site Edge Topology – Remote Site

Setting	Value
IP Address	VIP associated with FQDN of remote site Web Conferencing Edge Server role
Label	“OCS_E_WCE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #1 server configuration

Scaled Remote Site Edge Topology – Remote Site

Setting	Value
IP Address	Internal IP address of remote site Web Conferencing Edge Server computer <i>n</i>
Label	“OCS_WCE_SRV_” <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional Web Conferencing Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Remote Site Outer Perimeter WebMux

Farm #2 farm configuration

Scaled Remote Site Edge Topology – Remote Site

Setting	Value
IP Address	VIP associated with FQDN of remote site A/V Edge Server role
Label	“OCS_E_AVE”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Farm #2 MAP rules

Scaled Remote Site Edge Topology – Remote Site

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_E_AVE_MAP_1”
Port number	“5062”
Service	generic (TCP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_E_AVE_MAP_2”
Port number	“3478”
Service	generic (UDP)
SSL/TLS Termination?	(none)

Setting	Value
IP Address	The VIP of the current farm
Label	“OCS_E_AVE_MAP_3”
Port number	“0”
Service	generic (TCP/UDP)
SSL/TLS Termination?	(none)

Farm #2 server configuration Scaled Remote Site Edge Topology – Remote Site

Setting	Value
IP Address	Internal IP address of remote site A/V Edge Server computer <i>n</i>
Label	“OCS_AVE_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional A/V Edge Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

ISA Servers or other Reverse Proxy Servers

Office Communications Server 2007 Edge Servers work with an HTTP Reverse Proxy Server, such as Microsoft ISA Server. Multiple Reverse Proxy servers form their own WebMux farm.

Sample WebMux Settings for ISA Servers or other Reverse Proxy Servers

The following tables show the sample WebMux settings for ISA Servers or other Reverse Proxy Servers.

Farm configuration**ISA Servers or other Reverse Proxy Servers**

Setting	Value
IP Address	VIP associated with FQDN of ISA Server or other Reverse Proxy Server pool
Label	“RP”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections

Server configuration**ISA Servers or other Reverse Proxy Servers**

Setting	Value
IP Address	Internal IP address of ISA Server or other Reverse Proxy Server computer <i>n</i>
Label	“RP_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional HTTP Reverse Proxy Server computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “443” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

External Web Farm

Web farms are typically deployed in a DMZ, like the perimeter network, but can also be deployed in the internal network. A web farm comprises multiple web servers hosting the same content.

Sample WebMux Settings for an External Web Farm

The following tables show the sample WebMux settings for multiple web servers that comprise an external web farm.

Farm configuration**External Web Farm**

Setting	Value
IP Address	VIP associated with FQDN of the web farm
Label	“WebFarm”
Port number	“443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	(none)

Server configuration**External Web Farm**

Setting	Value
IP Address	Internal IP address of web server <i>n</i>
Label	“WebFarm_SRV_ <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional web servers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Deploying WebMux with Microsoft Office Communicator Web Access (2007 release)

Introduction

This appendix details the local and remote internal and perimeter network deployments for which Office Communications Server Communicator Web Access requires the use of a hardware load balancer:

- Multiple separate servers for internal users
- Multiple separate servers for external users
- Combination of separate and shared servers
- Multiple ISA Servers or other Reverse Proxy Servers

Sample WebMux configuration settings for Communicator Web Access pool

The following tables show the sample WebMux settings for two server arrays (one for internal users and the other for external users) where both virtual servers have the same VIP or different VIPs but use different ports, and where WebMux is being configured to perform SSL/TLS acceleration.

Farm #1 farm configuration Communicator Web Access – Internal Server Array

Setting	Value
IP Address	VIP associated with FQDN of the Communicator Web Access internal user server array
Label	“CWA_INT”
Port number	“80/443”
Service	HTTP/HTTPS Combined Ports
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	Select the SSL/TLS certificate to use for this farm, or “(none)” if you do not want WebMux to offload SSL/TLS encryption and decryption from the servers
SSL port	Leave blank
Block non-SSL access to farm?	Select ‘NO’ from the listbox to allow unencrypted traffic to the farm’s servers
Tag SSL-terminated HTTP requests?	Select ‘YES’ from the listbox if you want to add an “X-WebMux-SSL-termination: true” MIME header in the decryption HTTP request

Farm #1 MAP rule Communicator Web Access – Internal Server Array

Setting	Value
IP Address	The VIP of the current farm
Label	“CWA_INT_MAP”
Port number	“0”
Service	HTTPS - hypertext transfer protocol (TCP)
SSL/TLS Termination?	Select the SSL/TLS certificate to use for this farm, or (none) if you do not want WebMux to offload SSL/TLS encryption and decryption from the servers

Farm #1 server configuration Communicator Web Access – Internal Server Array

Setting	Value
IP Address	IP address of Communicator Web Access internal user server computer <i>n</i> . If a shared server, specify the IP address of the instance for internal users
Label	“CWA_INT_SRV_” <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional internal user access Communicator Web Access servers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Farm #2 farm configuration Communicator Web Access – External Server Array

Setting	Value
IP Address	VIP associated with FQDN of Communicator Web Access external user server array
Label	“CWA_EXT”
Port number	“80” if WebMux will be performing SSL/TLS termination; otherwise “444”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections, persistent
SSL/TLS Termination?	Select the SSL/TLS certificate to use for this farm, or (none) if you do not want WebMux to offload SSL/TLS encryption and decryption from the servers
SSL port	“444” if WebMux will be performing SSL/TLS termination; otherwise leave blank
Block non-SSL access to farm?	Select ‘NO’ from the listbox to allow unencrypted traffic to the farm’s servers
Tag SSL-terminated HTTP requests?	Select ‘YES’ from the listbox if you want to add an “X-WebMux-SSL-termination: true” MIME header in the decryption HTTP request

Farm #2 MAP rule**Communicator Web Access – External Server Array**

Setting	Value
IP Address	The VIP of the current farm
Label	“CWA_EXT_MAP_1”
Port number	“80” or “443”
Service	HTTP - hypertext transfer protocol (TCP)
SSL/TLS Termination?	Select ‘YES’ from the listbox if you want to add an “X-WebMux-SSL-termination: true” MIME header in the decryption HTTP request

Farm #2 server configuration**Communicator Web Access – External Server Array**

Setting	Value
IP Address	Internal IP address of Communicator Web Access server computer <i>n</i> . If a shared server, specify the IP address of the instance for internal users
Label	“CWA_EXT_SRV_” <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional Communicator Web Access servers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “same” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

ISA Servers or other Reverse Proxy Servers

Communicator Web Access requires a Reverse Proxy for external users. If using SSO (Single Sign-On) capability, the only supported Reverse Proxy is Microsoft ISA Server.

Sample WebMux Settings for ISA Servers or other Reverse Proxy Servers

The following tables show the sample WebMux settings for ISA Servers or other Reverse Proxy Servers.

Farm configuration

ISA Servers or other Reverse Proxy Servers

Setting	Value
IP Address	VIP associated with FQDN of ISA Server or other Reverse Proxy Server pool
Label	“RP”
Port number	“80” if WebMux will be performing SSL/TLS termination; otherwise “443”
Service	HTTPS - secure hypertext transfer protocol (TCP)
Scheduling Method	weighted least connections
SSL/TLS Termination?	Select the SSL/TLS certificate to use for this farm, or (none) if you do not want WebMux to offload SSL/TLS encryption and decryption from the servers
SSL port	“443” if WebMux will be performing SSL/TLS termination; otherwise leave blank
Block non-SSL access to farm?	Select ‘NO’ from the listbox to allow unencrypted traffic to the farm’s servers
Tag SSL-terminated HTTP requests?	Select ‘YES’ from the listbox if you want to add an “X-WebMux-SSL-termination: true” MIME header in the decryption HTTP request

Server configuration**ISA Servers or other Reverse Proxy Servers**

Setting	Value
IP Address	Internal IP address of ISA Server or other Reverse Proxy Server computer <i>n</i>
Label	“RP_SRV_” <i>n</i> ”
Port number	“same”
Weight	An integer value between 1 and 100 that reflects the server’s relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional HTTP Reverse Proxy Sever computers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, “443” for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm’s scheduling method is Weighted).

Deploying WebMux with Microsoft Office Communications Server 2007 Speech Server

Introduction

This appendix details the internal network deployments for which Speech Server requires the use of a hardware load balancer:

- Small Enterprise Topology or Large Enterprise Topology with multiple Speech Servers
- Small Enterprise Topology or Large Enterprise Topology with multiple Speech Servers and multiple separate Web Servers

Sample WebMux configuration settings for Speech Servers

The following tables show the sample WebMux settings for multiple Speech Servers in either the Small Enterprise or Large Enterprise topology. In this example, Speech Server is being deployed with a separate Web Server farm, and WebMux is configured to perform SSL/TLS acceleration.

Farm configuration**Speech Server – Speech Servers**

Setting	Value
IP Address	VIP associated with FQDN of the Speech Servers
Label	“SS_SS”
Port number	“80/443”
Service	HTTP/HTTPS Combined Ports
Scheduling Method	round robin
SSL/TLS Termination?	Select ‘YES’ from the listbox to offload TLS encryption and decryption from Speech Servers or ‘NO’ to have the Speech Servers do the work
SSL port	Leave blank
Block non-SSL access to farm?	Select ‘NO’ from the listbox to allow unencrypted traffic to the farm’s servers
Tag SSL-terminated HTTP requests?	Select ‘YES’ from the listbox if you want to add an “X-WebMux-SSL-termination: true” MIME header in the decryption HTTP request

Server configuration**Speech Server – Speech Servers**

Setting	Value
IP Address	IP address of Speech Server <i>n</i>
Label	“SS_SS_SRV_ <i>n</i> ”
Port	“same”
Weight	“1”
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional Speech Servers into this farm, use an arbitrary *Label*, the computer’s assigned *IP Address*, and “same” for *Port*.

Sample WebMux configuration settings for Speech Server Web farm

The following tables show the sample WebMux settings for multiple Web servers in the Large Enterprise topology.

Farm configuration**Speech Server – Web Servers**

Setting	Value
IP Address	VIP associated with FQDN of Speech Server's Web servers
Label	"SS_WS"
Port	"80/443"
Service	HTTP/HTTPS Combined Ports
Scheduling Method	weighted round robin
SSL/TLS Termination?	(none)
SSL port	Leave blank
Block non-SSL access to farm?	Select 'NO' from the listbox to allow unencrypted traffic to the farm's servers
Tag SSL-terminated HTTP requests?	Select 'YES' from the listbox if you want to add an "X-WebMux-SSL-termination: true" MIME header in the decryption HTTP request

Server configuration**Speech Server – Web Servers**

Setting	Value
IP Address	Internal IP address of Speech Server's Web server computer <i>n</i>
Label	"SS_WS_SRV_ <i>n</i> "
Port	"same"
Weight	An integer value between 1 and 100 that reflects the server's relative performance versus other servers in the farm (a server with a weight of 2 will be directed twice as much traffic as one with a weight of 1)
Run state	Choose whether the server should be treated by WebMux as active or standby

To add additional Web servers into this farm, use an arbitrary *Label*, the computer's assigned *IP Address* and "same" for *Port*, and whatever integer *Weight* is appropriate for the computer to reflect its power relative to other computers in the farm (assuming the farm's scheduling method is Weighted).

FAQs

Do I need WebMux for my particular Office Communications Server 2007 deployment?

If you are deploying Office Communications Server 2007 Enterprise Edition you need WebMux. If you are deploying the Standard Edition, you do not need WebMux unless you are deploying it with an Array of Directors (multiple Standard Edition Servers as a Director), or Communicator Web Access or Speech Server using multiple servers. See "Office Communications Server 2007 Load Balancer Requirements" in Chapter 4 for a discussion of how to determine if you require WebMux for your Office Communications Server 2007 deployment.

How many WebMuxes do I need?

It depends. If your deployment does not include any remote sites, one WebMux may be enough; otherwise, you will need at least three WebMuxes for each site. We recommend deploying WebMuxes in pairs to provide for WebMux fault tolerance. See "Number of WebMuxes Required" in Chapter 4 for a discussion of how to determine the number of WebMuxes you will require.

Can I use WebMux for systems other than Office Communications Server 2007?

Yes. WebMux can load-balance, traffic-manage, and provide failover capabilities for other types of servers, such as web servers, email servers, FTP servers, etc. The same WebMux(es) you deploy for Office Communications Server 2007 can handle other types of servers, depending upon your network configuration, except for the front end WebMux, which is dedicated to the Front End Server pool.

Can I use Microsoft's NLB as an instead of WebMux?

Microsoft supports only hardware load balancers for use with Office Communications Server 2007, therefore Network Load Balancing (NLB) using Windows NT Load Balancing Service (WLBS) is not supported.

Can I use NLB in a lab deployment?

Microsoft supports only hardware load balancers for Office Communications Server 2007 lab deployments.

Why can Transparent networking mode not be used for the front end WebMux?

Office Communications Server 2007 requires the Front End Servers to be in their own subnet, separate from other servers in the internal network. WebMux's Transparent mode causes WebMux to act as an Ethernet bridge, and as such all servers have the effect of being on the same network.

Why is Out-of-Path networking mode not supported for Office Communications Server 2007?

Out-of-Path mode is not supported for the Front End Server pool because it has the effect of blocking access to port 135, which is used for remote access using Office Communications Server 2007's administration tool. If your environment permits you to run the administrative snap-in locally and not from a remote computer then Out-of-Path mode can be used. Out-of-Path mode can be employed for other Office Communications Server 2007 components without restriction.

Why is WebMux's SSL termination documented for Communicator Web Access and Speech Server but not other Office Communications Server 2007 components?

Microsoft has not documented that SSL/TLS offloading for the Enterprise pool, Edge Servers, and other components can be used. They do, however, recommend it for other Office Communications Server 2007 modules. Although not documented, we feel SSL/TLS offloading of any Office Communications Server 2007 servers by WebMux should work properly.

What is the reason for specifying port 0 for some WebMux farms?

Some Office Communications Server 2007 servers use a wide range of ports that are dynamically allocated for handling certain user transactions which must be load-balanced and traffic-managed by WebMux. Port "0" causes WebMux to load-balance and traffic-manage all ports on all servers that are members of such farms.

Why do the services on some ports not require health checking?

The services for Front End Servers on ports 135 and 444 do not maintain activity, therefore health-checking these ports would cause WebMux to incorrectly determine that the servers are inactive; therefore no health checking is imposed on these ports or port 443. The SIP ports on the Front End Servers (5060 and 5061) are health-checked by WebMux to determine which servers are healthy and which are inoperative.

Glossary

array

A group of computers that perform the same function, with any being able to do the job. In Office Communications Server 2007, multiple Directors and Access Edge Servers, for example, may be deployed in arrays.

Array of Directors

Describes multiple identically configured servers being deployed to serve as the Director role in an Office Communications Server 2007 Standard Edition or Enterprise Edition configuration. Same as Array of Standard Edition Servers as a Director.

Array of Standard Edition Servers as a Director

See *Array of Directors*.

A/V Conferencing Server

An Office Communications Server 2007 server role that enables provides audio and video conferencing capabilities. In the Office Communications Server 2007 Standard configuration, the A/V Conferencing Server is installed on the Front End server along with other Office Communications Server 2007 servers; in the Consolidated configuration, it is installed on every Front End Server; in the Expanded configuration, it is installed on one or more separate, dedicated computers in the Enterprise pool.

Back-End Database server

In Office Communications Server 2007, this is a computer that hosts the Microsoft SQL Server database that stores the user data. In the Standard configuration, the database is not on a separate server, therefore there is no Back-End Database server. In both Enterprise configurations, the Back-End Database server is installed on a separate computer but not considered part of the Enterprise pool. In all cases, the back-end database (whether installed separately or collocated) is not load balanced by WebMux.

certificate

Refers to SSL or TLS certificate.

collocation

This refers to multiple entities existing on the same device. For Office Communications Server 2007, it refers to software servers resident on the same server computer (e.g., the Access Edge Server and Web Conferencing Edge Server are collocated on the same computer). For WebMux, multiple farms are collocated in the same WebMux.

connection persistence

Office Communications Server 2007 requires that transactions related to a connection resolve to the same server computer, rather than being allocated to another server as part of an agnostic load balancing scheme. WebMux calls its ability to manage an active connection's traffic to the same server "connection persistence".

CSR

Certificate Signing Request.

DDoS attack

Distributed denial of service attack, where there are multiple simultaneous attackers.

Director

This is an optional but recommended Office Communications Server 2007 server role in the internal network that comes into play when an Office Communications Server 2007 deployment has remote users or federation activity into the organization. The Director's main responsibility is to offload authentication from the existing Standard Edition or Front-End Server or the Enterprise pool. A Director can be deployed as a Standard Edition Server or multiple Standard Edition Servers with most of their roles deactivated (an Array of Directors or Array of Standard Edition Servers as a Director) or the Enterprise pool.

dispatch method

Another name for WebMux's networking mode.

dual WebMux

This is how we describe two identically-configured WebMuxes deployed as a pair for fault-tolerance purposes (as opposed to solo WebMux, which is not tolerant of WebMux failures)

DMZ

Abbreviation for "Demilitarized Zone". It is a network that sits between an organization's internal network and an external network (typically the Internet) and which is bounded by firewalls, protecting computers in the internal network in the event a computer in the DMZ is compromised. The perimeter network in Office Communications Server 2007 is a DMZ.

DNS

Domain Name System server that resolves FQDNs to IP addresses and vice versa.

DoS attack

Denial of Service attack.

Edge Server

In Office Communications Server 2007, this is a specialized proxy server that resides in the perimeter network at local and remote sites and provides connectivity for external users and public IM connections. Each local Edge Server has one or more of the

following roles: Access Edge Server, Web Conferencing Edge Server, A/V Edge Server, while remote Edge Servers do not have the Access Edge Server role.

Enterprise pool

A group of computers that host the servers for either the Standard, Consolidated, or Expanded configuration. In the Consolidated configuration, each computer in the Enterprise Edition Consolidated Pool is installed with the same multiple servers, whereas in the Enterprise Edition Expanded Pool there are multiple identical Front End Servers and also separate computers hosting other servers. (The Back-End Database is installed on a dedicated computer which resides in the Enterprise pool but is not itself considered an Enterprise Edition server.) In WebMux, Enterprise Edition servers in the Enterprise pool (which does not include the Back-End Database server) are assigned to one or more farms.

Enterprise server

In Office Communications Server 2007 terminology, this is a computer that is part of the Office Communications Server 2007 Enterprise Edition Consolidated or Expanded configuration, not including the database server.

epool WebMux

The WebMux in the internal network that load balances the Web Components Servers for the Office Communications Server 2007 Enterprise Edition Expanded Configuration and the Array of Directors in any configuration. It can also load balance web farms and other servers in the internal network.

front end WebMux

The WebMux in the internal network that load balances the Front End Servers.

external network

This is a network outside the organization, typically the Internet.

external DNS

The DNS server that serves the external network (public IP addresses)

external IP address

Public IP address.

external web farm

See *web farm*.

FQDN

Abbreviation for "Fully Qualified Domain Name", which is a full domain name terminated by a period ("."). WebMux farms in Office Communications Server 2007 are generally addressed by FQDN, which is resolved to the farm's VIP via an A Record or hosts file entry.

Front End Server

In Office Communications Server 2007, this is a computer that provides IM, presence, and conferencing services and is part of a Standard or Enterprise configuration. Front End Servers host the Focus Factory and always host the IM Conferencing Server and Telephony Conferencing Server. In the Consolidated configuration, Front End Servers also host the Web Conferencing and A/V Conferencing Server, and Web Components Server. In the Expanded configuration, the Web Conferencing Server, A/V Conferencing Server, and Web Components Server are each installed on one or more separate, dedicated computers. If there is more than one Front End Server, they require load balancing by WebMux.

farm

MS uses the term pool except when referring to a webfarm, we use farm

hardware load balancer

This is the generic term used by Office Communications Server 2007 for hardware-based network appliances that perform load balancing, like WebMux (compared with a software-based load balancer like Microsoft's WCLS).

HTTP Reverse Proxy Server

See Reverse proxy.

IM Conferencing Server

An Office Communications Server 2007 server role that enables provides group-enabled instant text messaging. In the Office Communications Server 2007 Standard configuration, the IM Conferencing Server is installed on the Front End server along with other Office Communications Server 2007 servers; in the Consolidated configuration, it is installed on every Front End Server; in the Expanded configuration, it is installed on one or more separate, dedicated computers in the Enterprise pool.

inner perimeter WebMux

One of two WebMuxes in the Office Communications Server 2007 perimeter network – the one next to the internal firewall – which load balances Edge server traffic from the internal network.

internal DNS

The DNS server that serves the internal network

internal IP address

An IP address that is only accessible from the internal network. Also know as private IP address.

internal network

In an Office Communications Server 2007 deployment, this is the network that contains the Standard or Enterprise server computers.

ISA Server

Microsoft Internet Security and Acceleration (ISA) Server 2006. In Office Communications Server deployments, it functions as a Reverse Proxy.

LACP

Link Aggregation Control Protocol. A network protocol that allows bundling several physical ports together to form a single logical channel.

LACP switch

A network switch that supports LACP (Link Aggregation Control Protocol). WebMux's 680PG model requires LACP-capable switches in order to achieve its full bandwidth utilization capabilities.

logical load balancer

This is how Office Communications Server 2007 refers to the concept of a WebMux farm, the idea being that one WebMux can handle multiple farms and so, in effect, it is like there are two load balancers.

loopback adapter

An adapter that causes the data a computer sends out to be delivered back to it. WebMux's Out-of-Path networking mode requires each server to be outfitted with a loopback adapter.

Management Console

WebMux's browser-based configuration interface.

Main Management Console

The main screen of WebMux's browser-based configuration interface.

MAP™ capability

MAP (Multiple Address/Port) capability is an exclusive WebMux feature that imposes an affinity between multiple ports on multiple servers in a WebMux farm such that if any protocol on any port on any server in a farm fails that server will be taken out of service and all traffic will be diverted to a healthy server in the farm.

NAT mode

A two-arm WebMux networking mode in which load-balanced servers are on a separate LAN than the devices in front of the WebMux. In NAT mode, WebMux translates source and/or IP addresses and/or port numbers from the *Router LAN* to those in the *Server LAN*.

NLB

Network Load Balancing by WLBS.

one-arm mode

Describes a network device's connection to the network: in one-arm mode, traffic passes through the device in one direction only (whereas in two-arm mode traffic passes through the device in both directions).

OOP mode

Out-of-path mode.

Out-of-Path mode

A one-arm WebMux networking mode in which load-balanced servers are effectively on the main LAN but equipped with loopback adapters.

outer perimeter WebMux

One of two WebMuxes in the Office Communications Server 2007 perimeter network – the one next to the external firewall – which load balances Edge server and Reverse Proxy traffic from the external network.

perimeter network

In an Office Communications Server 2007 deployment, this is the network that resides in a DMZ that contains the Edge server computers.

persistence

See *connection persistence*.

pool

A pool has more than one server, in the case of Office Communications Server 2007 may or may not be identical (replicated). Or can be a pool of users.

pool configurations

Office Communications Server 2007 refers to its core server configurations as pool configurations. Office Communications Server 2007 offers three pool configurations: one Standard Edition configuration and two Enterprise Edition configurations: Consolidated and Expanded. Both configurations consist of identical Front End Servers connected to a separate Microsoft SQL Server™ back end database. There may also be other pools in an Office Communications Server 2007 deployment, such as

port affinity

Port affinity is a feature of WebMux's MAP capability that involves the logical binding of specified ports on a server. Should the service specified for any of the logically bound ports fail, the server is considered inoperative and taken offline.

protocol

Office Communications Server 2007 uses this term to refer to various software protocols (like HTTP and SIP) while we describe these as "service". We use the term "protocol" to refer to transport protocols like TCP and UDP.

Router LAN

In WebMux terminology, this is the WebMux network interface that connects to the outside network. In an Office Communications Server 2007 deployment, for the inner perimeter WebMux it is the WebMux interface that connects to the internal users and, via a firewall, to the perimeter network; for the outer perimeter WebMux, it is the interface that connects, via a firewall, to the Internet and/or external network(s). The Router LAN is not relevant in Transparent mode, since the servers are effectively on the same network as the other servers.

Reverse proxy

A server residing in a DMZ that increases security of the origin server by routing all client requests through the Reverse Proxy server. The Reverse Proxy receives content from the origin server and streams it to the client so that the client never directly communicates with the origin server. Same as Reverse Proxy Server and HTTP Reverse Proxy Server. Office Communications Server 2007 recommends use of ISA Server.

role

See *server role*.

RSA

An algorithm for public-key cryptography.

scheduling method

WebMux uses the term "scheduling method" to describe one of its algorithms for load balancing and traffic management among multiple servers in a farm. In most cases, WebMux's Weighted least connections, persistent scheduling method is used for Office Communications Server 2007.

server array

A pool of content-identical servers.

Server LAN

In WebMux terminology, this is the WebMux network interface that connects to the servers. In an Office Communications Server 2007 deployment, for the front end WebMux and epool WebMux it is the WebMux interface that connects to the Standard or Enterprise servers; for the inner perimeter WebMux and outer perimeter WebMux, it is the interface that connects to the Edge Servers. The Server LAN is not relevant in Transparent mode, since the servers are effectively on the same network as the other servers.

server role

In Office Communications Server 2007, a set of functions that can be performed by software servers, generally on either dedicated computers or co-located with other roles on the same computer or computers. For example, an Edge Server computer that has the Access Edge Server and Web Conferencing Edge Server co-located on it is hosting two server roles.

SIP

Session Initiation Protocol, a signaling protocol for Internet telephony.

SIP peer

Used in Speech Server, they are trusted external components that provide telephony integration with Speech Server.

solo WebMux

This is how we describe a WebMux deployment with a single WebMux (as opposed to dual WebMux).

Speech Server

This is the term used for both the Speech Server product and also the primary servers used by the product.

SRV record

DNS SRV record. Service location record.

SSL

Secure Socket Layer protocol. A cryptographic protocol designed to provide secure communications between two applications. Succeeded by TLS protocol.

SSL key

See SSL/TLS key.

SSL certificate

See SSL/TLS certificate.

SSL port

If SSL/TLS termination is being performed by WebMux on behalf of servers in this farm, this is the port that will receive encrypted traffic. (The clear-traffic port to which traffic will be sent to the servers is specified in the Port field.)

SSL/TLS key

See SSL/TLS certificate.

SSL/TLS certificate

The digital certificate used to identify and authenticate sites communicating with each other via SSL or TLS protocol.

SSL/TLS certificate size

The number of bytes contained in an SSL or TLS certificate. Larger certificate sizes are more secure but take more resources to process.

Standard Edition Server as Director

A Standard Edition Server being deployed as a Director, where most Office Communications Server 2007 server roles have been deactivated.

static route

A fixed path between devices.

STP

Spanning Tree Protocol. A protocol that prevents switching loops in networks with redundant switched paths.

STP switch

A network switch that supports STP (Spanning Tree Protocol). If deploying a dual WebMux configuration with Transparent networking mode, switches are required to be STP capable.

subnet

Short for subnetwork. A range of logical addresses that have the effect of breaking a network up into smaller networks.

TCP-level affinity

See connection persistence.

Telephony Conferencing Server

An Office Communications Server 2007 server role that facilitates audio conference integration with external telephony conference services. In the Office Communications Server 2007 Standard configuration, the Telephony Conferencing Server is installed on the Front End server along with other Office Communications Server 2007 servers; in the Consolidated configuration, it is installed on every Front End Server; in the Expanded configuration, it is installed on one or more separate, dedicated computers in the Enterprise pool.

TLS

Transport Layer Security protocol. A cryptographic protocol designed to provide secure communications between two applications. Successor to SSL protocol.

TLS key

See SSL/TLS certificate.

TLS certificate

See SSL/TLS certificate.

Transparent mode

A two-arm WebMux networking mode in which load-balanced servers appear to be on the same network as other devices (as if WebMux was not there).

trunking

A feature of WebMux model 680PG which aggregates multiple ports on the WebMux to achieve higher bandwidth, working in conjunction with LACP switches.

two-arm mode

Describes a network device's connection to the network: in one-arm mode, traffic passes through the device in one direction only (whereas in two-arm mode traffic passes through the device in both directions).

VIP

Same as VIP address.

VIP address

Abbreviation for "Virtual IP Address". A "VIP" or "VIP address" is an IP address that is not assigned to a specific computer or network appliance but, in the case of WebMux, is assigned to a farm or a MAP rule. VIPs are made addressable by configuration in a DNS server or hosts file and in Office Communications Server 2007 are typically associated with an FQDN by which the farm is addressed.

virtual server.

A group of multiple servers having the same content that are members of a WebMux farm, such as Front End Servers and Edge Servers having the same role.

Web Components Server

An Office Communications Server 2007 server role that uses IIS (Microsoft Internet Information Server) and that facilitates operations like Address Book Downloads and group expansion. In the Office Communications Server 2007 Standard configuration, the Web Components Server is installed on the Front End server along with other Office Communications Server 2007 servers; in the Consolidated configuration, it is installed on every Front End Server; in the Expanded configuration, it is installed on one or more separate, dedicated computers in the Enterprise pool. Although the Web Components Server runs IIS, it is not the same as an external web farm, which may also be required in an Office Communications Server 2007 implementation.

Web Conferencing Server

An Office Communications Server 2007 server role that enables multiparty data collaboration and application sharing. In the Office Communications Server 2007 Standard configuration, the Web Conferencing Server is installed on the Front End server along with other Office Communications Server 2007 servers; in the Consolidated configuration, it is installed on every Front End Server; in the Expanded configuration, it is installed on one or more separate, dedicated computers in the Enterprise pool.

Web farm

One or more servers hosting web content. In Office Communications Server 2007, a web farm may be used as part of an Edge deployment and by Speech Server. It is not the same as the Web Components Server role.

Web server

A server hosting content and installed with Microsoft Internet Information Services (IIS), which within Office Communications Server 2007 can vary based on what component or module it is servicing.

WebMux

This is the name of CAI Networks' load balancer / traffic manager appliance product, and also used to refer to a unit of the product.

WLBS

Windows NT Load Balancing Service (WLBS)

Index

A/V Conferencing Server	153	Web farm	139
affinity		Web Farm	42
port.....	23	Director	154
TCP-level	22	director WebMux.....	28, 30, 32
array	6, 153	dispatch method	154
Array of Directors	32, 108, 153	DMZ	154
Array of Standard Edition Servers as a		DNS	71, 154
Director.....	See Array of Directors	DoS attack	154
attack protection	70, 76, 93, 96	downtime	
availability	10	planned.....	11
Back-End Database server.....	153	unplanned	10
backup WebMux configuration.....	93	dual Webmux	154
central location	See central site	dual WebMux configuration.....	72
central site.....	7	Edge Server	154
certificate	153	Enterprise Edition Configurations.....	105
collocation	153	Enterprise Edition Consolidated	
Communicator Web Access \b.....	141	Configuration	28
connection persistence	7, 22, 154	Enterprise Edition Expanded Configuration	30
CSR	154	Enterprise pool.....	155
data center.....	7	Enterprise server.....	155
DDoS attack.....	154	epool WebMux	155
deployment		external DNS.....	155
Array of Directors.....	32, 108	external interface of server.....	6
Communicator Web Access.....	141	external IP address.....	155
Edge topologies	34	external load balancer.....	6
Enterprise Edition Consolidated		external network	155
Configuration.....	28, 105	external web farm	155
Enterprise Edition Expanded Configuration		failover	
.....	30, 105	effect of multifarming.....	22
external web farm	139	farm	6, 156
HTTP Reverse Proxy Servers or ISA		IP address.....	69
Servers	41	network addressing	71
ISA Servers	41	farms	
ISA Servers	138	adding	87
Multiple Site with a Remote Site Edge		configurations.....	19, 97, 98
Topology.....	36, 38, 118	configuring	77
Multiple Site with a Scaled Remote Site		multifarming	20
Edge Topology	126, 133	network addressing	18
Reverse Proxy Servers.....	138	relationship to servers	12
Scaled Single-Site Edge Topology	34, 111	farms \b.....	12
Speech Server.....	147	firewall	19
Standard Edition	28	Firewall rules	71
Web Components Servers	107	firmware revision level	73

FQDN.....	70, 155	WebMux	73
Front End Server	156	networking mode	13, 67, 96
front end WebMux	28, 30, 155	networking modes	
hardware load balancer	6, 156	comparison table	16
health checking		NLB	157
effect of multifarming	22	Office Communications Server 2007	
hosts file.....	71	requirement for WebMux	20
HTTP Reverse Proxy Server	<i>See</i> Reverse proxy	one-arm mode	158
HTTP Reverse Proxy Servers.....	41	OOP mode.....	<i>See</i> Out-of-Path mode
IM Conferencing Server	156	outer perimeter WebMux	6, 158
inner perimeter WebMux.....	6, 156	Out-of-Path mode	15, 158
internal DNS	156	performance	10, 63
internal interface of server.....	6	perimeter network.....	158
internal IP address	156	persistence... <i>See</i> connection persistence, <i>See</i> connection persistence	
internal load balancer.....	6	pool.....	6, 158
internal network.....	156	pool configurations.....	158
IP address.....	69	port	
farm.....	69	assignments	70
MAP rule.....	69	port affinity	23, 158
server	69	ports	18, 97, 101
WebMux.....	69	assignment	18
ISA Server	157	blocking	19
ISA Servers.....	41, 138	effect of MAP.....	19
labels	67	values	19
LACP	157	protocol	7, 158
LACP switch	157	public interface of server.....	6
Layer 7	23	quiescing	
local location	<i>See</i> local site	effect of multifarming.....	22, 23, 24
local site	7	reliability	10
reference topology	50	remote location	<i>See</i> remote location
WebMux deployment for	50	remote site	7
logical load balancer	157	reference topology	52
loopback adapter	157	WebMux deployment for	52
Main Management Console.....	157	reset timeouts	96
Management Console.....	157	Reverse proxy	159
logging in	74	Reverse Proxy	7
MAP capability.....	23, 157	Reverse Proxy Servers	138
MAP rule	18	role.....	<i>See</i> server role
IP address	69	Router LAN	159
MAP rules		RSA	159
adding	89	run state	
configuring	78	effect of multifarming.....	22
multifarming	20	scalability	10
considerations	21	Scaled Single-Site Edge Topology	34, 111
Multiple Site with a Remote Site Edge		scheduling method.....	68, 159
Topology	36, 118	effect of multifarming.....	21
Multiple Site with a Scaled Remote Site Edge		scheduling methods	103
Topology	38, 126, 133	server	6
NAT mode	14, 157	IP address.....	69
network addressing	16	network addressing	70

Server	6	TCP-level affinity	7, 22, <i>See</i> connection persistence
server array	159	Telephony Conferencing Server	161
Server LAN	159	Terminology	5
Server LAN Gateway	75	TLS	25, 161, <i>See</i> SSL/TLS
server role	159	TLS certificate	<i>See</i> SSL/TLS certificate
server weight	<i>See</i> weight	TLS key	<i>See</i> SSL/TLS certificate
servers		Transparent mode	14, 161
adding	90	trunking	161
addressing	17	two-arm mode	162
configuring in WebMux	79	VIP	69, 162
network addressing	18	VIP address	162
relationship to farms	12	virtual server	6, 7, 162
relationship to WebMux	13	Web Components Server	162
service	7	Web Components Servers	32, 107
services	97, 101	Web Conferencing Server	162
SIP	160	Web farm	139, 162
SIP peer	160	Web Farm	42
solo Webmux	160	Web server	162
Speech Server	147	WebMux	6, 9, 163
SRV record	160	Administration settings	75
SSL	160, <i>See</i> SSL/TLS	Administrative settings	82
SSL certificate	<i>See</i> SSL/TLS certificate	Basic settings	75
SSL key	<i>See</i> SSL/TLS key	benefits	10
SSL/TLS		concepts	11
acceleration	24	configuring	73
certificate management	24	domain name	75
certificates	76	firewall	19
offloading	24	functional view	12
termination	24	host name	75
SSL/TLS certificate	160	how many required	58
SSL/TLS key	<i>See</i> SSL/TLS certificate	installing	71
SSL/TLS Offloading	10	models	63
SSL/TLS setup	84	network addressing	73
Standard Edition	28	network view	13
Standard Edition Server as Director	160	Office Communications Server 2007	
static route	161	requirements for	20
static routes	19	overview	11
STP	161	relationship to servers	13
STP switch	161	settings	95, 96
Stranded TCP Connection Reset	76	setup	81
subnet	161	weight	68
TCP idle timeout	80	effect of multifarming	21
TCP idle timeout retry interval	92	example of effect	69
TCP retry interval	80, 97	WLBS	163
TCP timeout	96		