WebMux™ Network Traffic Manager

AVANU®

Virtual WebMux™ Edition
AVANU®
It is All About the User Experience on Your Network and Keeping Everyone Connected™
Virtual WebMux™
Network Traffic Manager
Managing, Controlling, and Securing Local Network
Layers 4-7 Traffic Load Balancing Solution
WEBMUX NETWORK TRAFFIC MANAGER
A400X
AVANU

WebMux Setup Guide for Microsoft Exchange® Server

Version 11.xx

Edition April 2015

www.avanu.com

Table of Contents

Table of Figures

Introduction

It takes only minutes to configure the AVANU WebMux Network Traffic Management appliance, a hardware load balancer (HLB), for load-balancing Microsoft® Exchange. You will need to know your architecture, network topology, protocols, and how the load balancer integrates into your environment, but AVANU provides a wizard on the WebMux that will guide you through the details.

Note that there are separate wizards for Exchange 2010 and Exchange 2013 due to differences in load-balancing requirements. Exchange 2010 requires Layer 7 load-balancing to support use of cookies and, therefore, also requires SSL termination by the WebMux to use the cookies. The Exchange 2010 wizard automatically accommodates these requirements, configuring the decryption and setting up the load balancer created cookie.

The wizard includes an option to leave the connections behind the WebMux decrypted to port 80 instead of being re-encrypted to port 443. The default setting is to re-encrypt despite the load on the WebMux and the CAS servers. That is because not re-encrypting requires you to perform additional steps on the Exchange side and because re-encrypting is more secure. The section of the wizard on CAS Array configuration addresses your re-encryption options in more detail.

There are also instructions for configuring static ports for RPC services in Exchange 2010. Please review that information carefully when you come to it. The WebMux wizard for exchange 2010 assumes that you follow the instructions for Registry changes to set RPC to use ports 65533 and 65534. (Exchange 2013 uses RPC/HTTP, RPC over HTTP, for internal and external connectivity, eliminating the need for static RPC/TCP ports, so those steps should be ignored for Exchange 2013 environments. Just follow the Exchange 2013 wizard.)

You may also perform an additional series of steps, after the wizard finishes, for configuring management e-mail notification, Syslog, SNMP, and setting the password.

The wizard itself does not handle separate IP addresses for OWA and Hub Transport services but this guide provides the steps to make those configurations. Those, and other topics, will be addressed in the section titled “Finishing.”

The WebMux Configuration Wizard for Exchange

This section details the Exchange configuration Wizard that you will run on the WebMux. It shows you the screens that you will fill in. The wizard assumes that you have the answers, but don't worry if you don't. Just consult the sections of this document that explain those additional details.

Connect to the WebMux

Follow the Quick Start Guide to get your WebMux powered and on the network. At a minimum you will have configured an IP address for the "MGMT" port—so that you can manage the WebMux on the dedicated port (preferably, for security, on a separate ethernet LAN from the load-balanced traffic). Reach the wizard web interface of the WebMux by going to:

```
https://<WebMux_IP_Address>:35/exchange2010
```

or

```
https://<WebMux_IP_Address>:35/exchange2013
```

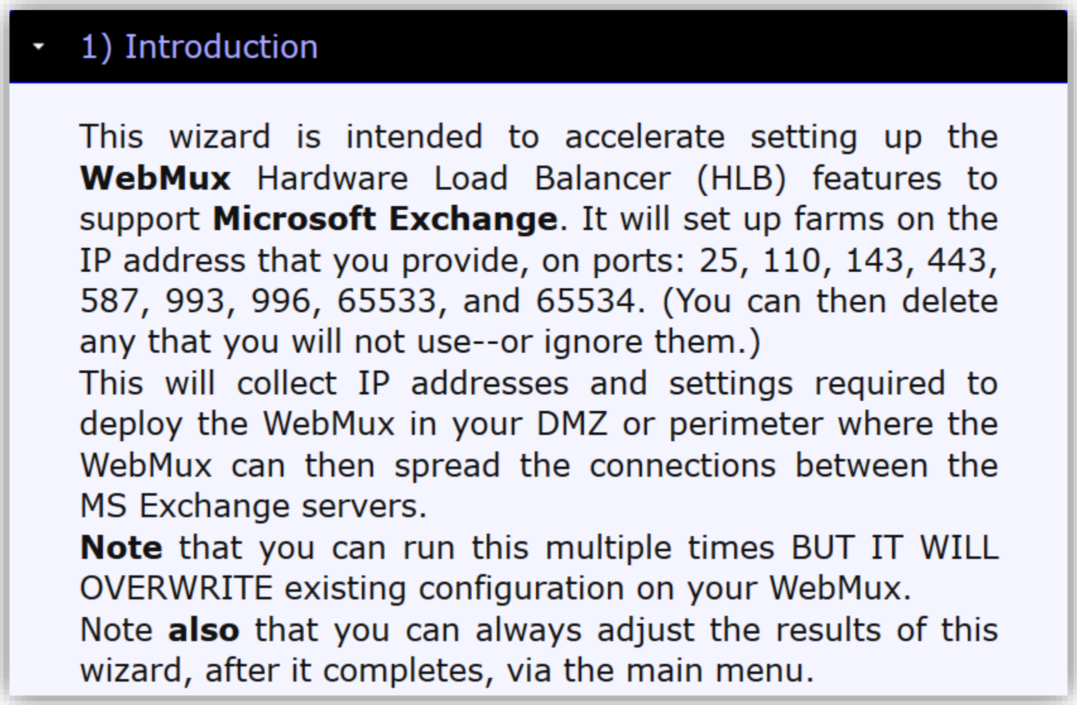
The two wizards require nearly identical input but will output different configurations because Exchange 2010 requires Layer 7 load balancing—and, therefore, TLS termination/decryption.

Now to walk you through the wizard. You should be able to answer the prompts, click through the configuration sections, provide the "superuser" management password, and have the WebMux up and running in minutes.

Introduction

You will see the wizard's "Introduction" once you've connected to one of the URLs above. The introduction tells you the basics of what the wizard does as well as how to navigate the wizard itself.

Note that you will not “time out” when using the wizard. You may take as long as you wish to consult Exchange documentation whenever you want.



1) Introduction

This wizard is intended to accelerate setting up the **WebMux** Hardware Load Balancer (HLB) features to support **Microsoft Exchange**. It will set up farms on the IP address that you provide, on ports: 25, 110, 143, 443, 587, 993, 996, 65533, and 65534. (You can then delete any that you will not use--or ignore them.)
This will collect IP addresses and settings required to deploy the WebMux in your DMZ or perimeter where the WebMux can then spread the connections between the MS Exchange servers.
Note that you can run this multiple times BUT IT WILL OVERWRITE existing configuration on your WebMux.
Note **also** that you can always adjust the results of this wizard, after it completes, via the main menu.

Figure 1 Exchange 2010 Wizard Introduction

Select the WebMux Architecture on the Network

The WebMux can be configured in one of four architectures, two are called “**1-Arm**” and two “**2-Arm**.” They are explained in detail below but, in brief, 2-Arm configurations are for **Network Address Translation (NAT)**, in which the WebMux client-side and server-side are on separate IP subnets and **2-Arm Transparent Bridging**, in which the WebMux client and server connections are on separate Ethernets. The 1-Arm configurations are **1-Arm Single Network** (acting as a proxy) and **1-Arm Direct Server Return**.

The following additional information is provided in a pop-up in the wizard if you need additional background on the “Arms” and network architecture:

2-Arm Network Address Translation (NAT) mode and 1-Arm Direct Server Return (DSR) mode are the most-recommended—though for different purposes. NAT mode is common because it is the only configuration to satisfy a requirement for addresses on two networks/subnets. DSR is the highest-performance option because traffic is balanced on the way in but the server response, back to the client, can bypass the WebMux on return. DSR does require configuration of a "loopback adapter" on each back-end server but that is simple and also not otherwise of significant impact on the server. DSR has no advantage if SSL termination is required on all of the farms, as traffic will have to return through the WebMux, so there are some scenarios where it is suboptimal.
"Arms" just means are there one or two LAN connections (typically "External" and "Internal").

2-Arm NAT, is the **required** configuration when you have two subnets. It is the common "Destination" NAT configuration in which the clients connect to an IP address on the WebMux and the WebMux proxies to the back-end servers. The servers "see" the IP address of the client, as if the WebMux was not there. **This is the required configuration when there are two IP subnets (Internet-side and Internal).**

2-Arm Transparent makes the WebMux an inline bridge--seeing all of the traffic below the IP layer and able to manage traffic without IP address changes. Note that, being a bridge, you must avoid bridge loops--having a circular path through inter-connected bridges. Also, being inline and 2-Arms, the load-balanced traffic flows through the WebMux.

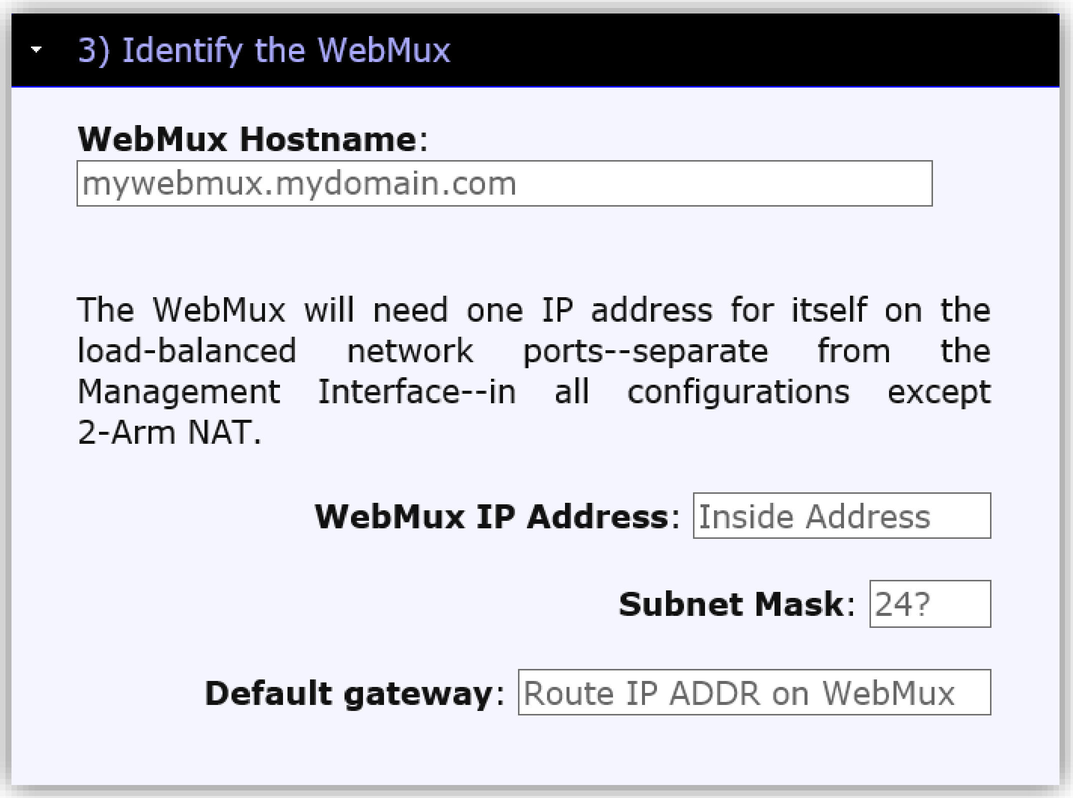
1-Arm "Single Network" is a special case of bridging in which the WebMux bridges internally on one interface (that can be bonded for higher capacity). The bridge loop issue is elimiated. Note that all traffic is **"source NATted" (aka SNAT)—so the WebMux becomes the client** and the server does not see the IP address of the client. A limitation of this configuration is that an additional IP address must be assigned to the WebMux for each 65,000 simultaneous connections--because of that SNAT configuration and client-server relationship. Troubleshooting is also more challenging because the WebMux IP address appears as the client instead of each individual client IP address being logged.

Direct Server Return is the highest-performance option in cases where it is supported, also known as "Direct Routing," or "Out of Path," this makes the WebMux the traffic director for incoming traffic but return traffic can route back bypassing the WebMux (unless the WebMux does TLS termination, as the WebMux will become the client to the server). **Note** that this requires a simple configuration of a "loopback adapter" on the Windows servers.

Refer to the AVANU Technical Tips for more related resources.

Identify the WebMux

You will only need to provide one IP address for the WebMux if you have selected any configuration except NAT. This section of the wizard will change between two modes depending on what you chose in Step 2 (Select the WebMux Architecture on the Network). One input form, shown below, requires just one IP address for the WebMux (because it is not NAT mode):



3) Identify the WebMux

WebMux Hostname: mywebmux.mydomain.com

The WebMux will need one IP address for itself on the load-balanced network ports--separate from the Management Interface--in all configurations except 2-Arm NAT.

WebMux IP Address: Inside Address

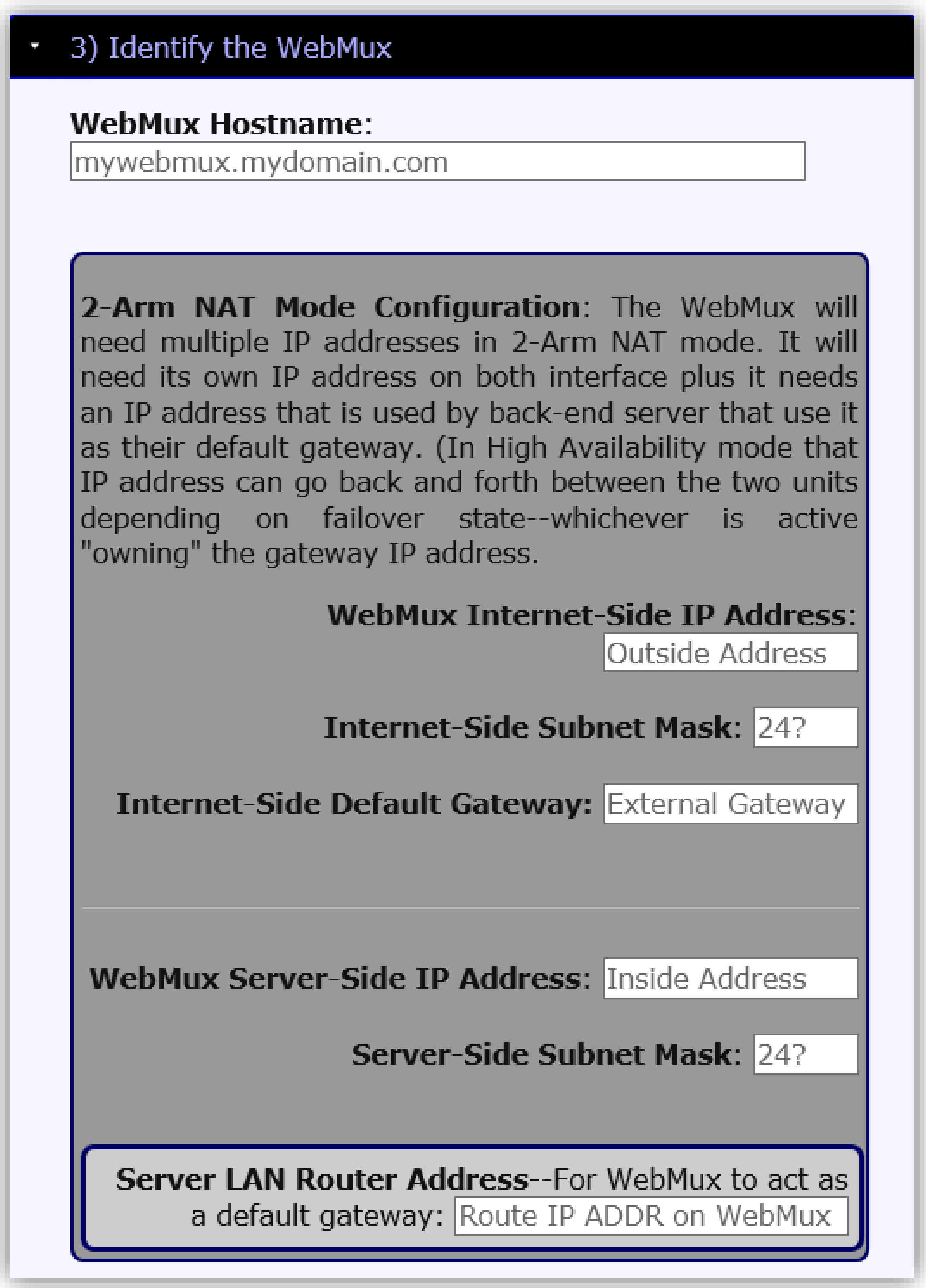
Subnet Mask: 24?

Default gateway: Route IP ADDR on WebMux

Figure 2 Identify the WebMux — Single IP Address

The next page shows the input required if using NAT mode. It not only requires two IP addresses for the WebMux, on two networks but it also requires an IP address that is used by load-balanced servers as their default gateway/router. It is called the "Server LAN Router Address", and its only function is to be the address for traffic returning from the servers on its way back to the clients. This IP address is shared between the two units, floating to whichever unit is active, in a High Availability configuration.

Note the terms, "Internet-Side" versus "Server-Side" in prompting for addresses. The server-side is the interface on which the Exchange servers reside. The clients connect via the "Internet" side.



3) Identify the WebMux

WebMux Hostname: mywebmux.mydomain.com

2-Arm NAT Mode Configuration: The WebMux will need multiple IP addresses in 2-Arm NAT mode. It will need its own IP address on both interface plus it needs an IP address that is used by back-end server that use it as their default gateway. (In High Availability mode that IP address can go back and forth between the two units depending on failover state--whichever is active "owning" the gateway IP address.

WebMux Internet-Side IP Address: Outside Address

Internet-Side Subnet Mask: 24?

Internet-Side Default Gateway: External Gateway

WebMux Server-Side IP Address: Inside Address

Server-Side Subnet Mask: 24?

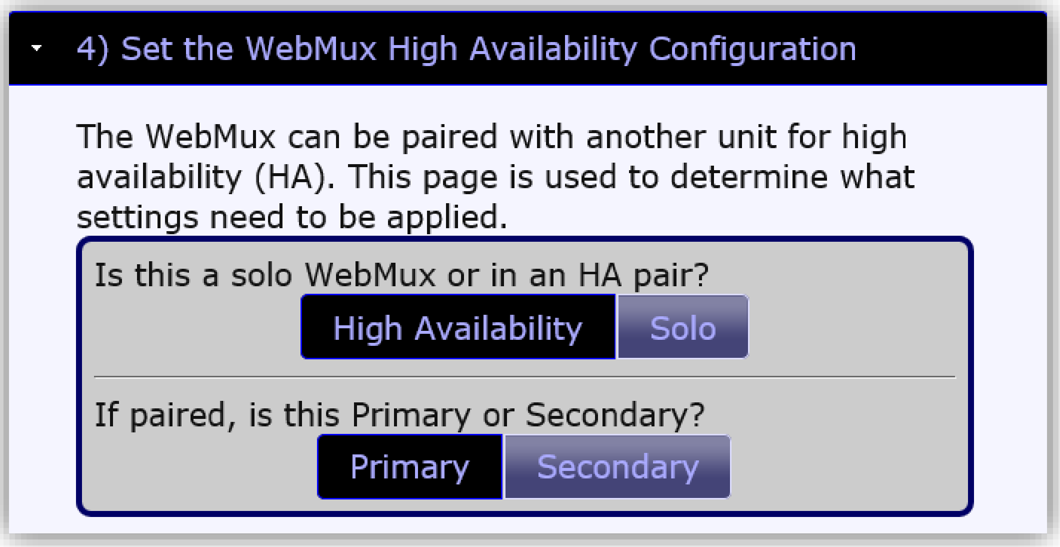
Server LAN Router Address--For WebMux to act as a default gateway: Route IP ADDR on WebMux

Figure 3 Identify the WebMux — Multiple IP Addresses

Set the WebMux High Availability Configuration

The WebMux can run as a solo unit, with no paired unit for redundancy, or it can be paired with another unit—with a LAN cable connecting their "BACKUP" ports—to reduce the possibility of a service failure. The WebMux has two functions, to improve performance by spreading load and to improve availability by reducing single points of failure. It is, therefore, recommended that two WebMux be paired together and powered on separate power circuits.

Selecting "High Availability" and "Secondary" will change the behavior of the wizard to not require input that is entered in the Primary unit. The Secondary will get its farm and server IP addresses, as well as PKI keys and certificates, from the Primary.



4) Set the WebMux High Availability Configuration

The WebMux can be paired with another unit for high availability (HA). This page is used to determine what settings need to be applied.

Is this a solo WebMux or in an HA pair?

If paired, is this Primary or Secondary?

Figure 4 WebMux High Availability Configuration

Farm / Virtual IP Address Configuration

This section defines both the IP address that clients connect to on the WebMux and the IP addresses of the CAS servers handling the load. For that reason the Microsoft instructions for configuring DNS are included at this point. You will also, for Exchange 2010, need to configure TCP ports for RPC services, documented after the Array and DNS definition.

The wizard will configure all Exchange ports, for CAS, OWA, and Hub Transport services on this one address with the expectation that, at worst, there will be ports defined that are not used. The section of this Guide titled "Finishing" provides details for manual changes, after the wizard has completed, to set up separate IP addresses for OWA and Hub Transport services.

Preparing Exchange 2010 Client Access Server for RPC Load-Balancing

The CAS array concept is used in Exchange 2010 for internal RPC/TCP connections. The arrays are configured on Exchange 2010 and then a WebMux farm configured with the IP address of the array to provide the Outlook client endpoint for load-balancing to the CAS servers. The WebMux will host the IP address receiving client connections in place of an individual CAS server and then pass the traffic to CAS servers. The clients will, therefore, need to rely on DNS responses directing traffic to the WebMux Farms/"Virtual IP's" (VIPs). The IP address is tied to the "CAS Array," an object/identity, defined for this puspose.

The following Technet link provides background on the CAS Array object and DNS requirements:

http://blogs.technet.com/b/exchange/archive/2012/03/23/demystifying-the-cas-array-object-part-1.aspx

There are, as mentioned, two parts to configuring for load-balancing: Create the CAS Array Object and assign it an IP Address mapping in DNS. You can check and set the object with **`Get-ClientAccessArray`**, **`New-ClientAccessArray`**, and **`Set-ClientAccessArray`**. From the Microsoft Technet resource on "**`New-ClientAccessArray`**:"

> This example creates the Client Access server array server.contoso.com.
>
> ```
> New-ClientAccessArray -Fqdn server.contoso.com -Site "Redmond" -Name "server.contoso.com"
> ```

Next set the DNS mapping. Pick an IP address for the CAS Array object that you just defined. That IP address is the IP address that you will input into the WebMux wizard as the "CAS Array (Farm/"VIP") Address." Create an 'A' record in DNS for the CAS Array for clients to resolve to the IP address. Per Microsoft's documentation, "This IP address will most likely be the virtual IP (VIP) of the LB reachable only by internal clients. This VIP is where Outlook or any other MAPI/RPC capable application will then connect to gain access to Exchange 2010 mailbox resources."

Related Resources:

Exchange 2010 Management Shell:
https://technet.microsoft.com/en-us/library/dd795097%28v=exchg.141%29.aspx
Exchange 2010 Management Shell CAS Cmdlets:
https://technet.microsoft.com/en-us/library/aa998005%28v=exchg.141%29.aspx

Exchange 2013 Management Shell and Exchange Administration Center (EAC):
https://technet.microsoft.com/en-us/library/bb123778%28v=exchg.150%29.aspx
https://technet.microsoft.com/en-us/library/jj150562%28v=exchg.150%29.aspx

Exchange Load Balancing (mostly about 2013 but with the key 2010 information and links):
https://technet.microsoft.com/en-us/library/jj898588%28v=exchg.150%29.aspx

Setting Static Ports for Load Balancing RPC Services for Exchange 2010

The WebMux configuration wizard for Microsoft Exchange uses ports 65533 and 65534 for Client Access and Address Book services, respectively, and requires registry changes on CAS servers. **This is for Exchange 2010 only.** Refer to Microsoft "Load Balancing Requirements of Exchange Protocols" for full details:

https://technet.microsoft.com/en-us/library/ff625248.aspx

For more background on the RPC-based services for Client Access and Address Book:

https://technet.microsoft.com/en-us/library/ee332317(v=exchg.141).aspx

For explanation of Exchange 2013 and RPC ports as well as affinity refer to:

http://blogs.technet.com/b/exchange/archive/2013/01/25/exchange-2013-client-access-server-role.aspx

The endpoint TCP ports for these services are, by default, allocated by the RPC endpoint manager on the CAS but must be assigned two static ports for load-balancing (one for the RPC Client Access service and the other for Address Book service). Once the ports are statically mapped, as shown below, the traffic will be restricted to ports 135, 65533, and 65534.

Configure two static port mapping for all RPC-based services in the registry as follows:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeRPC\ParametersSystem
Value: TCP/IP Port
Type: DWORD
```

Set that port to 65533 (creating the key if it does not exist). Verify all CAS servers, as well as public folder servers, are set the same so that you don't get any "RPC Server is Unavailable" error messages.

Now for the Exchange Address Book service. Set that too:

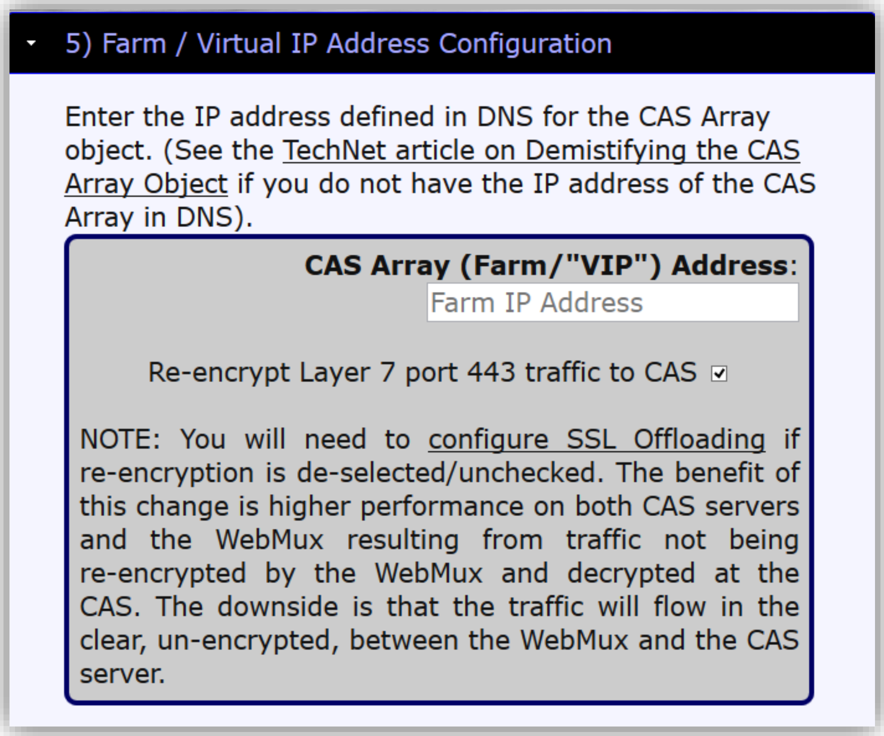
```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeAB\Parameters
Value: RpcTcpPort
Type: REG_SZ (String)
```

Use port 65534. Verify all CAS and Mailbox servers are set.

Restart both the "Microsoft Exchange RPC Client Access" and "Microsoft Exchange Address Book" services after making changes.

You are now ready to provide the IP addresses of the CAS Array and the CAS servers to the WebMux wizard.

NOTE: The checkbox for "Re-encrypt Layer 7 Port 443 traffic to CAS," below, is only for Exchange 2010.
It is not visible in the wizard for Exchange 2013.



▾ 5) Farm / Virtual IP Address Configuration

Enter the IP address defined in DNS for the CAS Array object. (See the TechNet article on Demistifying the CAS Array Object if you do not have the IP address of the CAS Array in DNS).

CAS Array (Farm/"VIP") Address:

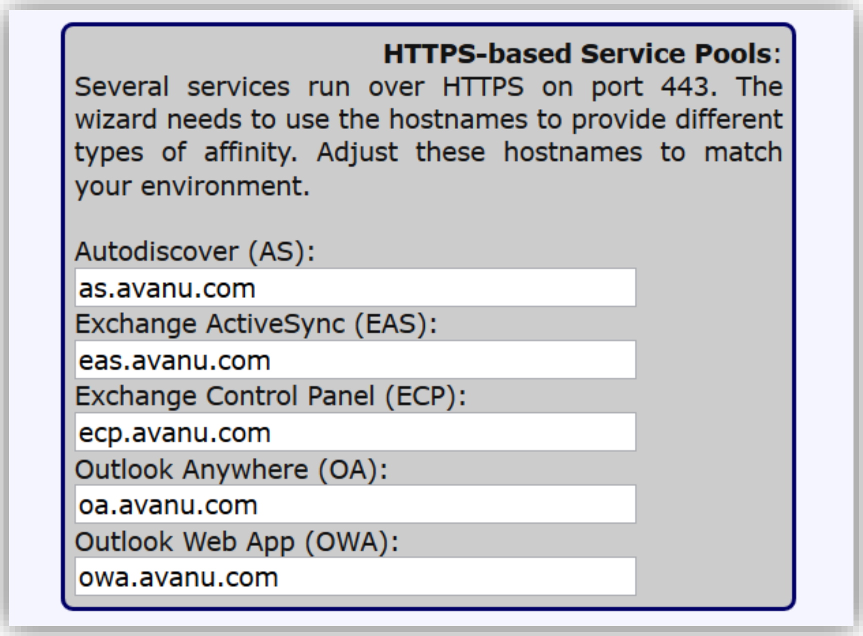
Farm IP Address

Re-encrypt Layer 7 port 443 traffic to CAS ☑

NOTE: You will need to configure SSL Offloading if re-encryption is de-selected/unchecked. The benefit of this change is higher performance on both CAS servers and the WebMux resulting from traffic not being re-encrypted by the WebMux and decrypted at the CAS. The downside is that the traffic will flow in the clear, un-encrypted, between the WebMux and the CAS server.

Figure 5 WebMux CAS Array Farm Settings

You will, also for Exchange 2010 only, see the following Wizard input screen. Exchange 2010 has affinity requirements that vary dependent on client and service capabilities and the WebMux will configure them automatically. Provide the Exchange 2010 service hostname information for each of the following.

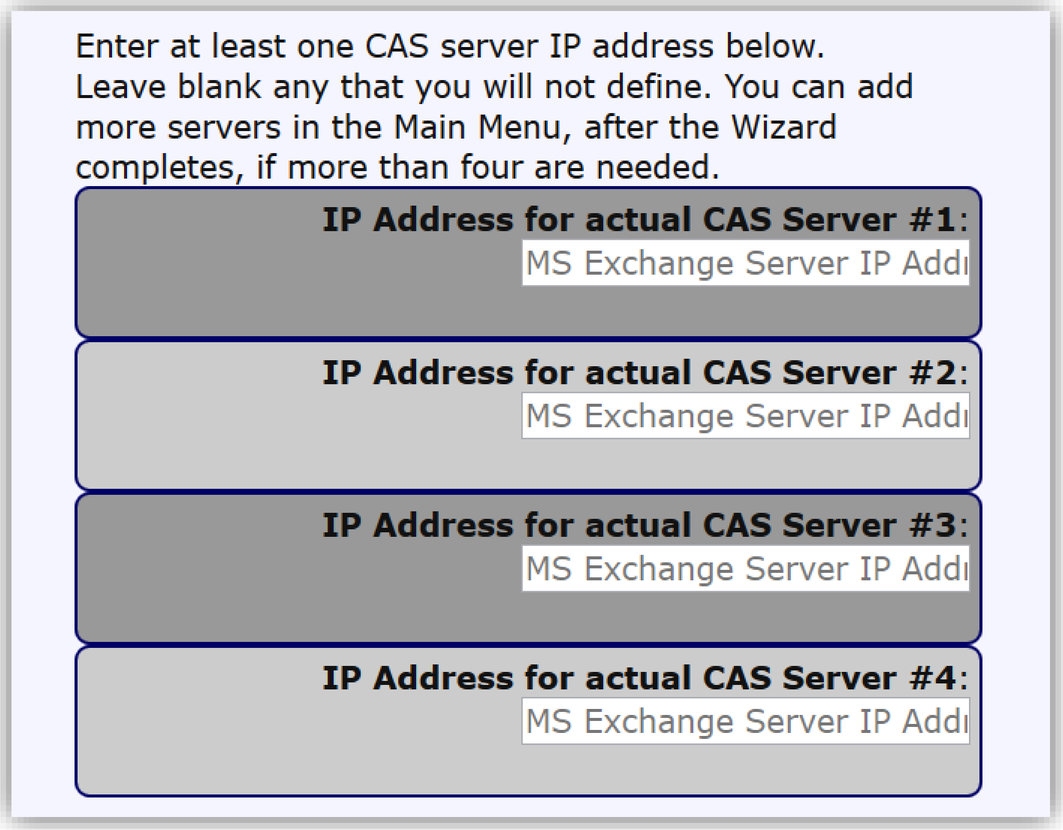


HTTPS-based Service Pools:
Several services run over HTTPS on port 443. The wizard needs to use the hostnames to provide different types of affinity. Adjust these hostnames to match your environment.

Autodiscover (AS):
as.avanu.com
Exchange ActiveSync (EAS):
eas.avanu.com
Exchange Control Panel (ECP):
ecp.avanu.com
Outlook Anywhere (OA):
oa.avanu.com
Outlook Web App (OWA):
owa.avanu.com

Figure 6 Exchange 2010 Hostnames

The next part of Section 5 of the wizard is to enter IP addresses of the individual CAS servers in the array. (This documentation focuses on the CAS array. Additional steps can be followed, later in the instructions, for setting up separate Hub Transport and OWA server farms.) Most sites use two servers but you can add up to four in the wizard and more, manually, once the wizard completes.



Enter at least one CAS server IP address below. Leave blank any that you will not define. You can add more servers in the Main Menu, after the Wizard completes, if more than four are needed.

IP Address for actual CAS Server #1: MS Exchange Server IP Addı

IP Address for actual CAS Server #2: MS Exchange Server IP Addı

IP Address for actual CAS Server #3: MS Exchange Server IP Addı

IP Address for actual CAS Server #4: MS Exchange Server IP Addı

Figure 7 WebMux Farm CAS Servers for Exchange 2013

PKI Key and Certificate Assignment (Exchange 2010 Only)

You will, for Exchange 2010 only, and ony for the Primary unit in a High-Availabilty pair, need to add the PKI key and certificate from Exchange prior to submitting the configuration. This is required for Layer 7 load-balancing of TLS/SSL traffic because the WebMux must be the TLS/SSL endpoint in order to manage the cookie used for affinity (associating a client with a server via the cookie).

Extract PKI Certificates from the Microsoft Exchange CAS server:

http://technet.microsoft.com/en-us/library/dd351274.aspx

NOTE: Remember the password that you assign to the key/cert PFX file as you wil need it below.

Convert PKI Certificates for Import into the WebMux:

1. First, you will need to convert the extracted key and certificate from Personal Information Exchange (PFX) format to Privacy Enhanced Mail (PEM) format into the format used by the WebMux. You can do this by installing OpenSSL and following the instructions provided here or you can send the PFX file to AVANU Technical Support (techsupport@avanu.com) for conversion. There are sites on the Internet which will perform the conversion but you should note that they may retain your private key, even inadvertently, introducing a security vulnerability. If you decide to install OpenSSL then follow along:

    a. Using the PFX file you obtained from Exchange, run:

```
openssl pkcs12 -in mycert.pfx -out mycert.pem
```

    b. Enter your PFX file password when prompted. Then, to extract the private key, run the command:

```
openssl rsa -in mycert.pem -out privatekey.pem
```

    c. If the key and certificate are saved separately, use these commands to convert both.

```
openssl x509 -in input.crt -inform DER -out output.crt -outform PEM

openssl rsa -in input.key -inform DER -out output.key -outform PEM

openssl rsa -in output.key -out newkey.pem
```

2. The final command removes the password from the encrypted key. You will be prompted to enter the password once more while running. You now have the `output.crt` and `newkey.pem`.
3. Open each of the files in Notepad. (Notepad is recommended for opening the files as it will not modify any text. Some editors will substitute character for the original raw text, sometimes as a result of Unicode conversion.)

Upload the certificate to the WebMux:

4. Open another browser window and connect to your WebMux at its IP address and port 35.

```
https://<webmux_IP>:35
```

5. Log in to the WebMux as "superuser"

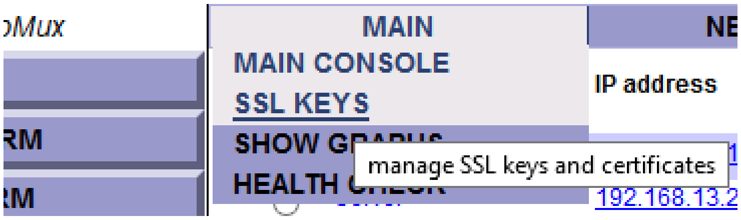
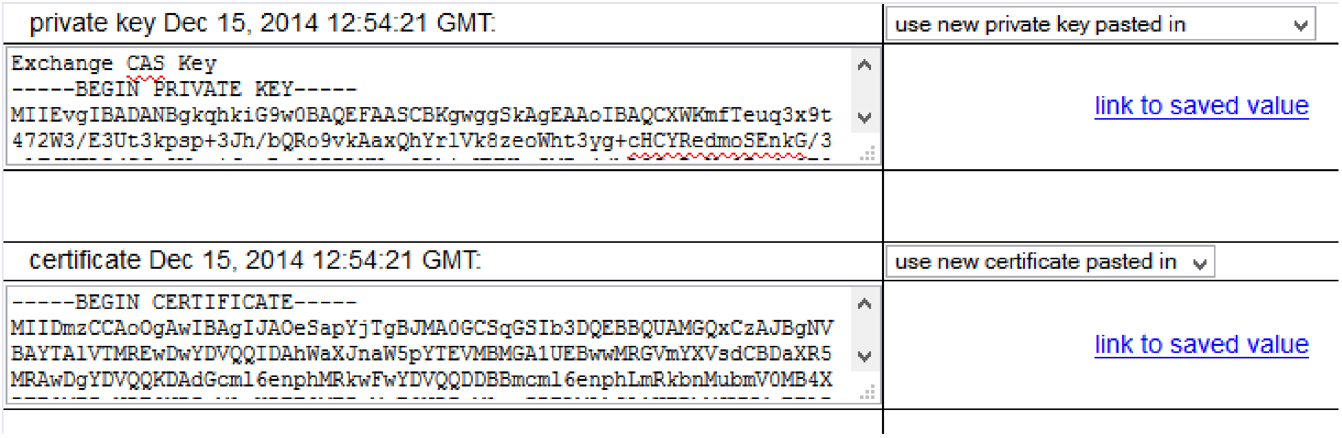


Figure 8 Manage SSL Keys

6. Hover over “MAIN” and select “SSL KEYS”
7. Click on Key number 5.
8. Choose “use new private key pasted in” for both “Key” and “Certificate” sections. Type a label at the beginning of the key, as shown in the example below, and then paste the text of the private key followed by pasting in the text of the certificate (including intermediate certificates) in the “Certificate” section. For both key and cert make sure that you include from the “-----BEGIN” to the “-----END PRIVATE KEY-----” and “-----END CERTIFICATE-----.” Note that it is **very important** to capture all of the text to cut and paste. All of the hyphens at the beginning and end are required.



private key Dec 15, 2014 12:54:21 GMT: use new private key pasted in

```
Exchange CAS Key
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCXWKmfTeuq3x9t
472W3/E3Ut3kpsp+3Jh/bQRo9vkAaxQhYrlVk8zeoWht3yg+cHCYRedmoSEnkG/3
```

certificate Dec 15, 2014 12:54:21 GMT: use new certificate pasted in

```
-----BEGIN CERTIFICATE-----
MIIDmzCCAoOgAwIBAgIJAOeSapYjTgBJMA0GCSqGSIb3DQEBBQUAMGQxCzAJBgNV
BAYTAlVTMREwDwYDVQQIDAhWaXJnaW5pYTEVMBMGA1UEBwwMRGVmYXVsdCBDaXR5
MRAwDgYDVQQKDAdGcml6enphMRkwFwYDVQQDDBBmcml6enphLmRkbnMubmV0MB4X
```

Figure 9 Adding PKI Key and Certificates

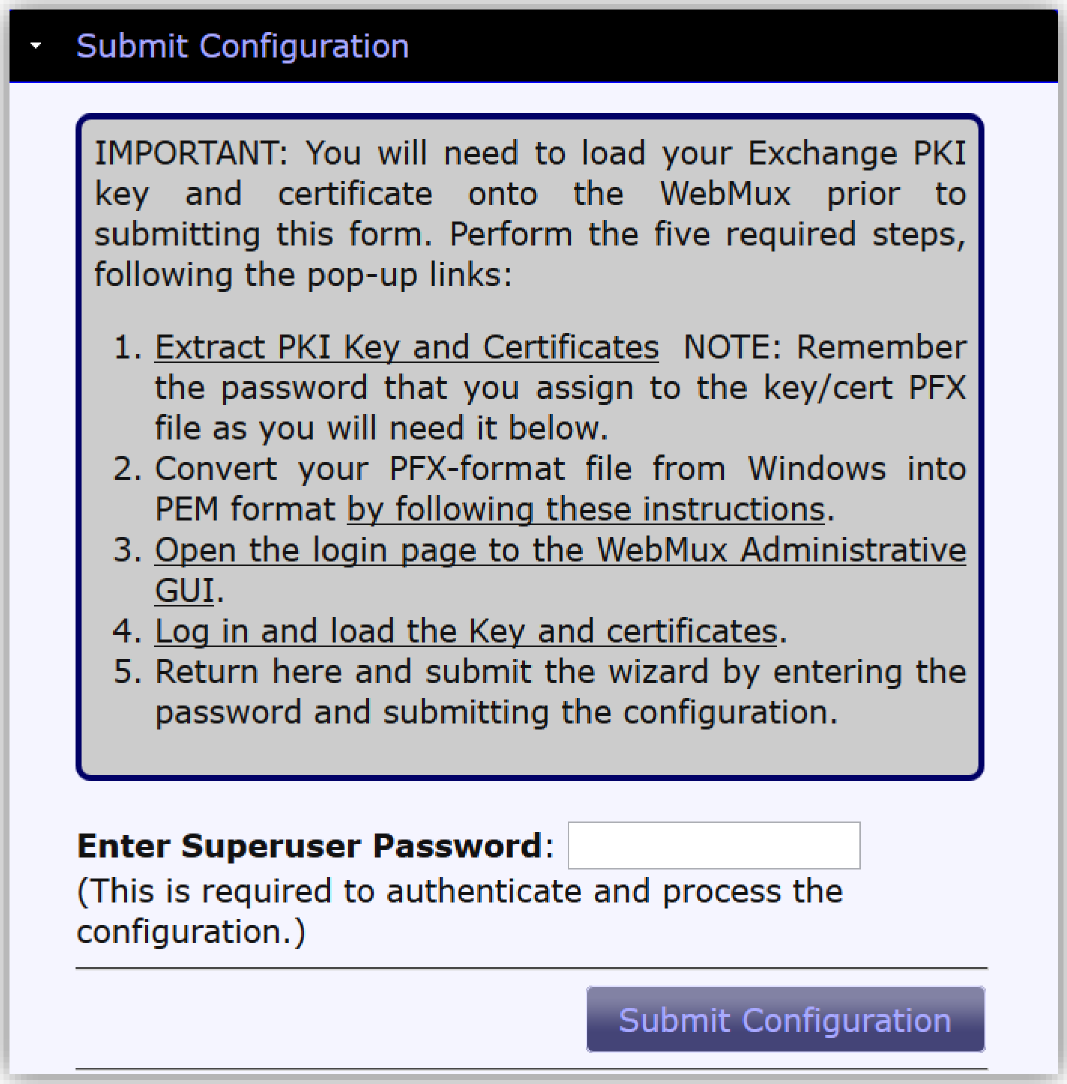
9. Click “Submit.”

You can now proceed to submitting the wizard. Go back to the browser window with the wizard and finish.

Submit Configuration

This is the step in which you enter the password for the “superuser” account and submit. You likely are doing this for the first time so you can enter the default password for that account, which is “superuser.” Please be certain to change that password as soon as practical.

The Exchange 2010 Wizard submission page is different from the page for Exchange 2013 because it includes the instructions for managing the PKI key and certificates. Both wizard pages are shown below:

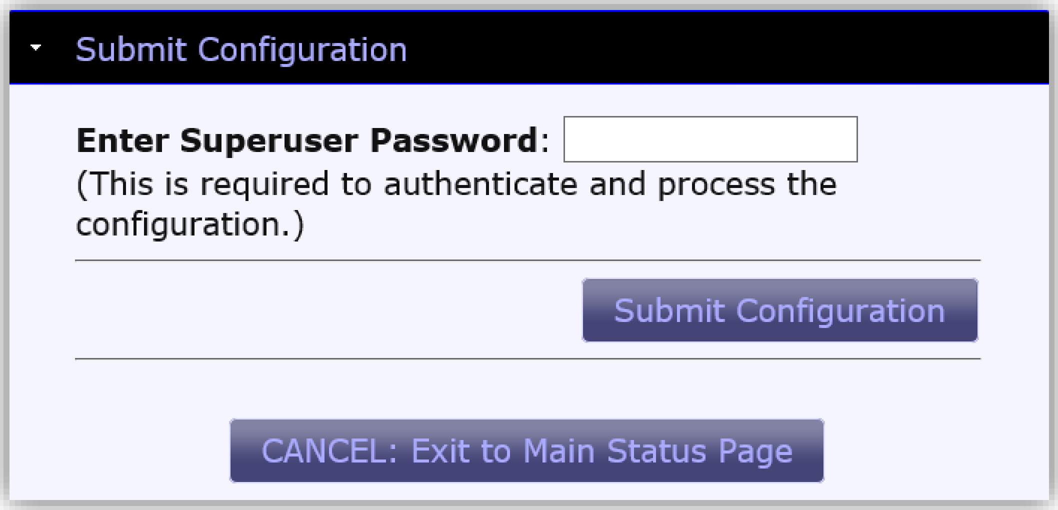


IMPORTANT: You will need to load your Exchange PKI key and certificate onto the WebMux prior to submitting this form. Perform the five required steps, following the pop-up links:

1. Extract PKI Key and Certificates NOTE: Remember the password that you assign to the key/cert PFX file as you will need it below.
2. Convert your PFX-format file from Windows into PEM format by following these instructions.
3. Open the login page to the WebMux Administrative GUI.
4. Log in and load the Key and certificates.
5. Return here and submit the wizard by entering the password and submitting the configuration.

Enter Superuser Password:
(This is required to authenticate and process the configuration.)

Figure 10 Submit wizard configuration—Exchange 2010

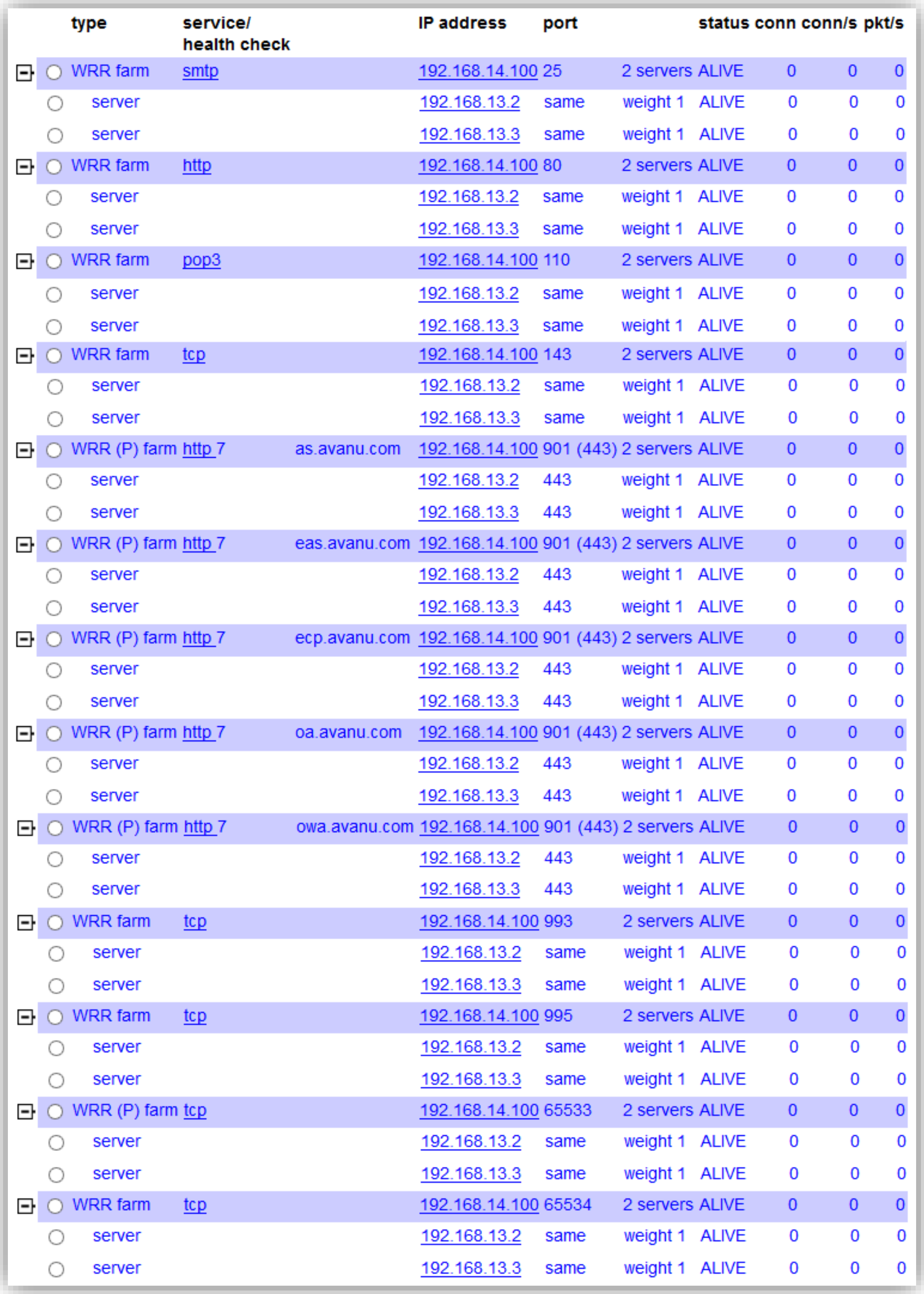


Enter Superuser Password:
(This is required to authenticate and process the configuration.)

Figure 11 Submit wizard configuration—Exchange 2013

WebMux Farm Configuration

You will get a notification page counting down to the WebMux rebooting and then it will load the Login page. Log in and you will see the farms that have been created through the wizard. Below is an example of the main farm display, showing all of the farms (passing zero traffic in this example, but those packet counters would show your real traffic once you start using them):



		type	service/ health check		IP address	port		status	conn	conn/s	pkt/s
⊟	○	WRR farm	smtp		192.168.14.100	25	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	same	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	same	weight 1	ALIVE	0	0	0
⊟	○	WRR farm	http		192.168.14.100	80	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	same	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	same	weight 1	ALIVE	0	0	0
⊟	○	WRR farm	pop3		192.168.14.100	110	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	same	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	same	weight 1	ALIVE	0	0	0
⊟	○	WRR farm	tcp		192.168.14.100	143	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	same	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	same	weight 1	ALIVE	0	0	0
⊟	○	WRR (P) farm	http 7	as.avanu.com	192.168.14.100	901 (443)	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	443	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	443	weight 1	ALIVE	0	0	0
⊟	○	WRR (P) farm	http 7	eas.avanu.com	192.168.14.100	901 (443)	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	443	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	443	weight 1	ALIVE	0	0	0
⊟	○	WRR (P) farm	http 7	ecp.avanu.com	192.168.14.100	901 (443)	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	443	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	443	weight 1	ALIVE	0	0	0
⊟	○	WRR (P) farm	http 7	oa.avanu.com	192.168.14.100	901 (443)	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	443	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	443	weight 1	ALIVE	0	0	0
⊟	○	WRR (P) farm	http 7	owa.avanu.com	192.168.14.100	901 (443)	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	443	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	443	weight 1	ALIVE	0	0	0
⊟	○	WRR farm	tcp		192.168.14.100	993	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	same	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	same	weight 1	ALIVE	0	0	0
⊟	○	WRR farm	tcp		192.168.14.100	995	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	same	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	same	weight 1	ALIVE	0	0	0
⊟	○	WRR (P) farm	tcp		192.168.14.100	65533	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	same	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	same	weight 1	ALIVE	0	0	0
⊟	○	WRR farm	tcp		192.168.14.100	65534	2 servers	ALIVE	0	0	0
	○	server			192.168.13.2	same	weight 1	ALIVE	0	0	0
	○	server			192.168.13.3	same	weight 1	ALIVE	0	0	0

Figure 12 WebMux Farms for Exchange 2010

The above display shows rows for farms (labeled “farm”) and rows for servers. You can delete farms that you do not need, if you know that you will not be using some of them, or you can just leave them. If you will be setting up separate Hub Transport or OWA servers then use these farms as models and follow the instructions in the next sections.

Notice the several farms created for port 443 with different hostnames associated with them. They are HTTP Layer 7 farms listening on port 443 but each one has a designated hostname for the separate services. The WebMux reads the packets, determines the hostname from the URL, and directs traffic to the back-end servers based on that information. This is done both to allow separate back-end servers and also because of differing cookie support. Some of the services support the load balancer inserting cookies for affinity and the WebMux will do so for the services that are compatible. (Some of the clients and services support cookies and others do not.)

You can also see the farm configuration details by using the feature for backing up the farm configuration as a text file. (From the main menu, under “Miscellaneous,” go to “Upload/Download,” and click the link to download the Farm configuration.) You will find, below, an extract of a farm configuration showing just those port443 farms with the PKI key #5 (“ssl5”), the SSL listening port being port 443, the back-end servers being HTTPS (indicated by “https_serv”), the various hostnames, and the load balancer cookie named “webmux” on the farms that support cookies.

```
# This source has 2 destinations starting at 14:
as%2Eavanu%2Ecom:         wrr_p   192.168.14.100   901 http   ssl5 sslport443 https_serv mark \
             host="as%2Eavanu%2Ecom" \
             load_balancer_cookie="webmux"
            dest 192.168.13.2  443 1
            dest 192.168.13.3  443 1

# This source has 2 destinations starting at 17:
eas%2Eavanu%2Ecom:        wrr_p   192.168.14.100   901 http   ssl5 sslport443 https_serv mark \
             host="eas%2Eavanu%2Ecom"
            dest 192.168.13.2  443 1
            dest 192.168.13.3  443 1

# This source has 2 destinations starting at 20:
ecp%2Eavanu%2Ecom:        wrr_p   192.168.14.100   901 http   ssl5 sslport443 https_serv mark \
             host="ecp%2Eavanu%2Ecom" \
             load_balancer_cookie="webmux"
            dest 192.168.13.2  443 1
            dest 192.168.13.3  443 1

# This source has 2 destinations starting at 23:
oa%2Eavanu%2Ecom:         wrr_p   192.168.14.100   901 http   ssl5 sslport443 https_serv mark \
             host="oa%2Eavanu%2Ecom"
            dest 192.168.13.2  443 1
            dest 192.168.13.3  443 1

# This source has 2 destinations starting at 26:
owa%2Eavanu%2Ecom:        wrr_p   192.168.14.100   901 http   ssl5 sslport443 https_serv mark \
             host="owa%2Eavanu%2Ecom" \
             load_balancer_cookie="webux"
            dest 192.168.13.2  443 1
            dest 192.168.13.3  443 1
```

Finishing

You will, on completing the wizard and waiting for the reboot, see a message informing you of some additional steps that you may take to improve management of your WebMux—such as changing the "superuser" password. After logging into the Web GUI go to "**NETWORK**" then "**NETWORK MANAGEMENT**." Some of the useful configuration items are:

- E-mail configuration for notification:
    - E-mail server URL for notification with numeric IP address
    - E-mail user name
    - E-mail user password
    - E-mail addresses for notification
- Long-term/bulk archiving of status messages from the WebMux
    - UDP Syslog server IP address for notification
- SNMP Management Information
    - WebMux SNMP UDP port
    - WebMux SNMP community
- Global Persistence timeout
    - Persistence timeout
- Time Synchronization—to Internet source or your infrastructure
    - NTP time server IP address

Do not forget to go to "**SECURITY**," and "**CHANGE PASSWORD**."

Modifying the Wizard-Generated Configuration

Setting Alternate Hub Transport Servers

The wizard leaves you with a configuration that assumes that all CAS and Hub Transport services are on one Farm/"Virtual IP" address, and all traffic is handled by one set of CAS servers, for the sake of simplicity. If you need to configure Hub Transport protocols to be handles by Hub Transport servers instead of using the addresses of the CAS servers then simply add the Hub servers that should receive the traffic for the farms for ports 25 and 587 and delete the CAS server's IP addresses. To add a server to a farm you click on the radio button next to the farm's entry and click on the "Add Server" button. Fill in the IP address of the Hub server and hit the "Submit" button. Repeat for each Hub server. To delete the CAS servers from the farm's list of servers you click the radio button for a server and hit the "DELETE SERVER" button.

Setting Separate OWA Farm IP Address

The wizard leaves your OWA services all going through the CAS. Simply add another farm, and its related servers, if you need a separate IP address for OWA. (You can delete the related farms from the set created by the wizard but nothing will break if you don't. You should see no traffic on those farms.) There are two sets of instructions, for Exchange 2010 and Exchange 2013. **Skip past the 2010 instructions if you are using Exchange 2013.** Here is a link to jump there: OWA Farms for Exchange 2013.

OWA Farms for Exchange 2010

Create a farm for port 80/HTTP traffic and one for 443/HTTPS traffic for Exchange 2010. The HTTPS farm requires SSL/TLS decryption in order to handle load balancer cookie used for affinity. If you want to perform re-encryption then follow the separate instructions for decyption and re-encryption. Recall that decrypting and sending port 80 traffic to the back end servers requires less processing but is less secure and requires the servers to be configured to handle the port 80 traffic. Here is a document on the SSL/TLS offloading:

http://social.technet.microsoft.com/wiki/contents/articles/1267.how-to-configure-ssl-offloading-in-exchange-2010.aspx

If you do the offloading of TLS decryption at the WebMux then the farm configuration is simpler, not requiring re-encryption, so be careful which instructions you follow for the port 443 traffic.

OWA Port 80 Farm

1. Click the "ADD FARM" button and enter the IP address of the OWA farm.
2. Click the "SUBMIT" button. (The default is to create an HTTP farm on port 80.)

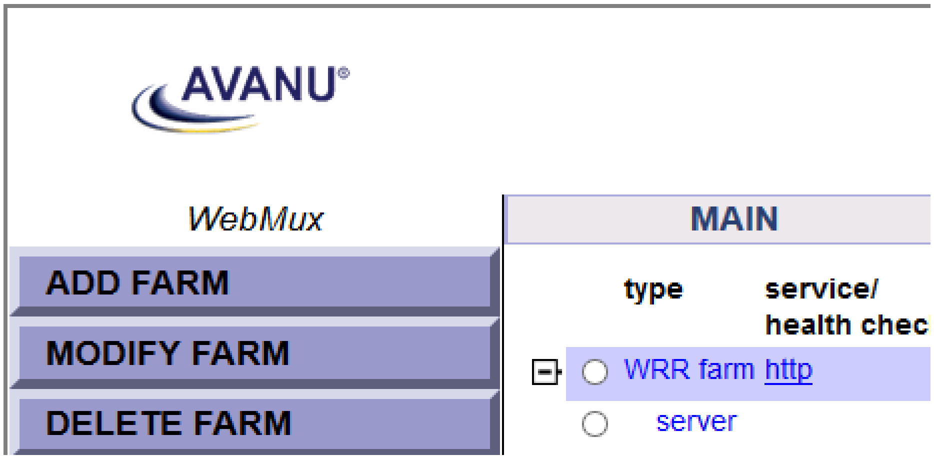


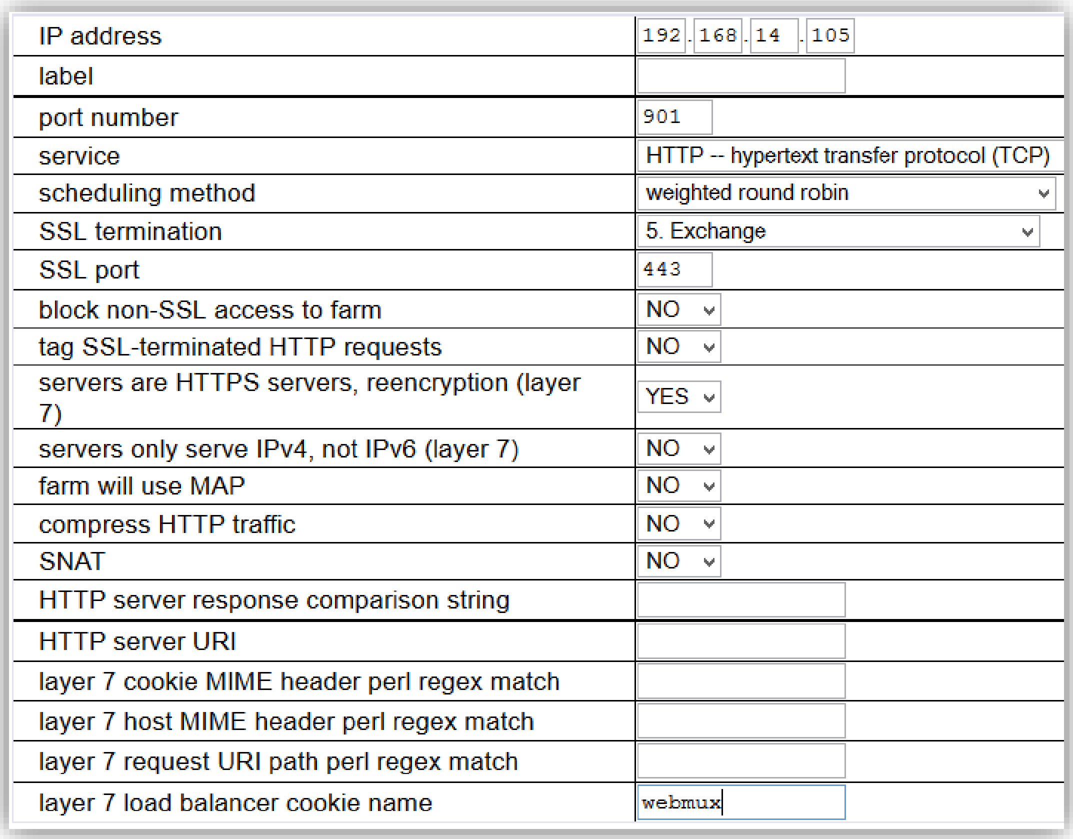
Figure 13 Add Farm

OWA Port 443 Farm — Offloading Decryption to the WebMux and passing port 80 Traffic to the OWA Servers

1. Click the “ADD FARM” button and enter the same IP address of the OWA farm.
2. Leave “HTTP” selected in the “Service” drop-down menu—because the “Service” is that of the back-end servers.
3. Under “SSL Termination” make sure to choose key/certificate pair #5 from the drop-down list as that is the data uploaded to the WebMux previously (during the last steps prior to submitting the wizard configuration). That is the step that ends the encryption at the WebMux, using a key that the clients trust.
4. Enter “webmux” as the value for the “Layer load balancer cookie name.”
5. Click the “SUBMIT” button. (This will create an HTTPS farm that will send HTTP traffic to the back end. Accepting the default port, when you add servers for this farm, leave the port field blank and they will get traffic on port 80. You can enter “80” when adding the servers but it is unnecessary.)

OWA Port 443 Farm — Decrypting and RE-encrypting at the WebMux and passing port 443 Traffic to the OWA Servers

6. Click the “ADD FARM” button and enter the same IP address of the OWA farm.
7. Enter “901” as the “port number” value. This is used internally by the WebMux.
8. Leave “HTTP” for the “Service” because that is what the WebMux will be handling internally, HTTP.
9. Under “SSL Termination” make sure to choose key/certificate pair #5 from the drop-down list as that is the data uploaded to the WebMux previously (during the last steps prior to submitting the wizard configuration). That is the step that ends the encryption at the WebMux, using a key that the clients trust. You can, of course, use other key/certificate pairs. There are 99 slots on the WebMux. Consistent reference to Key #5 is for simplicirty. If you need separate key/certificate pairs then use another one.
10. Verify that the “SSL port” has become “443” as soon as you click in that field.
11. Choose “YES” as the value for “servers are HTTPS servers, reencryption (layer 7).” That is what causes the traffic to be re-encrypted.
12. Enter “webmux” as the value for the “Layer 7 load balancer cookie name.”
13. It should look something like this:



IP address	192 . 168 . 14 . 105
label	
port number	901
service	HTTP -- hypertext transfer protocol (TCP)
scheduling method	weighted round robin
SSL termination	5. Exchange
SSL port	443
block non-SSL access to farm	NO
tag SSL-terminated HTTP requests	NO
servers are HTTPS servers, reencryption (layer 7)	YES
servers only serve IPv4, not IPv6 (layer 7)	NO
farm will use MAP	NO
compress HTTP traffic	NO
SNAT	NO
HTTP server response comparison string	
HTTP server URI	
layer 7 cookie MIME header perl regex match	
layer 7 host MIME header perl regex match	
layer 7 request URI path perl regex match	
layer 7 load balancer cookie name	webmux

Figure 14 Decryption and RE-Encryption Farm Configuration

14. Click the "SUBMIT" button. (This will create an HTTPS farm that will decrypt, manage the load balancer cookie used for affinity, re-encrypt, and send HTTPS traffic to the back end—and the reverse. Accepting the default port, when you add servers for this farm, leaving the port field blank and they will get traffic on port 443. You can enter "443" when adding the servers but it is unnecessary.)

Add the OWA Servers

1. Click the radio button for the OWA port 80 Farm
2. Click the ADD SERVER button
3. Enter the first IP address of the actual server that will listen on port 80 and handle the OWA traffic and click the "SUBMIT" button.
4. Repeat for each additional server.
5. Click the radio button for the OWA port 443 Farm
6. Click the ADD SERVER button

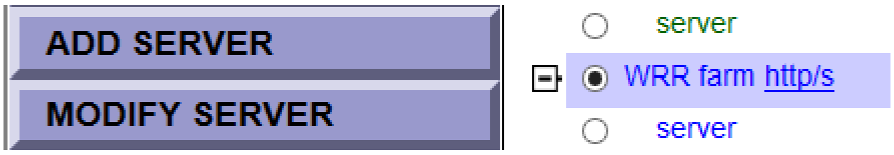


Figure 15 Add Server

7. Enter the first IP address of the actual server that will listen on port 443 and handle the OWA HTTPS traffic and click the “SUBMIT” button.

OWA Farms for Exchange 2013

You will create a farm for port 80/HTTP traffic and one for 443/HTTPS traffic for Exchange 2013:

OWA Port 80 Farm

1. Click the “ADD FARM” button and enter the IP address of the OWA farm.
2. Click the “SUBMIT” button. (The default is to create an HTTP farm on port 80.)

OWA Port 443 Farm

15. Click the “ADD FARM” button and enter the same IP address of the OWA farm.
16. Select “HTTPS” from the “Service” drop-down menu.
17. Click the “SUBMIT” button. (The default is to create an HTTP farm on port 80.)

Add the OWA Servers

8. Click the radio button for the OWA port 80 Farm
9. Click the ADD SERVER button
10. Enter the first IP address of the actual server that will listen on port 80 and handle the OWA traffic and click the “SUBMIT” button.
11. Repeat for each additional server.
12. Click the radio button for the OWA port 443 Farm
13. Click the ADD SERVER button
14. Enter the first IP address of the actual server that will listen on port 443 and handle the OWA HTTPS traffic and click the “SUBMIT” button.

Additional Background

Ports, Protocols, and Services

This following links are to Microsoft resources related to load-balancing Exchange 2010.

Understanding load balancing in Exchange 2010:

https://technet.microsoft.com/library/ff625247(exchg.141)

Load Balancing Requirements of Exchange Protocols:

https://technet.microsoft.com/library/ff625248(exchg.141)

Exchange 2010 port reference:

http://technet.microsoft.com/en-us/library/bb331973.aspx

Exchange 2010 Static RPC Port Configuration notes:

http://social.technet.microsoft.com/wiki/contents/articles/configure-static-rpc-ports-on-an-exchange-2010-client-access-server.aspx

Routing, Asymmetric Routing, Server LAN Gateway, and SNAT

You may, aside from the configuration of the WebMux for load balancing, find problems or questions about how traffic is routed or directed. You may encounter routing problems in implementing load-balancing because of the roles that load balancers play at the Ethernet, IP, and TCP layers. A common scenario is called "Asymmetric Routing" and the following references may help you avoid or recover from some known scenarios.

NAT Mode with External Users

This shows how NAT traffic flows for external users and it stresses the importance of the default gateway configuration for the servers to use the WebMux—and for the WebMux to be configured with a correct value, the "Server LAN Gateway," that serves that default gateway function.

Asymmetric Routing Problems with Local Users

Asymmetric routing can happen with the server's return traffic taking the wrong path to the client and being ignored/dropped.

Asymmetric Routing Solution: Enforce Default Gateway

One solution is to properly configure the default gateway, at the servers, to go back through the WebMux Server LAN Gateway.

Asymmetric Routing Solution: Static Route

Sometimes a static route is required on the back-end servers to get their traffic to follow the right path.

Asymmetric Routing Solution: SNAT

There are cases where configuring the WebMux to use Source NAT (SNAT), to stand in for the actual client, is the best solution for an asymmetric route problem.

Asymmetric Routing Solutions: Tradeoffs and Cautions

This is a quick run-down of issues that you may run into in trying to solve asymmetric routing problems.

GENERAL INFORMATION

About AVANU®

AVANU, Inc. is headquartered in San Jose, California and is a privately held product developer with manufacturing and production in the United States. The company's products are used in mid-sized to Fortune 500 companies and are specific for the network infrastructure and data center environments. The company's primary product line is the WebMux Network Traffic Manager, a load balancing network appliance. Founded in 1997, AVANU is a certified participant in the U.S. SBA's 8(a)/SDB development program and is WOSB Certified.

For additional information, please visit www.avanu.com.

Audience

The intended audience for this Microsoft® Exchange® Server 2010 and Exchange® 2013 User Guide is IT professionals that are intimately familiar with administration of networks and Microsoft® Exchange®. Other material available from AVANU may be useful to sales and marketing professionals. This primer is designed to be a guide to the configuration of a WebMux and to help understand how a WebMux functions with Microsoft® Exchange® Server 2010 and Exchange® 2013. The complete WebMux Network Traffic Manager User Manual can be found at www.avanu.com/documents.

Notice of Rights

Notice of Liability

Information in any WebMux document is distributed "as is" and without warranty. While every precaution has been taken in the preparation and manufacture of our products, AVANU nor its resellers and representatives shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information and instructions contained in any of these documents or by any computer software and hardware described within.

Trademarks

AVANU and Flood Control are registered trademarks of AVANU, Inc. AVANUAdvantage, AVANews, AVE, BAM, BlogWithUs, DNSMux, Inspired to Innovate, MAP, and WebMux are trademarks of AVANU, Inc. AVANU states that we are using any and all trademarked names in an editorial fashion and to the benefit of the trademark owner with no intention of infringement of the trademark. All trademarks and registered trademarks are the property of their respective owner(s).

Update Information

AVANU will always work to insure that the data contained in any WebMux documents are kept up to date. As such, please visit our website at www.avanu.com/documents to retrieve the latest version of our documents. All products and specifications are subject to change without notice.

Contact Information

Mailing Address

AVANU®
5205 Prospect Rd # 135-143
San Jose CA 95129-5034
United States

Service Center

AVANU®
15011 Parkway Loop
Building 10, Suite D
Tustin CA 92780-6522
United States

Email

Sales & Product Info: sales@avanu.com
Product Technical Support: techsupport@avanu.com
Administration: customerservice@avanu.com

Online Form Request: www.avanu.com/contact

Telephone Numbers

1.888.248.4900 US Toll Free
1.408.248.8960 International
1.408.248.8961 FAX

Sales and Information: Extension 201
Product Technical Support: Extension 202
Customer Service: Extension 203

Hours of Operation

8:00 am to 5:00 pm Pacific Time
Monday through Friday except for US Holidays