Load Balancing Exchange 2010 OWA for External Access using WebMux

Published: April 2011

Contents

Introduction

This guide will outline how to implement the WebMux hardware load balancer with Microsoft Exchange 2010 Outlook Web Access (OWA) for external user access and using the WebMux for SSL offloading and high availability.

Planning and Deployment Overview

Implementing the WebMux for OWA includes the following tasks:

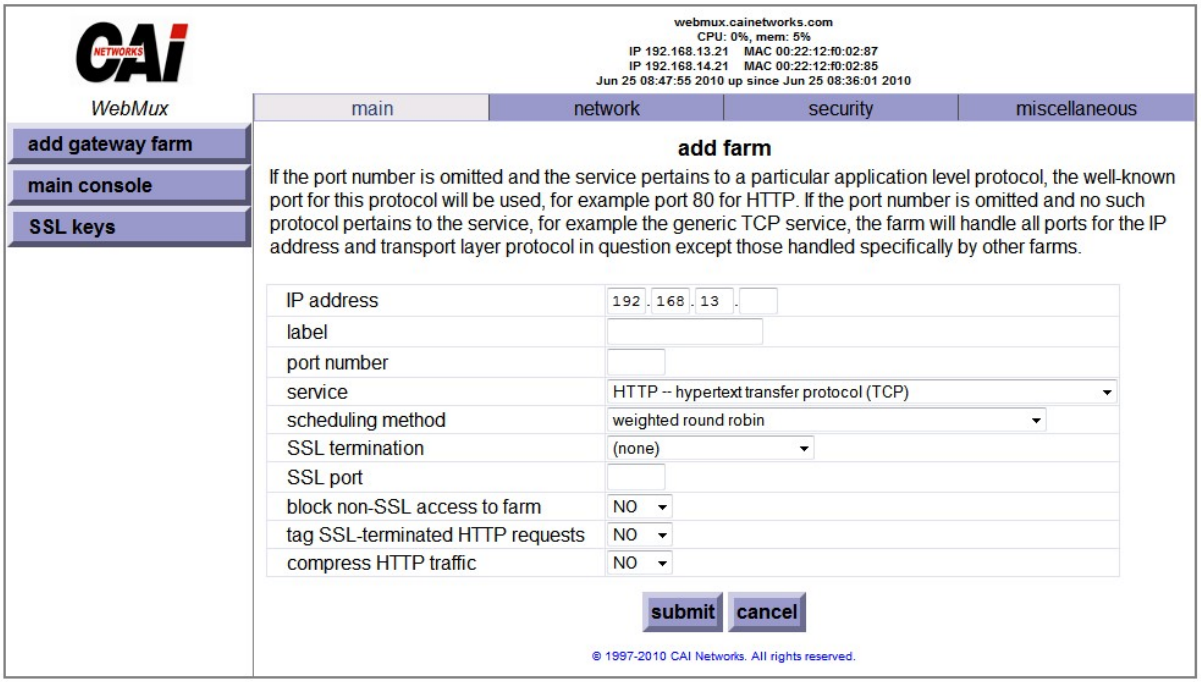
- Setting up the WebMux for SSL offloading and OWA high availability
- Configuring the CAS for external access
- Configuring the CAS for SSL offloading
- Updating the DNS for the FQDN for external OWA access through the Farm IP

Chapter 1: Configuring the WebMux

For the simplest configuration, we recommend that you configure your WebMux to run in Single Network Mode. The following instructions assume that you are running in Single Network Mode. Please refer to the WebMux user manual for details about configuring the WebMux to run in Single Network Mode if you have done so already.

We recommend offloading the SSL termination on the WebMux instead of on the servers so that you will only have to worry about one certificate for the single FQDN you will be using. You should already have a valid key and certificate imported in the WebMux to use for the OWA farm. Please refer to the WebMux user manual regarding importing SSL keys and certificates if you have not done so already.

- Create a new farm by clicking on the "Add Farm" button on the left side of the main console screen.



webmux.cainetworks.com
CPU: 0%, mem: 5%
IP 192.168.13.21 MAC 00:22:12:f0:02:87
IP 192.168.14.21 MAC 00:22:12:f0:02:85
Jun 25 08:47:55 2010 up since Jun 25 08:36:01 2010

add farm

If the port number is omitted and the service pertains to a particular application level protocol, the well-known port for this protocol will be used, for example port 80 for HTTP. If the port number is omitted and no such protocol pertains to the service, for example the generic TCP service, the farm will handle all ports for the IP address and transport layer protocol in question except those handled specifically by other farms.

IP address	192 . 168 . 13 .
label	
port number	
service	HTTP -- hypertext transfer protocol (TCP)
scheduling method	weighted round robin
SSL termination	(none)
SSL port	
block non-SSL access to farm	NO
tag SSL-terminated HTTP requests	NO
compress HTTP traffic	NO

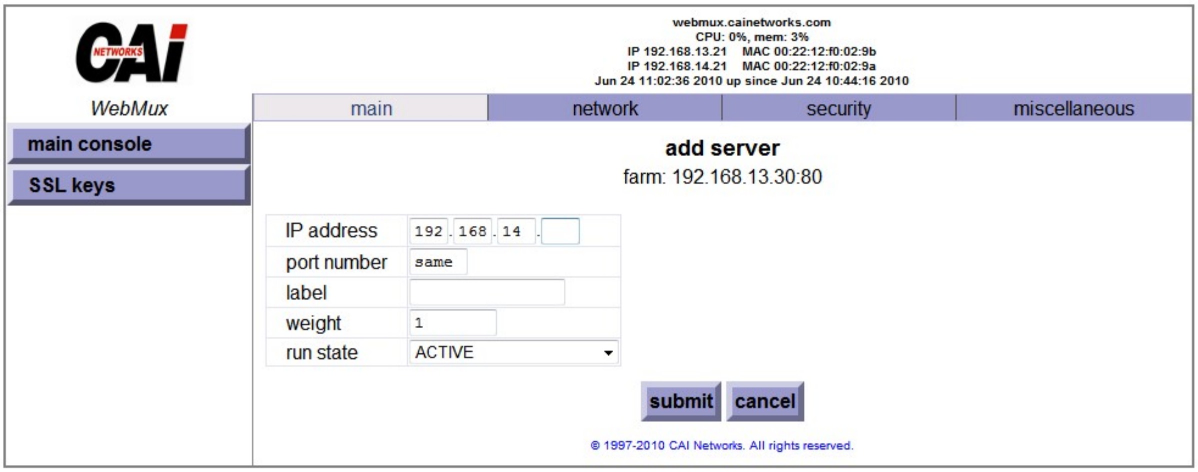
© 1997-2010 CAI Networks. All rights reserved.

Figure 1 Example of the Add Farm screen

- In the Add Farm screen, enter the IP address for the farm. This will be the IP address you will use to point the external Client Access FQDN in your DNS.
- For the service, select "HTTP - hypertext transfer protocol (TCP)"
- For the scheduling method, select "round robin - persistent"

- In the SSL termination field, select the key/cert slot you imported you SSL key and certificate in.
- Submit the page and you will have a new farm entry in the main console.

Next you will add the servers in the farm. Click on the radio button next the the farm IP and then click on the “Add Server” button on the left of the screen.



webmux.cainetworks.com
CPU: 0%, mem: 3%
IP 192.168.13.21 MAC 00:22:12:f0:02:9b
IP 192.168.14.21 MAC 00:22:12:f0:02:9a
Jun 24 11:02:36 2010 up since Jun 24 10:44:16 2010

add server

farm: 192.168.13.30:80

IP address	192 . 168 . 14 .
port number	same
label	
weight	1
run state	ACTIVE

© 1997-2010 CAI Networks. All rights reserved.

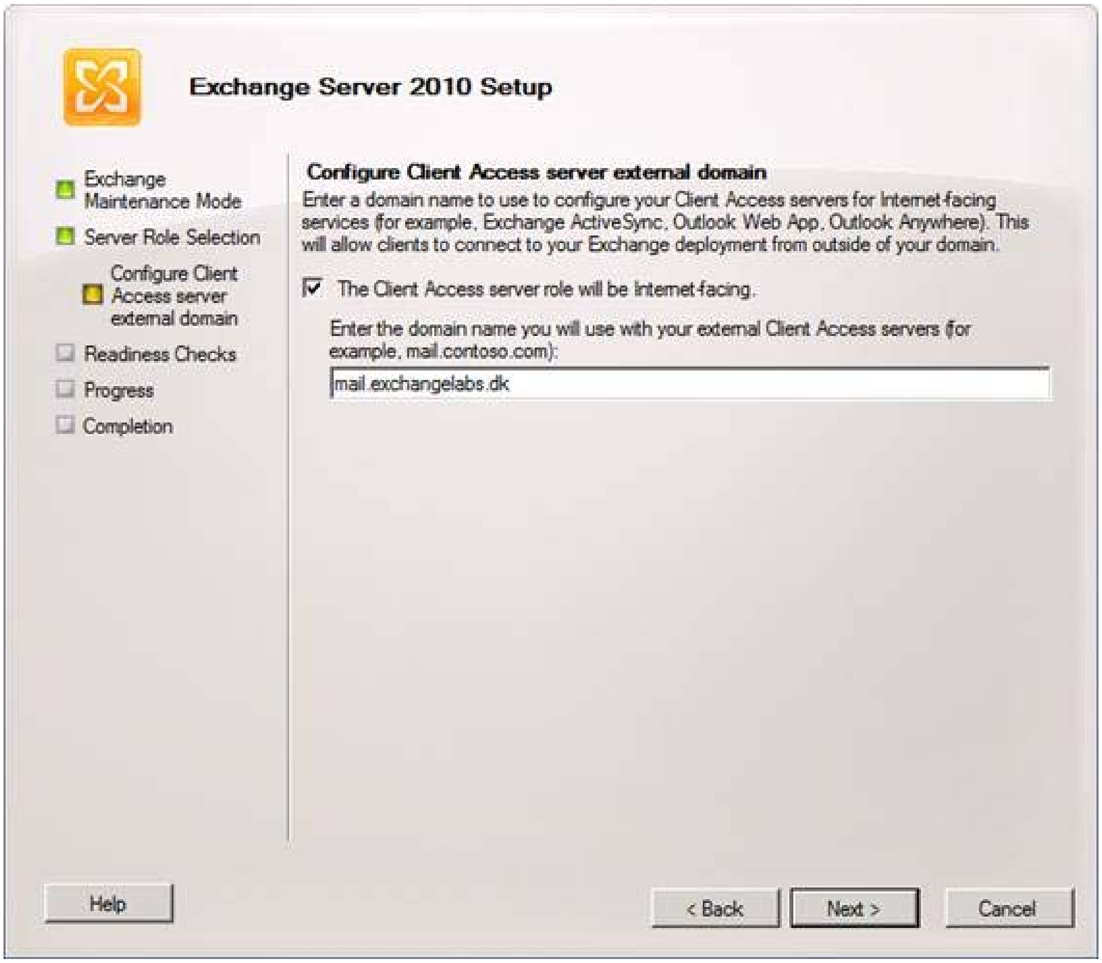
Figure 2 Example of the Add Server screen

- Enter the real IP address of the CAS and click the submit button.
- Repeat adding the IP address for all the CAS in your Exchange 2010 system.

This completes the WebMux configuration.

Chapter 2: Configuring CAS

On each of the CAS, you will need to configure the external domain. When you first set up the CAS, you were presented with this screen:



Exchange Server 2010 Setup

- Exchange Maintenance Mode
- Server Role Selection
- Configure Client Access server external domain
- Readiness Checks
- Progress
- Completion

Configure Client Access server external domain

Enter a domain name to use to configure your Client Access servers for Internet-facing services (for example, Exchange ActiveSync, Outlook Web App, Outlook Anywhere). This will allow clients to connect to your Exchange deployment from outside of your domain.

☑ The Client Access server role will be Internet-facing.

Enter the domain name you will use with your external Client Access servers (for example, mail.contoso.com):

mail.exchangelabs.dk

Figure 3 Configure Client Access server external domain

Be sure to check the “Client Access server role will be Internet-facing” option and enter the domain name you will use. If did not configure this portion in your initial CAS setup, you can still do so using the Exchange Management Console.

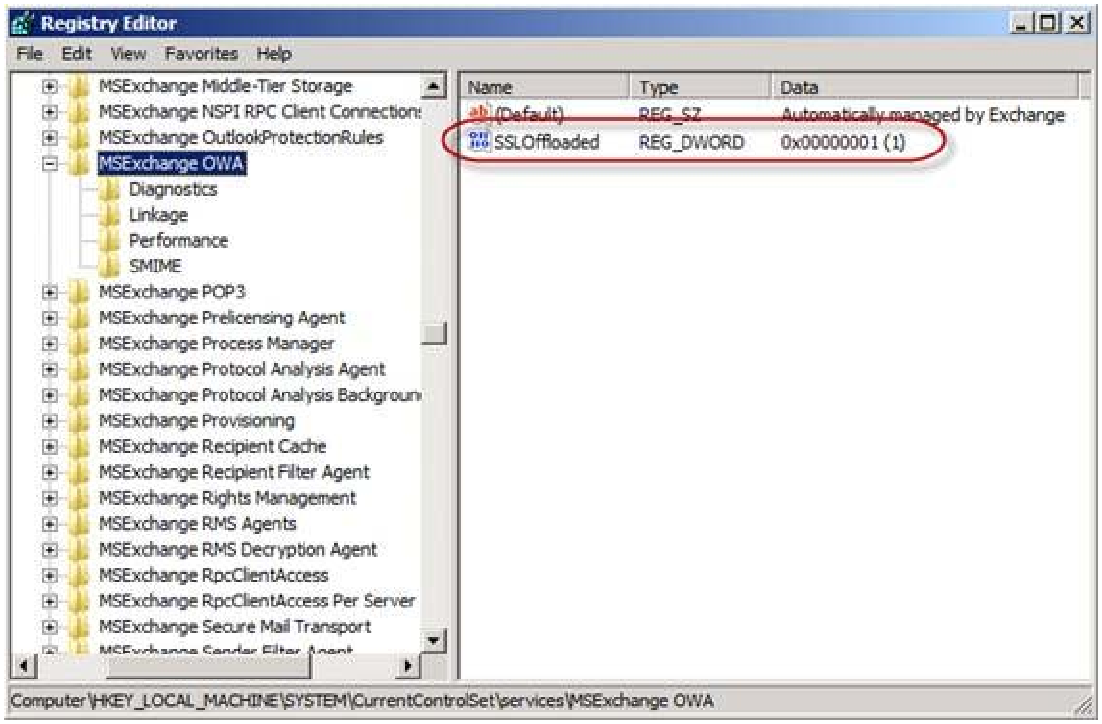
Since you will be offloading SSL termination on the WebMux, you will need to make a couple of changes on each CAS in the CAS array.

First you need to add an SSL offload REG_DWORD key:

Open “regedit” and search for

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA

Under this registry key, create a new REG_DWORD key called “SSLOffloaded” and set the value to “1”.


Registry Editor
File
Edit
View
Favorites
Help
MSExchange Middle-Tier Storage
MSExchange NSPI RPC Client Connections
MSExchange OutlookProtectionRules
MSExchange OWA
Diagnostics
Linkage
Performance
SMIME
MSExchange POP3
MSExchange Prelicensing Agent
MSExchange Process Manager
MSExchange Protocol Analysis Agent
MSExchange Protocol Analysis Backgroun
MSExchange Provisioning
MSExchange Recipient Cache
MSExchange Recipient Filter Agent
MSExchange Rights Management
MSExchange RMS Agents
MSExchange RMS Decryption Agent
MSExchange RpcClientAccess
MSExchange RpcClientAccess Per Server
MSExchange Secure Mail Transport
MSExchange Sender Filter Agent

Name	Type	Data
(Default)	REG_SZ	Automatically managed by Exchange
SSLOffloaded	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchange OWA

Figure 4 Windows Registry Entry

Next, we need to disable the SSL requirement on the OWA virtual directory.

Open the IIS Manager and look for the "OWA" virtual directory inside the "Default Web Site".

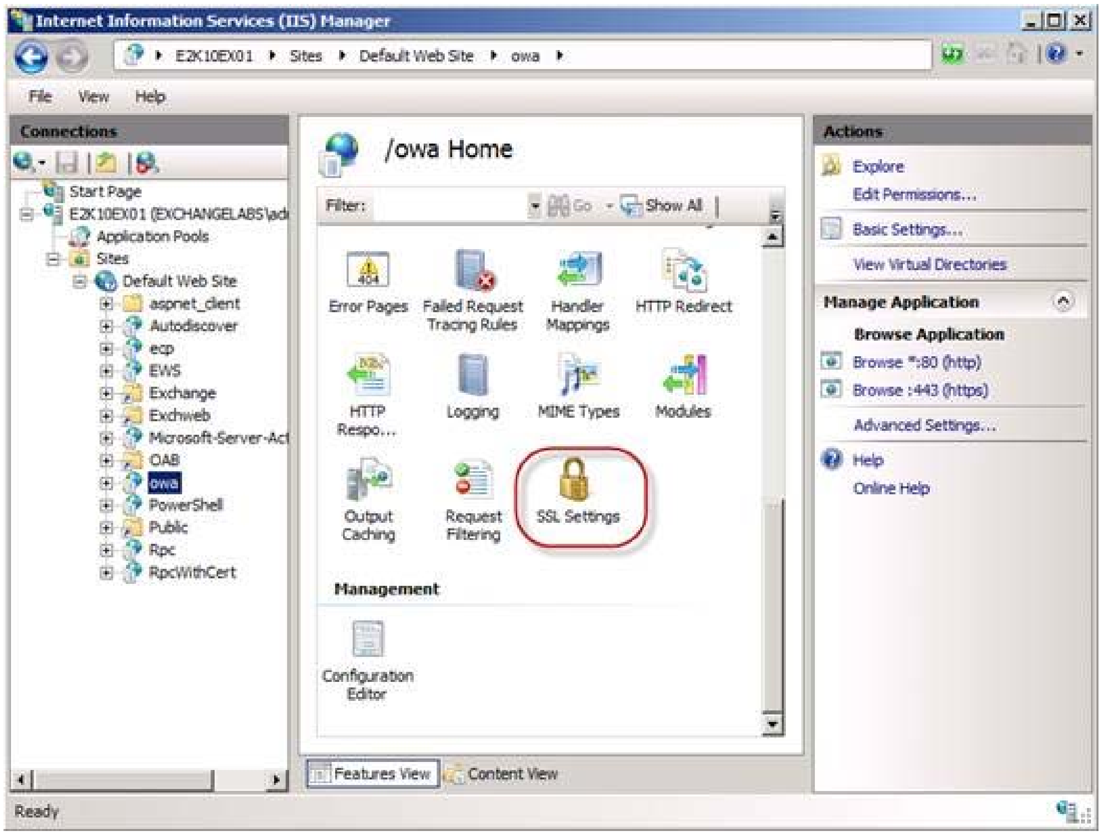
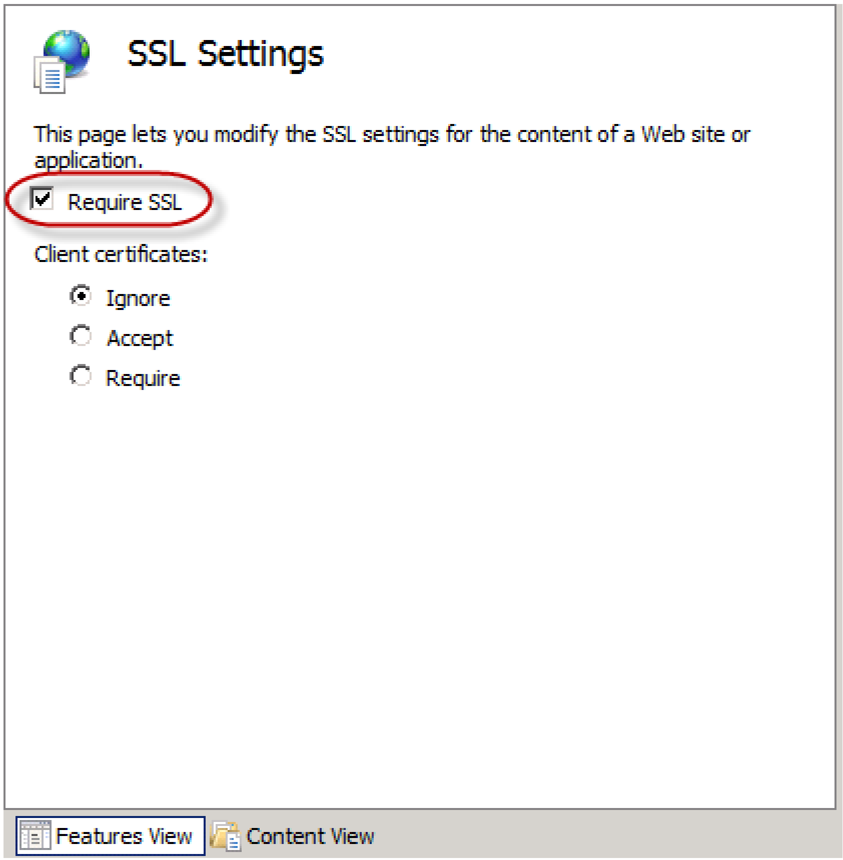


Figure 5 IIS Management

Click on the “owa” virtual directory and then open the “SSL Settings”



SSL Settings

This page lets you modify the SSL settings for the content of a Web site or application.

☑ Require SSL

Client certificates:

● Ignore

○ Accept

○ Require

Figure 6 SSL Settings

Inside the “SSL Settings” uncheck “Require SSL” and click “Apply”.

Finally, restart the IIS service by running “iisreset /noforce” on the command line or by rebooting the server.

Chapter 3: External DNS records.

Lastly, you need to point your external DNS record to the Farm IP of the WebMux. You should now be able to access OWA from the internet.