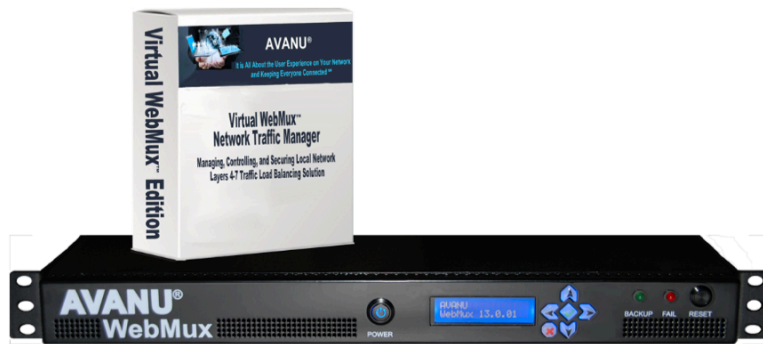# WebMux™
Network Traffic Manager

User Manual
Virtual WebMux and Network Hardware Appliances

Version v14.x
(Rev May 2020)

avanu.com

Table of Contents

SECTION I - 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-size 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, an application delivery network load balancing solution. Founded in 1997, AVANU is a graduate of the U.S. SBA's 8(a)/SDB development program and is WOSB Certified.

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

WebMux User Manual

Audience

The intended audience for this User Manual is IT professionals that are intimately familiar with administration of networks. Other material available from AVANU may be useful to sales and marketing professionals. This primer is designed to be a guide to the installation of a WebMux in a network, to answer questions that may arise during installation of this product, and to help understand how a WebMux functions.

The WebMux is a network traffic manager for load balancing Layers 4-7 of the OSI model (Transport layer of OSI and TCP/IP) of networking supporting an extensive range of applications and services.

Notice of Rights

Copyright 2013-2020 AVANU, Inc. All rights reserved. No part of any related WebMux documents may be reproduced or transmitted in any form by any means without the prior written permission of AVANU, the publisher, and the copyright holder. The AVANU central office may be reached at customerservice@avanu.com for information on getting permission for reprints and excerpts.

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, FireEdge, 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.

Packing List

One (1) WebMux Network Traffic Manager unit
One (1) Power Cord (Two for Dual Power Supply)
One (1) WebMux Quick Setup Guide
One (1) Product Registration Form

Contact Information

Mailing Address

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

Service Center

AVANU®
2122 South Grand Ave Ste H
Santa Ana CA 92705
United States

Email

Product Info: info@avanu.com
Product Technical Support: techsupport@avanu.com
Administration: service@avanu.com

Online Form Request: Technical Support Request Form

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

SECTION II - WEBMUX MAIN COMPONENTS

Front View

H/A Config Failure/Overheat Reset

Power   Quick Configuration
LCD Panel/Key Pad

Switches and Indicator Lights

Power

This switch toggles power on and off. To power off, the switch must be pressed and held for 5 seconds. However, it is recommended that you do not regularly use this power switch to shut down the unit.

✍ It is highly recommended to use the LCD panel, web interface, or command line interface to issue a proper system shut down.

LCD and Keypad

Up Arrow Button and Down Arrow Button

These buttons navigate through the menus when the LCD cursor is in the LEFTMOST position and also allow changing characters in the input fields that you will see to the right of that position. Note that it is generally best to use the "Checkmark" button for proceeding through the menus in the LCD display. When the cursor is in the LEFTMOST position, the "Up arrow" will take you to the previous screen.

These buttons will change letters and numbers (cycling through a list) in the fields where you enter data. It goes through lower case letters, upper case letters, numbers and symbols.

Left Arrow Button and Right Arrow Button

These move the cursor left and right, into data entry fields and back. Note that the "Checkmark" button can be pressed when input is complete, rather than moving back to the leftmost position, to proceed through the menus.

HA Config / Backup LAN Indicator

When two WebMux units are connected together via the Backup ports in an HA configuration, this LED will flicker, indicating communication between the primary and secondary units.

Failure / Overheat Indicator

The system monitors the CPU and will flash this indictor light if it should fail. If the system exceeds the CPU temperature limit, this indicator light will go on and the CPU will add idle

cylces - lowering performance (and heat). This is only likely to occur in cases of CPU fan failure or a data center cooling failure to the WebMux.

Reset

The HARD RESET button to force restart the WebMux. When this button is pushed in, it will force a reboot of the WebMux. Only use this to reboot the WebMux if all other normal means to reboot the unit (through the LCD, web GUI, or CLI) does not work.

✍ It will take about a minute for the WebMux to completely reboot and begin reporting activity in the LCD display. This will not reset your settings. It is for forcing restarts. To perform a factory reset refer to the Factory Reset part in Section IV for LCD instructions or CLI reference.

Rear View

Hot-swap power supplies   RS-232   IPMI/USB   Backup   Management   Network Traffic
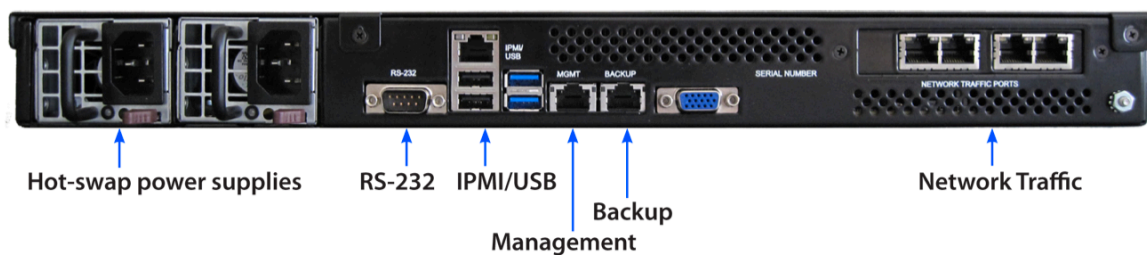
Power Supply

WebMux hot-swappable universal power supplies supports 90-264V input.

✍ Devices with redundant power supplies should have the power cords plugged in to separate circuits so WebMux does not fail due to one failed circuit. Properly ground the WebMux at the grounding terminal.

Ports

IPMI port is for connecting to a management network for access to IPMI services on the WebMux. This allows you to remotely control power on/off (including soft and hard resets), monitor temperature, and even access a remote console.

USB port may be used for firmware updates and to collect log data when network options for those functions are not available. This is a future option that is currently in development.

RS-232 port is available for serial console connections as well as for modem-dependent services, such as paging—where Internet-based services may be limited for security purposes. To connect to this port using a serial communications terminal, set the communications software for 115200 baud, 8 bit, Parity none, 1 stop bit.

MGMT port is a Gigabit Ethernet LAN connection that enables management (GUI and command- line) to be limited to a separate port and network. By default, this interface will get its IP via DHCP. A static IP can be assigned through the LCD setup or from the CLI.

BACKUP port is used in a High-Availability (HA) configuration to connect two (2) WebMux units together. The cable is auto-sensed where straight or crossover cables can be used. Link status LEDs will be lit when they are connected.

Network Traffic ports are the ports used for Internet-to-Server load balancing. The ports can be configured to all be on the same network (in Transparent, Single Network, and Direct Server Return modes) or on separate networks (NAT mode). In two port models, the "Internet" side port is on the left; the "Server" side port is on the right. For units with four physical ports, the "Internet" side are the two ports on the left; the "Servers" side are the two ports on the right. In the four port models, the two port pairs are configured as bonded/LACP ports that can be paired with a switch that is configured to aggregate the links and increase you bandwidth.

Other are the standard mouse, keyboard, USB, and VGA ports used for technical troubleshooting should the system's console need to be accessed.

SECTION III - WEBMUX TOPOLOGY OVERVIEW

WebMux Topology Modes

- Two-Armed Network Address Translation/NAT Mode

- Two-Armed Transparent Mode

- One- Armed Single Network Mode

- One-Armed Direct Server Return/DSR

IPv4 and IPv6 work in all the modes. Each mode has its advantages and disadvantages.

In NAT mode, the farm IP address is on the router LAN/Internet side that will be used to as the access point for the site. The real web or application server must have its IP address in the address range of the Server LAN subnet. The WebMux accepts incoming connects to the farm IP address and does NAT to forward the requests to the real server IP address. You can also use the IP address you assigned as the Router LAN IP of the WebMux as a farm address in order to save an IP address from being used up in your network, if your available public IPs are limited. You can create more farms with the same IP address as long as the port number is different.

In NAT mode, the WebMux also acts as a firewall. All ports except the farm port(s) are blocked. All servers behind the WebMux are reachable from the outside only through a WebMux farm.

Traffic from the servers to the outside network will be seen as coming from the WebMux unit's Router LAN IP address or the front proxy address (if you assigned one in the Network Management). If a WebMux is placed behind a firewall, be sure to allow the WebMux Router LAN IP address access to go outbound to anywhere or any port. All farm IP addresses should have rules to allow incoming traffic mapped to the address and port number, as well as the return traffic for each farm IP address to go outbound any port, anywhere.

In Transparent Mode or Single Network Mode, there is no firewall protection from the WebMux. All servers talk to each other freely across the WebMux. Load balancing occurs when the farm IP is accessed.

In Direct Server Return Mode, only the Server LAN port is connected, and the farm(s) must use a different IP address than the WebMux Server LAN IP address. You can use reuse an IP address for more than one farm as long as the port number is different from each other. In this mode, each server must have a loopback adapter. In a Windows® server the route for the loopback adapter must be removed. Please reference the section on adding a Loopback Adapter in this User Manual for additional information. The WebMux has been tested extensively to work with all versions of Windows®, Linux® and HP-UX® 11.X under this mode. Other operating systems should also work.

Two-Armed NAT Mode

o
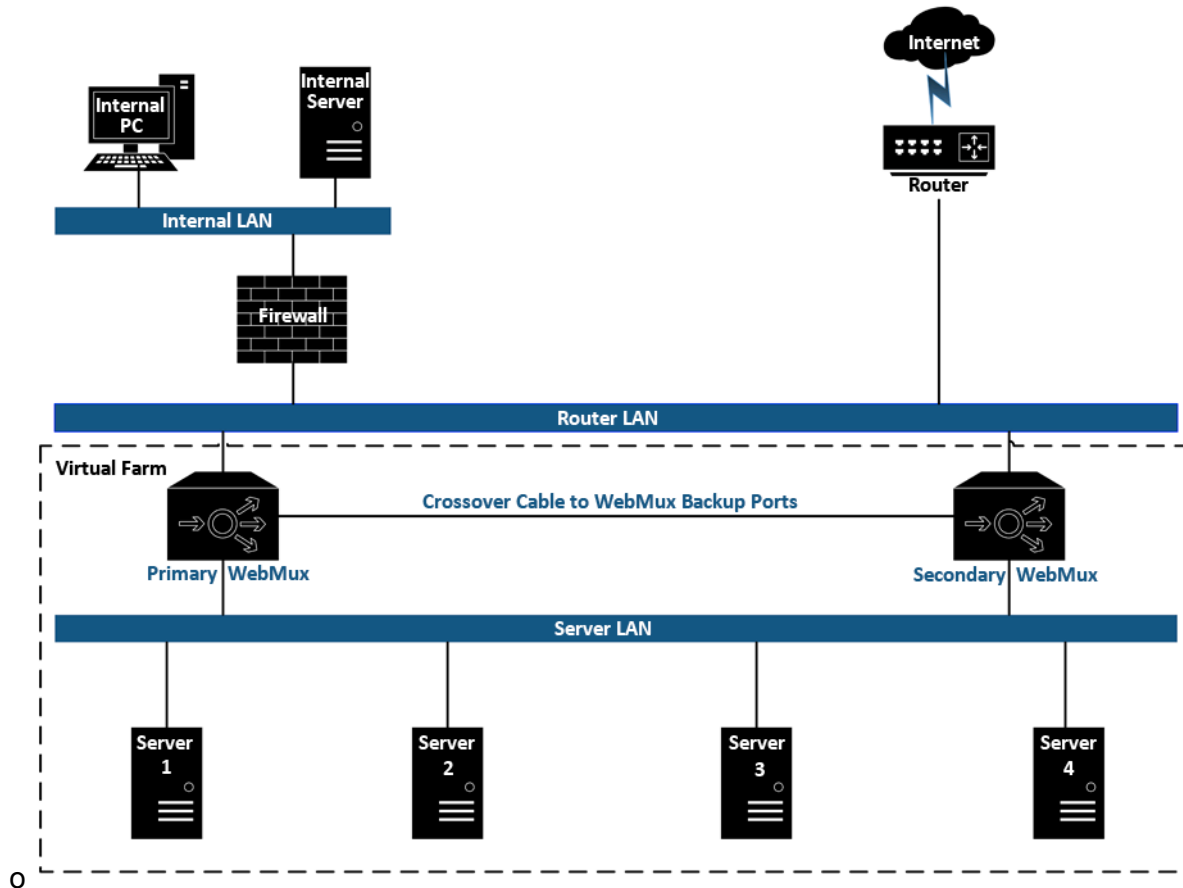
The main purpose of the WebMux is to balance IP traffic amongst multiple web, or other, servers. The diagram above shows a NAT installation with two WebMux units. In this example, one WebMux is serving as the primary, and the other is serving as the secondary, or backup, providing a fault tolerant solution (also called High Avaliability or HA).

In order for the web servers to share the incoming traffic, the WebMux must be connected to the network. There may be two or four load balanced interfaces on the WebMux. The left-side, load balanced interfaces connect to the Router LAN. This is the network to which the Internet router is connected. The right-side, load balanced interfaces are connected to the Server LAN. This network connects to all of the web servers. The WebMux routes traffic between these two networks.

Next, virtual farms must be configured on the WebMux. A virtual farm is a single representation of the servers to the clients. A farm consists of a group of servers that serve the same domain, website or services.

For example, to configure a farm (or virtual farm) to serve www.avanu.com:

- First, Server 1 and Server 2 would each need the website www.avanu.com configured on them and HTTP/HTTPS services started; and

- Second, a farm on the WebMux is defined with Server 1 and Server 2 in it. The servers could be setup to either share the traffic (load balancing), or setup as a primary server

and standby server. In either case, if Server 1 goes down, Webux will redirect all traffic to Server 2.

Two-Armed NAT Mode (Single WebMux)

Internet

Public IP: 65.25.35.156 NATed to
FARM 1 IP: 205.133.156.200

Public IP: 65.25.35.157 NATed to
FARM 2 IP: 205.133.156.210

Firewall/Router

Router LAN Switch

To WebMux Internet Port
To WebMux Server Port

Primary WebMux
WebMux IP on Router LAN: 205.133.156.220
External Router IP: 205.133.156.1
Server LAN IP: 192.168.199.251
Server LAN Netmask: 255.255.255.0
Server LAN Gateway: 192.168.199.1

Server LAN Switch

FARM 1 IP: 205.133.156.200

FARM 2 IP: 205.133.156.210

Server 1
Server IP: 192.168.199.10
Gateway: 192.168.199.1

Server 2
Server IP: 192.168.199.20
Gateway: 192.168.199.1

Server 3
Server IP: 192.168.199.30
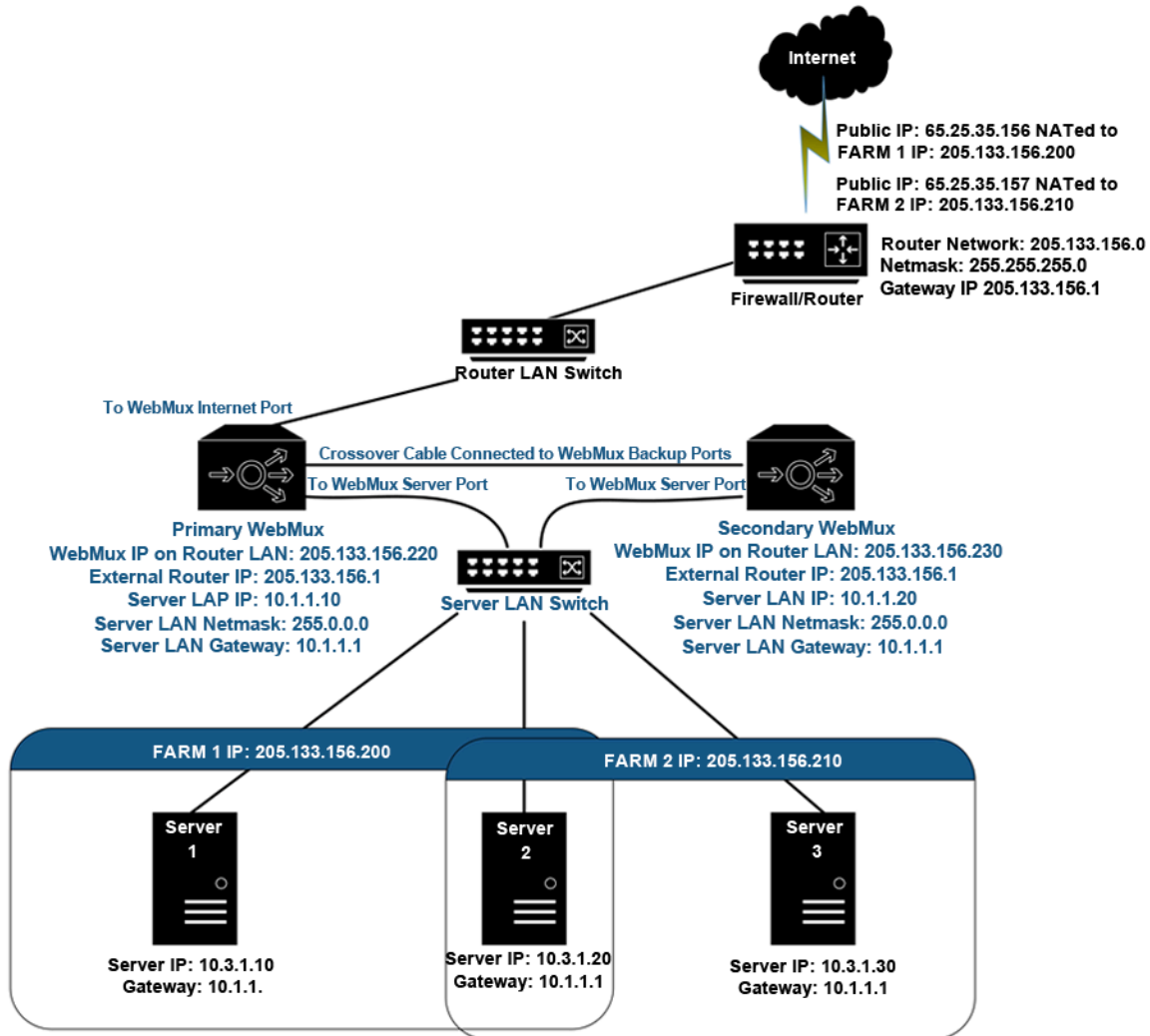Gateway: 192.168.199.1

In this example,

- One WebMux unit is used

- One WebMux interface (internet) connects to the router LAN. The other interface (server) connects to the server LAN

- The WebMux translates the router LAN IP addresses to private Class C addresses. In this example, the netmask is 255.555.255.0. The IP address of the WebMux interface on the router LAN is 205.133.156.220. The IP address of the WebMux interface attached to the Server LAN is 192.168.199.251.

- The Default Gateway for all the servers is 192.168.199.1

- Farm 2 IP address is 205.133.156.210. Servers 2 and 3 serve Farm 2

15

- Changes to the server: Set their IP addresses to the 192.168.199.xxx subnet and make their default gateway point to 192.168.199.1. If a service on the server (HTTP/S, FTP, etc.) is listening on a specific IP address, please make sure the service is configured to listen on the new IP address.

  ✍ Although the WebMux can work with any IP address range, all servers IP should be private addresses.

If there is a firewall between the WebMux and the Internet router, a rule must be defined to allow the farm IP address to communicate out to the Internet on all ports. In NAT mode, the main IP address of the WebMux is used as the masquerade IP of outbound traffic. Both the farm address and the main WebMux interface address must be translated to communicate outbound on all ports.

Two-Armed NAT Mode (Redundant WebMux Installation)

Internet

Public IP: 65.25.35.156 NATed to
FARM 1 IP: 205.133.156.200

Public IP: 65.25.35.157 NATed to
FARM 2 IP: 205.133.156.210

Router Network: 205.133.156.0
Netmask: 255.255.255.0
Gateway IP 205.133.156.1

Firewall/Router

Router LAN Switch

To WebMux Internet Port

Crossover Cable Connected to WebMux Backup Ports

To WebMux Server Port   To WebMux Server Port

Primary WebMux
WebMux IP on Router LAN: 205.133.156.220
External Router IP: 205.133.156.1
Server LAP IP: 10.1.1.10
Server LAN Netmask: 255.0.0.0
Server LAN Gateway: 10.1.1.1

Secondary WebMux
WebMux IP on Router LAN: 205.133.156.230
External Router IP: 205.133.156.1
Server LAN IP: 10.1.1.20
Server LAN Netmask: 255.0.0.0
Server LAN Gateway: 10.1.1.1

Server LAN Switch

FARM 1 IP: 205.133.156.200   FARM 2 IP: 205.133.156.210

Server 1
Server IP: 10.3.1.10
Gateway: 10.1.1.

Server 2
Server IP: 10.3.1.20
Gateway: 10.1.1.1

Server 3
Server IP: 10.3.1.30
Gateway: 10.1.1.1

In this example,

- Two WebMux units are used. One is the primary and the other is the secondary. They connect together with an Ethernet cable (straight or crossover) or through a hub or switch. The primary's Backup interface IP address is 192.168.255.253; the secondary's Backup interface IP address is 192.168.255.254. They cannot be changed.

- Both WebMux units connect to the Router LAN and to the Server LAN. Each WebMux interface has a unique IP address.

- The IP address of the WebMux units' virtual farms must be in the same network range as the Internet router.

- The WebMux translates the Router LAN IP addresses to a private Class A address. In this example, the subnet mask is 255.0.0.0. The IP address of the WebMux interfaces attached to the Server LAN are 10.1.1.10 and 10.1.1.20.

- The default gateway for all the servers is 10.1.1.1

- Farm 1 IP address is 205.133.156.200

- Servers 1 and 2 serve Farm 1

- Farm 2 IP address is 205.133.156.210

- Servers 2 and 3 serve Farm 2

- Change the default gateway on the servers to 10.1.1.1, as well as the IP addresses to the 10.3.1.10/20/30 addresses. If there is a service on the server (HTTP/S, FTP, etc) that is listening on a specific IP address, please make sure the service is listening on the new IP address.

  ✍ Although the WebMux can work with any IP address range, all server IP addresses should be private addresses.

If there is a firewall between the WebMux and the Internet router, a rule must be defined in the firewall to allow the IP address of the WebMux interfaces on the Router LAN in addition to the farm IP address (could be same as the WebMux Router LAN IP address) to communicate out to the Internet on all ports. Since the WebMux is doing Network Address Translation of the farm address to a non-routable address, the farm addresses on the WebMux must be able to communicate outbound on all ports defined in the farms.

  ✍ When two WebMux units are in a high availability pair, the secondary unit will not be reachable via its router side interface IP when it is in standby mode. You will be able to reach it from its back interface IP.

Two-Armed Transparent Mode

Transparent Mode is a WebMux configuration that allows you to keep the existing IP addresses of your servers. Like Direct Server Return Mode (explained later), the servers and the WebMux will be on the same IP network segment. However, physically, the servers will be connected to the WebMux in the same way they would be for NAT mode: on the server LAN port. The "internet" port on the WebMux is connected towards the Firewall/ Router. In this mode, the WebMux functions as an Ethernet bridge.

Two-Armed Transparent Mode (Installation without IP Address Change)
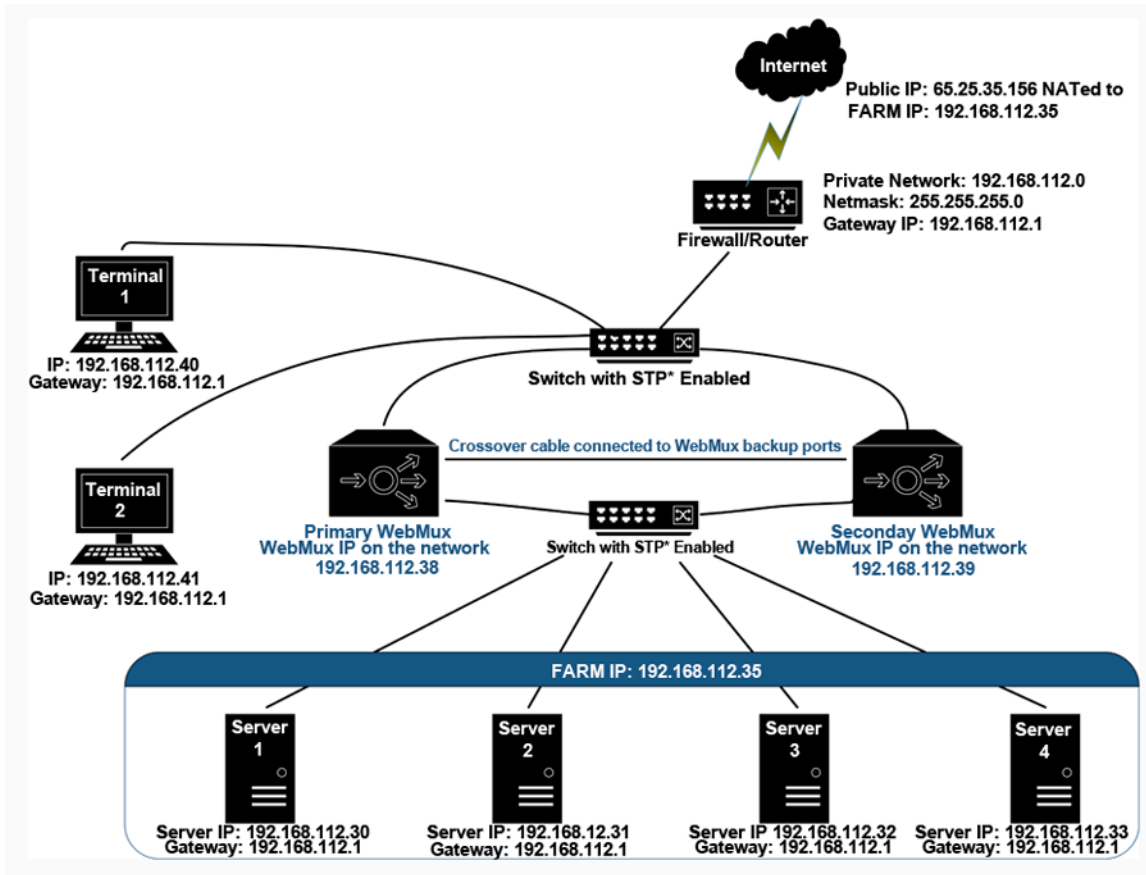
* STP = Spanning Tree Protocol

In Two-Armed Transparent Mode, the servers need to be isolated from the rest of the network with the WebMux in between, even though they are in the same network segment. All communication from servers to other servers or clients must flow through the WebMux. The WebMux will load balance any traffic targeted to the farm address and let all other traffic flow through like a network switch. This simplifies some network configuration, but isolating the servers is an additional requirement.

Since the WebMux acts as an Ethernet Bridge, anything connected to its back interface (server LAN) is on the same network segment as its front interface (internet/router LAN). If you look at the diagram above, you will see that the terminals are on the same network segment as the servers, even though the servers are "behind" the WebMux. The terminals

19

can communicate with the servers IP directly as if the WebMux was not there, and vice versa.

When creating a farm, choose a unique IP for the farm address in the network, and then add the server IP address under that farm. Load balancing occurs when the "Farm IP" is accessed instead of   the servers' actual IP.

There are no configuration changes that need to be made on the servers, except for the way they are physically connected to the network.

The diagram also gives an example of a redundant WebMux setup. In this case, it is absolutely required that the WebMux units are connected in between two switches. It is also very important to remember that you should not have any network path that will bypass the WebMux between the server side and the Internet/Router side. No parallel paths along-side the WebMux whatsoever. Doing so will create bridge loops and will cause broadcast flooding, effectively halting the network.

During a failover situation, you may immediately notice that the backup becomes temporarily unreachable though the Internet LAN side.

✍ When two WebMux units are in a high availability pair, the secondary unit will not be reachable via its router side interface when it is in standby mode. You will be able to reach it from its back interface.

One-Armed Single Network Mode

The WebMux supports two kinds of "One-Armed" modes: Single Network Mode and Direct Server Return (DSR) Mode. For Single Network Mode, there are no changes required for the network topology or server IP addresses. Requests from clients go to the farm address on the WebMux, which will in turn go to the servers through load balancing methods. The server replies are directed back to the WebMux and sent back to the clients. Single Network Mode has a 65,000 concurrent connections limit per farm.

One-Armed Single Network Mode (Installation without IP Address Change)
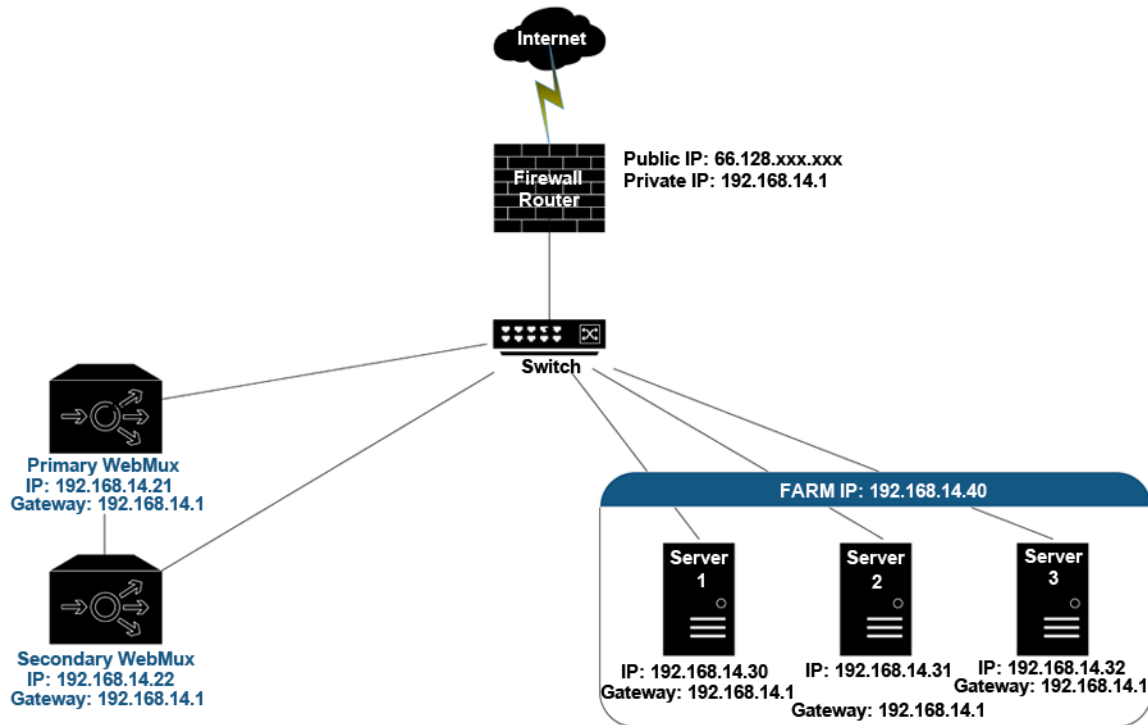
In Single Network Mode, connections being load balanced and going to the real servers will appear to come from the WebMux itself. You will not need to make any changes on your servers since the servers will always reply back to the WebMux when sending back their reply. You will only need to connect the "server LAN" side of the WebMux to the network. Do not connect the "router LAN" side interfaces to your network.

Be aware that in this mode, the client's real IP addresses will not be logged in your server log unless you modify your server's logging filter rules. You have to make sure your server logs the "X-Forwarded-For" (XFF) HTTP MIME header content to find the client's real IP address. If the HTTP header already has the X-Forwarded-For tag in it, the WebMux will not alter the tag. If the traffic is not for the HTTP port, WebMux will not insert the XFF header for the traffic. Enabling XFF header insertion is optional on a per farm basis. If your host software does not need this header, it is better not to insert it to reduce the WebMux CPU usage.

One-Armed Direct Server Return/DSR

In Direct Server Return (DSR) Mode, only the server LAN is connected to the network. Internet traffic or local connections can both be directly sent to the WebMux, which forwards the packets to the proper server(s). The server(s) routes the return traffic back to the remote or local clients directly.
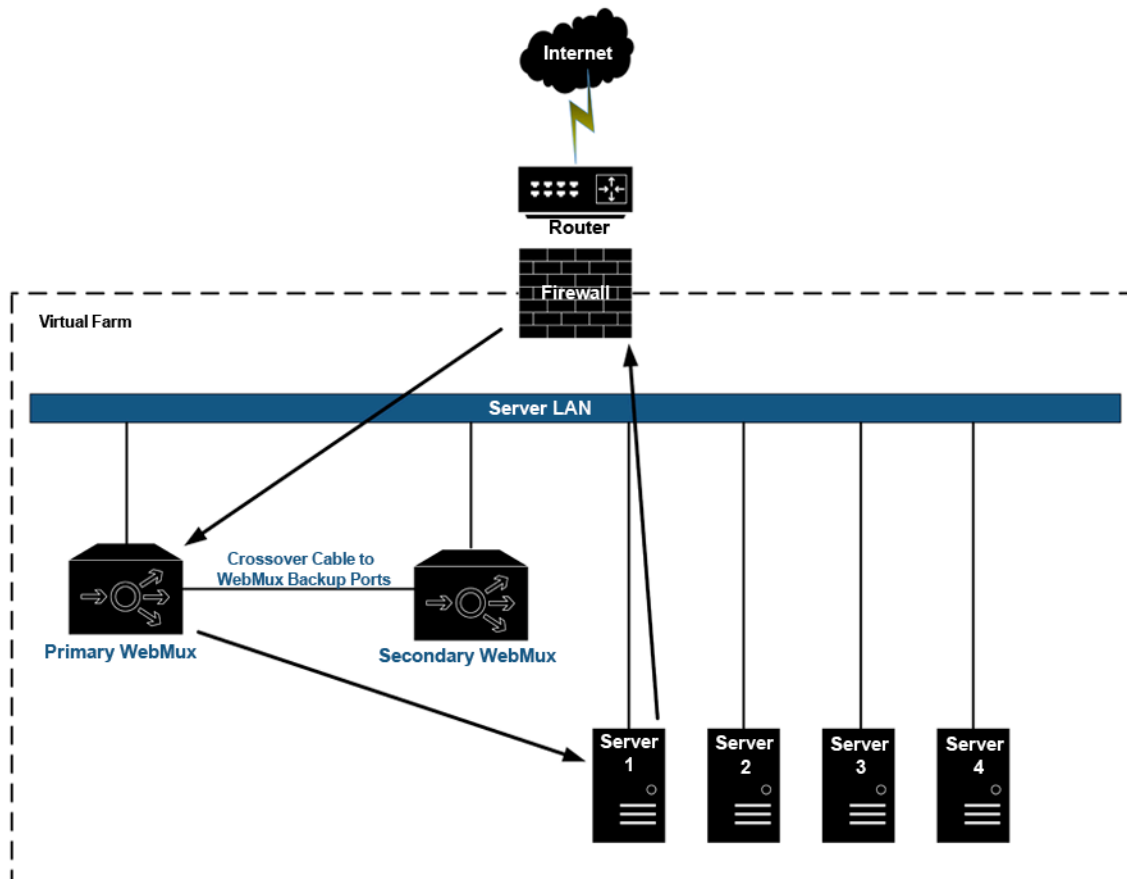
In most situations, incoming traffic is in small requests and return traffic from servers back to clients is large amounts of data (pictures or documents). Using Direct Server Return Mode will allow up to 100 times more traffic to be handled by the WebMux load balancer. The disadvantage for DSR Mode is that the inherent firewall protections of NAT Mode will no longer function. Users must provide their own firewall for incoming and outgoing traffic.

Also, when using SSL termination, DSR Mode does not gain any advantage due to the requirement that return traffic from servers must go back to WebMux for examination of the data headers and/or re-encryption the data packets.

One-Armed Direct Server Return/DSR Mode (Installation without IP Address Change)
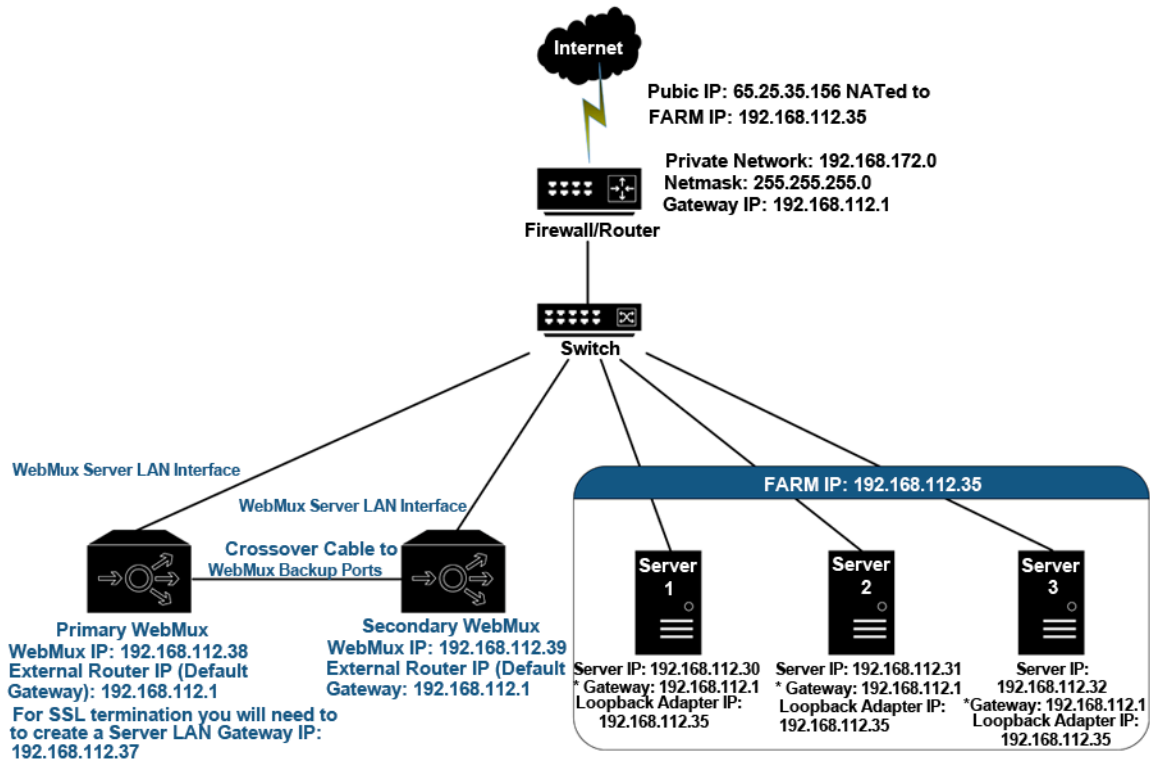
The above diagram is an example about how to configure the WebMux in DSR Mode without changing the IP addresses of the web servers and other servers that already exist on the network. This is another option that can be used if changing the existing network topology of the servers causes problems.

In this configuration, all the servers still remain on the same IP network and can communicate. From the servers' "view," the WebMux is on the same network as the servers. On the WebMux, only the server LAN side is connected, since there is only one network in Direct Server Return Mode. The WebMux takes at least two IP addresses to work in this mode - the server LAN Interface IP address, which is the management IP address of the WebMux, and the farm IP addresses.

If you are connected to a switch that allows you to create Link Aggregation Groups (LAG - sometimes called "EtherChannel" or "Port Channel"), the Internet port and Server port on the WebMux can both be connected to the switch and they will behave as one logical port with about twice the bandwidth capabilities. It is important that you configure the switch properly before connecting both interfaces. Please refer to your switch's user manual about creating Link Aggregation Groups.

Two simple changes must be made to each server in the farm.

1) Have a new loopback adapter installed and have its address set to the farm address. Do not set the gateway on the loopback adapter. Reference the Loopback Adapter section within this User Manual for additional information on how to add a loopback adapter.

23

✍ For DSR Mode to work properly, the loopback adapter must route the return traffic through the real network interface. In other words, the loopback adapter cannot have the gateway specified. Information on how to add a loopback adapter on servers can be found in the "How to Add a Loopback Adapter" section. In case the server is running Windows® 2003/2008, the route created when adding a loopback adapter cannot be deleted; please make sure the loopback adapter metric has a higher number.

2) If your service binds to any specific IP address, add the loopback adapter's IP address to that service.

The firewall configuration must be changed to point to the new farm address on the WebMux. Since the WebMux always uses one IP address in the server LAN, the farm address must be a different IP address in the server LAN in Direct Server Return Mode.

Direct Server Return Mode also allows for redundancy. The two WebMux units are connected to each other on their "backup" ports via a straight or crossover Ethernet cable or with a hub or switch in between.

✍ Under normal Direct Server Return operations, you will only need to set the external gateway IP address for the WebMux. However, if you are going to have the WebMux perform SSL termination, you must set a "server LAN gateway" IP in the WebMux and have the servers' default gateway point to that IP address.

Link Aggregation Group (Port Bonding) in Direct Server Return/DSR

When the WebMux is in Direct Server Return mode, the "Internet" and "Server" ports are configured in a Link Aggregation Group. If you have switch that has "LAG," "EtherChannel," or "Port Channel" capabilities, the "Internet" and "Server" interfaces will behave as a single interface and effectively double the amount of data throughput. You must enable the LAG/EtherChannel/ Port Channel capability in your switch to take advantage of this feature.

IPv6 Considerations

The WebMux can load balance IPv4 and IPv6 traffic in all above modes. Both IPv4 and IPv6 can work in Layer 4. Simply specifying the IPv6 prefix will enable WebMux load balancing in IPv6 only.

Because IPv6 uses the colon (:) symbol in the address, there are special considerations needed when using the IPv6 address in a web browser because the colon (:) is also used to denote a port number (i.e. 192.168.12.21:24). Because accessing the WebMux unit's web management requires access to port 24, you cannot simply put the IPv6 address in the address bar of the browser like you would for an IPv4 address. You must enclose the address in brackets ([]). For example, if the IPv6 address of the WebMux is fec0::c0a8:c15, then you would enter http://[fec0::c0a8:c15]:24/ to get to the web management.

There are also IPv6 versions of some basic networking tools such as ping6, traceroute6, and tcpdump with the IPv6 flag, ip –f inet6, route –inet6, etc. in the CLI. Please be sure that network software/client is indeed IPv6 capable or is the correct IPv6 version to use before assuming that your network is not working.

Also, when adding an IPv6 address to your server's NIC (network interface card), your server's OS might not automatically add a default gateway in its routing table for the IPv6 address. Please

double check the routing tables and make sure the proper entries are there. If your servers are not accessible from the outside but are accessible within the subnet, you might want to check and make sure that the default gateway was set up correctly.

WebMux IPv6 is supported all modes of operation: Two-Armed NAT mode, Transparent mode, as well as One-Armed Single Network mode and Direct Server Return/DSR mode. It allows SNAT Layer 4 operations, as well as SSL termination. It also allows incoming IPv6 traffic to be load balanced to internal IPv4 based servers. However, for traffic initiated behind the WebMux (not load balanced), it does not translate IPv4 to IPv6.

High Availability and Configuration

Two WebMux units can be paired together for high availability. In this configuration one unit must be explicitly configured as a "primary" unit and "NOT running solo."   The other unit must be configured as "NOT primary."   This can be done through the LCD setup or though the Administrative Web Management Interface at /cgi-bin/rec or by going to the "reconfigure" screen from the "network" menu in the main console of the Administrative Web Management Interface. It can also be done by running the "rec" utility from the CLI.

Each unit will need to complete the LCD setup or "reconfigure."   Be sure that each unit is assigned its own unique IP address to avoid addressing conflicts on your network. In some modes such as NAT mode and Direct Server Return mode, there is a setting for the Server LAN gateway IP address. The Server LAN gateway IP is the IP address that the servers "behind" the WebMux will use as their default gateway. This is optional in Direct Server Return mode, but is required in NAT mode and if you plan on doing SSL offloading or Layer 7 load directing in DSR mode. Please review the Direct Server Return mode configuration section to decide whether or not you need this. The Server LAN gateway IP setting will only show up for the primary unit setup. This setting is automatically passed to the secondary unit during synchronization. This IP address is up only on the active unit.

If the primary unit goes down, the secondary unit will activate the Server LAN gateway IP on itself to ensure that the real servers will always have a valid default gateway to use.

After these settings have been made, you will need to connect the two units together using a crossover network cable plugged into the "backup" ports of the WebMux units.

To properly sync the two units, begin with both units turned off and be sure the Ethernet cable is connected to the "backup" ports of both units. Turn the primary unit power on and wait for it to fully boot and go into the active state. You will see the LCD screen showing the updating status. You can now power on the secondary unit. When fully booted, the secondary will show the host/domain name and "[backup standby]" underneath. You will also see the message "(backed up by <IP address of the secondary unit>)" at the top of the main console screen of the web management GUI of the primary unit, underneath the unit's IP address(es). If you access the secondary unit, you will see the message "Inactive member of a WebMux pair" and "(backed up by <IP address of primary unit>)." A text version of the farm configurations will also appear on the secondary unit's main web console. This indicates that the units have properly synchronized. Setting and configurations made on the primary unit will automatically synchronize with the secondary unit. It is important that you explicitly click the save button on the main console page of the primary unit when changes are made. Changes will not propagate to the secondary unit until this is done.

There are a few things to keep in mind when you have two units paired in a high availability configuration. In NAT, Transparent, and Single Network modes, you will not be able to access the secondary WebMux through the "Internet" interface. You generally will not ever need to access the secondary unit when it is on standby. But, if you need to, you could access it from the "Server"

interface. In NAT and Transparent modes the server interfaces are on a different physical network segment. Be sure your client machine is on the proper side of the network if you desire to access the secondary unit. In Single Network and Direct Server Return modes only the "Server" interface is used and you will always be able to access the secondary unit through that interface.

If you log in to the secondary WebMux, a text version of your farm configurations will be shown. Please note that farm configurations can only be modified on the active unit. This is to ensure that there will not be duplicate IP addresses on your network. You can, also, verify that the secondary does in fact have the farm configurations by logging in to its command line interface and running "getconfig." You will see a text output of the farm configurations that the secondary unit received from the primary.

When a failover occurs, the secondary unit's LCD will show the updating information screen. Its web console will show "backup webmux takeover." Please note that if the primary unit remains powered on and the conditions that caused it to failover has been fixed (for example, if a network cable got unplugged and you were able to plug it back in), the primary unit will not take back control unless you reboot the machine. Upon reboot of the primary unit, the secondary unit will return control to the primary unit when it is up and running. The backup unit will return to the "[backup standby]" state. Otherwise, the secondary unit will remain the active WebMux of the pair. Also, the secondary WebMux will not failover back to the primary unit if there is a condition that will trigger its failure. The primary unit must be restarted.

We suggest that you address the problems with the primary unit as soon as possible to ensure that high availability is intact. Also, the secondary unit has a safeguard to not take over immediately if it just recently gave back to the primary unit. After about 5 minutes the secondary unit will be available to take over should the primary fail again.

It is recommended that you test the WebMux failover behaviors in a test environment and become familiar with it before you put it in production. The WebMux failover logic behaves in the following ways (these scenarios pertain to events on the primary unit):

1) **NAT mode:**

   a) Internet port cable physically disconnected or reports no link level connection, server port cable still connected (should failover to secondary)

   b) Server port cable physically disconnected or reports no link level connection, Internet port cable still connected (should failover to secondary)

   c) Front network verification enabled with at least one farm configured. If for some reason the primary unit is unable to get a response from its default gateway, the WebMux will see that as a failure and will relinquish control over to the secondary unit. The primary unit will assume that the problem is it own and that the secondary unit should be able to get to the   default gateway. In this scenario, it is VERY IMPORTANT that you ensure that your default gateway, Internet router, or firewall will respond always to the WebMux probes. Otherwise, a failover will occur and if the secondary unit is unable to get a response from the default gateway as well, both units can potentially become inactive.

   d) Multiple uplink gateways/next hop farms. The WebMux will not failover to the secondary unit as long as there is one active gateway available.

2) **Transparent mode:**

   a) Internet port cable physically disconnected or reports no link level connection, server port cable still connected (should failover to secondary)

b) Server port cable physically disconnected or reports no link level connection, Internet port cable still connected (should failover to secondary)

c) Front network verification enabled with one farm configured. (See the explanation in NAT mode)

d) Multiple uplink gateways/nexthop farms. (See the explanation in NAT mode)

3) Single Network mode

Only one port needs to be connected in Single Network mode. The following scenarios take the possibility that either the Internet port is used OR the Server port is used)

a) Internet port not connected, server port cable connected (should NOT failover to secondary)

b) Server port not connected, Internet port cable connected (should NOT failover to secondary)

c) Both ports not connected or reports no link level connection (should failover to secondary)

d) Front network verification enabled with one farm configured. (See the explanation in NAT mode)

e) Multiple uplink gateways/nexthop farms. (See the explanation in NAT mode)

4) Direct Server Return mode

Ports are bonded in this mode. Both ports can be connected at the same time, but it should be OK for only one or the other to be connected

a) Internet port cable physically removed or reports no link level connection, server port cable still connected (should NOT failover to secondary)

b) Server port cable physically removed or reports no link level connection, Internet port cable still connected (should NOT failover to secondary)

c) Both port cables disconnected (should failover to secondary)

d) Front network verification enabled with one farm configured. (See the explanation in NAT mode)

e) Multiple uplink gateways/nexthop farm. (See the explanation in NAT mode)

SECTION IV - CONFIGURING THE WEBMUX

Getting Started

Please collect the information about names and IP addresses designated by the arrows in the network topology below.
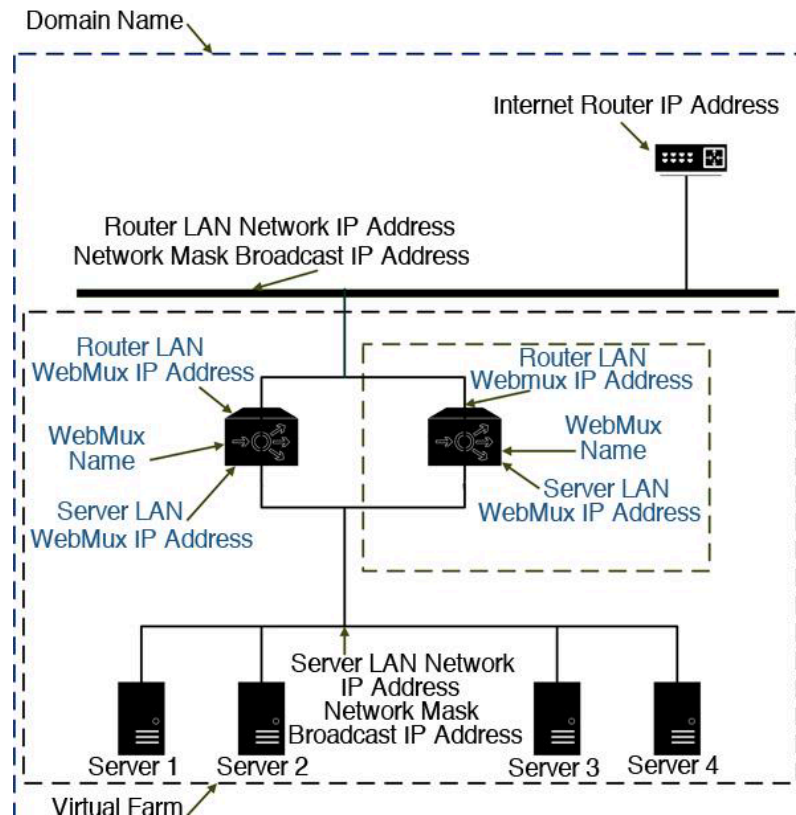
Network Terminology

A Virtual Farm includes the WebMux and the servers under it. Functionally, it acts as a single unit on a network. For example, http://www.you.com can be one virtual server farm; https://www.me.com is another farm, and ftp://ftp.avanu.com is the third farm. The first farm works on a set of servers on port 80, the second farm consists of another set of servers on port 443, and the third farm works on a set of servers on port 21. The WebMux supports combining ports 80 and 443 one single farm, so that same client browsing the site in HTTP mode will be sent to the same server for HTTPS requests. In the combined configuration, you must select HTTP/S as the farm service. Ports 80/443 will then be combined into one farm.

To serve the Internet, there must be at least one Internet Router. The local area network that connects the router and the WebMux is called the Router LAN. In this LAN, the WebMux takes the Internet traffic and distributes it to the servers behind it. The LAN connecting the WebMux and real servers together is called Server LAN.

The WebMux has four modes: Two-Armed Network Address Translation/NAT Mode, Two-Arm Transparent Mode, One-Armed Single Network Mode, and One-Armed Direct Server Return/DSR

Mode. In NAT mode, the WebMux units are connected to both Router LAN and Server LAN. At least one WebMux is needed to define the Router LAN and the Server LAN. We will explain other modes in detail in later chapters.

The side of the WebMux that connects to the Router LAN sends and receives all the IP packets from the router to the Internet. The side of the WebMux that connects to the Server LAN sends and receives IP packets to and from the servers in the farms. By properly configuring the WebMux, one can create one or more Virtual Farms on top of the physical hardware.

Hardware Setup - Collect Information

- Make a drawing of the existing network and note all the configuration settings. This will help you to fall back to the existing configurations if needed

- Make a new drawing for the new setup with the WebMux and the web farm in place. This will be used as a guide for setup and preparation of all the necessary material and equipment

- Collect all the IP addresses, their network masks, network addresses, and broadcast addresses for the Server LAN and Router LAN WebMux interfaces. The IP address of the Internet router is also needed

- Label all the cables and prepare additional cables if needed

- Make sure there are enough electrical or UPS outlets for all the new equipment

Hardware Setup - Network Environment

- Install WebMux in network environment

- If you have a secondary WebMux, connect the WebMux units with a crossover Ethernet cable

- Connect the servers to the Server LAN

- Connect the WebMux to the uplink switch

- Take all necessary measures to initiate basic network communications between all devices in new configuration.

- Verify that all the devices are up and running

- The WebMux is now ready to be configured

Initial Setup Though LCD Panel

Warning! Do not proceed without collecting all necessary information

✍ The IP addresses in the following examples are general examples and are not meant for literal use in an actual setup

Turn on the WebMux by pushing the power-on button in the front of the WebMux momentarily. You will see the version number on the LCD panel like this:

After the unit has fully booted, you will see a scrolling instruction screen. Hold down the Check-Mark button on the WebMux until the LCD displays the first question - "Enter WebMux host name."

During the initial configuration, you will be asked to provide names and IP addresses. (See next section)

Each item is explained in the order it is asked.

Answer the questions. Reboot to save and activate you setting.

✍ When reboot is complete, the service statistics screen will appear

Log into the web management interface.

The LCD Setup Screens

Enter WebMux Host Name:

Enter the host name of the WebMux. Use the right arrow to move the position, the up and down arrows to select characters, left arrow to move back in position, and the check mark button to confirm the change. This host name is for identification purposes. You may call it webmux1, webmux2, etc. (Press and hold down the up/down button for more than a second to make quicker changes.) Note the left most down arrow on the LCD allows the user to move to other settings.

Enter WebMux Domain Name:

This is for identification only; this has no effect for network operation. Although it can be any name, we suggest using the primary domain name of the Router LAN network. If you have only one domain, use that domain name. Note the left most position on the LCD has changed to an up and down arrow, allowing the user to go back and forth for questions and answers.

Is this a Primary WebMux?

If this is the Primary, answer Yes. If this is the Secondary WebMux, answer NO. Please note, you must still do the initial configuration on the secondary unit as well.

Primary WebMux Information

This question is not asked for the Secondary WebMux.

Is this WebMux running solo without a backup WebMux?

```
running solo?
↕    YES ▮NO
```

If the Primary WebMux is running in a standalone configuration (see sample configuration—Standalone WebMux), answer Yes. If you plan to add a second WebMux in the future, you may answer NO, even there is only one WebMux at the time. When you add a second WebMux later on, the WebMux will automatically detect the backup and start functioning as an active/standby pair.

Choose the WebMux Mode:

```
2arm svr LAN NAT        2arm transparent        1arm single netw        1arm out-of-path
↕    *YES    NO         ↕   *YES    NO          ↕   *YES    NO          ↕   *YES    NO
```

This is where to choose which mode you want to run the WebMux: Two-Armed NAT, Two-Arm Transparent, One-Armed Single Network, or One-Armed DSR Mode. The "*" indicates the default or selected option. Two-Armed NAT provides protection to the servers; it can handle large amounts of data as noted in the specification. It provides the best security for isolating servers from any other part of the networks. Two-Armed Transparent Mode or One-Armed Single Network Mode provides the convenience of preserving your server IPs, but may require physical relocation of the network connection or modifying the default gateways. DSR provides better performance when large amounts of data need to go back to clients (up to 100X more than on the specification chart); it also does not require a change to the server IP address. The screens will cycle among the modes until you select yes on one of them. Once one is selected it will continue to the next setup screen. Continue on to the related mode in the following pages.

NAT Mode Related Configuration

Enter Router LAN WebMux IP Address:

```
rtr LAN ip addr
↕ 205.133.156.200
```

This will be the IP address of the WebMux interface that connect to the router LAN side. This will also be the IP address that the WebMux uses as the masquerade IP address when it functions as a proxy for outbound traffic, particularly in NAT mode. (This IP address can be also be used as a farm IP, in NAT mode). When any server behind the WebMux (on the Server LAN) initiates communication with another host, the WebMux substitutes the servers' IP address with this address. (This is true for all services, except FTP services, which uses the FTP farm IP address for passive FTP connection). In a redundant setup in NAT mode, the secondary WebMux can also use the same IP address as the primary unit for this entry. This address floats between primary and secondary WebMux units.

✍   This is not true in Transparent, Single Network, or Direct Server Return modes. Using the same router LAN IP both units will create duplicate IPs.

Enter Router LAN Network IP Address Mask:

```
rtr LAN net mask
↕ 255.255.255.  0
```

This is the network mask of the Router LAN network. It is usually 255.255.255.0 for Class C networks. Choose what applies for your specific environment.

Enter Server LAN WebMux IP Address:

```
svr LAN ip addr
▮192.168.199.251
```

This is the IP address of the WebMux interface that connects to the Server LAN side. This IP address must also be unique for each WebMux.

✍ This address must be different from the server LAN gateway address

The purpose of this IP address is to allow the WebMux to check the network and server health situation. Even for the backup WebMux, this address must be unique. It is highly recommended to add this IP address to your servers /etc/hosts file, along with the gateway IP address, to allow faster name resolution in UNIX® or Linux® operating systems.

In an installation with a primary and secondary WebMux, a unique IP address is required for each WebMux interface that connects to the Server LAN. Those two unique IP addresses are in addition to the gateway IP address that is floating between the primary and secondary WebMux.

These IP addresses cannot be your Internet registered addresses. They must be Internet non-routable.

Enter Server LAN Network IP Address Mask:

```
svr LAN net mask
▮255.255.255.  0
```

This is the network mask of the Server LAN. For a Class A network, it may be 255.0.0.0. For a Class C network, it may be 255.255.255.0. Choose what applies for your specific environment.

Enter Router LAN VLAN ID (Optional):

```
rtr LAN vlan id
▲
▼       ...........200
```

This is the optional VLAN ID tag that will be used for the Router LAN (Internet) interface. You may enter values from 1 – 4067. The cursor position will only go from 0 to 9. To enter a value greater than a single digit, press the left arrow button to move the cursor to the next digit.

Enter zero (0) to disable the VLAN ID for the Router LAN (Internet) interface.

Enter Server LAN VLAN ID (Optional):

```
srv LAN vlan id
▮       ..........300
```

This is the optional VLAN ID tag that will be used for the Router LAN (Internet) interface. You may enter values from 1 – 4067. The cursor position will only go from 0 to 9. To enter a value greater than a single digit, press the left arrow button to move the cursor to the next digit. Enter zero (0) to disable the VLAN ID for the Router LAN (Internet) interface.

✍ The VLAN ID is used for full 802.1q VLAN support. This means that your switch must be configured to be using "tagged" VLAN. For additional details reference the section Using VLAN with WebMux in this User Manual.

The IP address you put here will be assigned to the Server LAN interface. Make sure it is a unique, unused IP address.

In the single WebMux setup, this address CANNOT be the same as the WebMux IP interface address on the Server LAN. When configuring a backup unit, this screen will not be displayed.

Enter Server LAN Gateway IP Address (Required):

```
svr LAN gateway
‡ 192.168.199.  1
```

The Server LAN Gateway IP address is required to be set for NAT mode. The IP address you put for this setting is an IP alias (an additional IP address) on the server LAN interface of the WebMux. THIS IS NOT YOUR INTERNET GATEWAY/ROUTER/FIREWALL IP. This is the IP address that the servers behind the WebMux will be using as their default gateway. It must be a unique IP address, otherwise you will create a duplicate IP problem on your network, and it cannot be the same IP you used in for the Server LAN IP. In a single WebMux deployment, it does not make a lot of sense to have two IP addresses on the server LAN interface. It is certainly logical to use the WebMux server LAN IP that has already been assigned earlier as the default gateway for the servers. However, for best practice, we recommend that you use this server LAN gateway IP address in the case that you may want to deploy a secondary backup unit.

In the primary/secondary HA configuration, each WebMux will have its own server LAN IP address. If you were to use the server LAN IP as the server's default gateway and WebMux went out of service, that IP address would no longer be valid because the other WebMux would have a different IP address. Therefore, the server LAN gateway IP is used instead. The server LAN gateway IP is only up on the active WebMux. The the primary WebMux automatically propagates this information to the secondary WebMux, but it will not be active on the interface when the unit is in standby. When the active WebMux goes down, the secondary unit will become active and bring up the server LAN gateway IP address on its server LAN interface. That way the servers behind the WebMux will always have a valid default gateway no matter which WebMux is active.

Continue to the [Common Configuration section](#) to complete the WebMux setup.

Transparent Mode or Single Network Mode Related Configuration

Enter Bridge IP Address:

```
bridge ip addr
▉192.168.  11.  32
```

This will be the IP address of the WebMux on the network so that you can use a web browser to manage it. Although the "server" and "internet" ports are interchangeable in transparent mode, it is recommended that you stick with a labeling scheme and connect the port labeled "internet" to the switch on the firewall/router side and connect switch on the servers to the port labeled "server."

Enter Bridge Net Mask:

```
bridge net mask
‡ 255.255.255.  0
```

This should match the subnet mask of the existing network the containing the WebMux.

Enter Router LAN VLAN ID (Optional):

```
rtr LAN vlan id
▲
▼         ..........200
```

Enter Server LAN VLAN ID (Optional):

```
srv LAN vlan id
▌         ..........300
```

✍ The VLAN ID is used for full 802.1q VLAN support. In Single Network Mode the Router LAN VLAN ID and Server LAN VLAN ID still pertain to the specific ports on the WebMux and they cannot be the same value. Even though you only need to use one of the ports in Single Network Mode, it is important that your switch setting matches the value of the port you are connecting to.

If you entered a non-zero value for the VLAN IDs, you will see an additional screen:

```
bond svr/rtr NI?
▲
▼     YES  *NO
```

Bond rtr/svr NI? ("Bond router and server Network Interfaces"):

This option will allow you to use the "Internet/rtr" port and "Server/svr" port as a single "bonded" interface, also known as Port Channel or Link Aggregation Group, allowing substantially more data throughput than a single physical interface. Additional information on this feature is in the "Bond All Interfaces Setup" section near the end of this chapter.

Continue to the Common Configuration section to complete WebMux setup.

Direct Server Return Related Configuration

```
svr LAN ip addr
▌192.168.199.251
```

Enter Server LAN WebMux IP Address:

In Direct Server Return Mode, at minimum, you only need to connect the Server LAN interface. This is the IP address of the WebMux Server LAN interface. This IP address must also be unique for each WebMux. The purpose of this IP address is to allow the WebMux to check the network and server health. Even for the backup WebMux, this address must be unique. It is highly recommended that one should add this IP address to your servers /etc/hosts file, along with the gateway IP address, to allow faster name resolution, especially on Linux®/UNIX® systems.

In an installation with a primary and secondary WebMux, one unique IP address is required for each WebMux interface that connects to the Server LAN. Those two unique IP addresses are in addition to the farm IP address that is floating between the primary and secondary WebMux.

```
svr LAN net mask
▌255.255.255.  0
```

Enter Server LAN Network IP Address Mask:

This is the network mask of the Server LAN. For a Class A network, it may be 255.0.0.0. For a Class C network, it may be 255.255.255.0.

```
srv LAN vlan id
▌         ..........300
```

34

Enter Server LAN VLAN ID (Optional):

✍ The VLAN ID is used for full 802.1q VLAN support

Enter Server LAN Gateway IP Address (Optional):

```
svr LAN gateway
↕ 192.168.199.  1
```

This is an optional configuration that is used only if you are going to do SSL termination. Keep in mind that this is an IP address assigned to the Server LAN network interface. Be sure to use a unique IP address or duplicate IPs on the network will occur. Enter 0.0.0.0 if not needed.

If your setup requires you to put a server LAN gateway IP, be aware that the IP address you put for this setting is an IP alias (an additional IP address) on the server LAN interface of the WebMux. THIS IS NOT YOUR INTERNET GATEWAY/ROUTER/FIREWALL IP. This is the IP address that the servers behind the WebMux will be using as their default gateway. It must be a unique IP address, otherwise you will create a duplicate IP problem on your network, and it cannot be the same IP you used in for the Server LAN IP. In a single WebMux deployment, it does not make a lot of sense to have two IP addresses on the server LAN interface. It is certainly logical to use the WebMux server LAN IP that has already been assigned earlier as the default gateway for the servers. However, for best practice, we recommend that you use this server LAN gateway IP address in the case that you may want to deploy a secondary backup unit.

In the primary/secondary HA configuration, each WebMux will have its own server LAN IP address. If you were to use the server LAN IP as the server's default gateway and WebMux went out of service, that IP address would no longer be valid because the other WebMux would have a different IP address. Therefore, the server LAN gateway IP is used instead. The server LAN gateway IP is only up on the active WebMux. The the primary WebMux automatically propagates this information to the secondary WebMux, but it will not be active on the interface when the unit is in standby. When the active WebMux goes down, the secondary unit will become active and bring up the server LAN gateway IP address on its server LAN interface. That way the servers behind the WebMux will always have a valid default gateway no matter which WebMux is active.

Common Configuration - For NAT, Transparent, Single Network, and Direct Server Return Mode

Enter External Gateway:

```
external gateway
▮192.168.  11.  2
```

This is the common setup for NAT, Transparent, Single Network and Direct Server Return modes. This is an address on the firewall or router local interface. In NAT mode, the WebMux needs to know this to route the server replies back to the clients. Although in Direct Server Return Mode this is not being used to route return traffic back to the Internet clients, the WebMux uses this IP address to check the connectivity of the external network on this gateway or through this gateway to the ISP side routers. For SSL termination, servers must route traffic back to the WebMux via the server LAN gateway (previously mentioned). The WebMux then forwards it to the client through the external gateway. If health check on external gateway is enabled (by default), WebMux will turn the farm listing red to indicate the external gateway failure.

Clear Allowed Host File?

```
clr alowd hosts?
▮    YES  *NO
```

The allowed host file prevents any unauthorized access to the WebMux Management Console. If a workstation's IP address is not in the allowed host file, that computer will not be able to reach the WebMux management console through the network. However, sometimes a wrong IP address is entered so that no computer can access the browser management console. At that point, clearing the allowed host file will allow any browser to access it. By default, the allowed host list is empty so that any IP address can access the WebMux. We do encourage adding the host IP addresses that you would allow to manage the WebMux into the list. See configuration through the browser interface for more details.

Remake Passwords?

```
remake passwds?
▲▼   YES   *NO
```

This function is provided in case you have forgotten the passwords to access the Management Console. Please use a browser to access Management Console for normal password changes. The factory default password is the same as the login ID on the screen. Answer Y to reset the Passwords to factory default. Answer N to leave them unchanged.

Enter Admin HTTP Port Number:

```
http admin port
▮       .............24
```

This is the HTTP port number for accessing the Management Console in non-secure mode. Any unused port number can be used. The factory default port number is 24 and one could choose to use any unused port below 1024 or port number above 1024 for this. Using a port number above 1024 will require you to set up an "admin farm." Basically, this is just a farm configured with that port, without any servers in it. Creating the "admin farm" reserves that port for use to that farm only and prevents port collision in case passive FTP is one of the other farms. Using port number below 1024 will not require setting up an "admin farm."

Enter Admin HTTPS Port Number:

```
https admin port
▮       ..............35
```

This is the HTTPS port number for accessing Management Console in secure mode. The factory default port number is 35, and one could choose to use any unused port below 1024 or port number above 1024 for this. Using a port number above 1024 will require you to set up an "admin farm IP". Basically, this is just a farm configured with that port, without any servers in it. Creating the "admin farm IP" reserves that port for use to that farm only and prevents port collision in case passive FTP is one of the other farms. Using port number below 1024 will not require setting up an "admin farm IP."

Discard Changes Made?

```
discard changes?
▲▼   YES  *NO
```

If you select YES at this point, all the changes made will be discarded and you will exit the setup mode. By default the answer is NO; all the changes will be saved. Only when you select NO (do not discard changes), changes will be saved to the internal solid-state storage. Changes will take effect after next reboot.

The next question will be Reboot Now?

Reboot Now?
```
reboot? (hold √)
▲
▼
```

This is the end of initial configuration. Most of the setup or changes require a reboot to tak effect.

Press and hold the center Check-Mark button to make the WebMux reboot. Use the UP arrow button to return to "Discard Changes" and select "Yes" to exit without change. Press the Down arrow or the Cross Button to continue to the Factory Reset option (see Factory Reset below).

```
REBOOT...
```

After the WebMux is rebooted, the statistics of the incoming packets, outgoing packets, etc. will be displayed on the LCD display periodically.

```
webmux.avanu.com
opkt  /s:            0
```

Power Off:
```
pwroff? (hold √)
▲
▼
```

Pressing the "Down" button at the "Reboot?" screen will bring you to the "Power Off" screen. We recommend that you always power down the WebMux via the LCD panel, Web GUI, or Command Line Interface.

LCD Brightness:

Pressing the "Down" button at the "Power off?" screen will bring you to the LCD Brightness screen. This screen will allow you adjust the brightness of the LCD backlight. The setting will default at 50. Valid values are from 0 to 100. The setting is activated when you press the check mark button.

Going back to this screen will bring the value back to the default of 50.

Factory Reset:

Pressing the "down" button or the check mark button from the "LCD Brightness" screen will bring you to the factory reset option. You will see:

```
FRSET? (hold √)
▮
```

This option will clear all current settings and reset the WebMux to original factory settings. Press and hold the check-mark button for at least 20 seconds to activate the factory reset. The process will take a few minutes and the WebMux will reboot itself.

Fixing Configuration Mistakes

You can always make changes to the hardware settings by pressing the Check-Mark button for three (3) seconds when the statistic screen showing. It will start the prompt questions that will allow you to navigate from one prompt to another by using the up/down button on the left most LCD position.

For example, if you configured the Allowed Hosts wrong and lock yourself out, you can go to the push buttons and select "Clr Allowed Hosts" option, save changes and reboot, which will allow all the IP address to access the management console through browser. You can clear the allowed hosts but not reset the password, or change one option and not change the others.

Bond All Interfaces Setup

When you specify a non-zero VLAN ID in NAT Mode or Transparent Mode, you will be given an additional option to "Bond rtr/svr NI". This feature allows you to use the "Internet" and "Server" ports as a "single" bonded interface (also known as Port Channel or Link Aggregation Group). When this option is enabled, the traditional "front" and "back" LAN of the WebMux is no longer partitioned on the WebMux itself, rather, on the network SWITCH using tagged and untagged VLAN ID settings.

Specific concepts need to be followed when setting up the WebMux with VLAN IDs. One is that the ports on the switch connected to the WebMux MUST be configured to be using "tagged" VLAN (802.1q). VLAN IDs configured on the WebMux for any mode (NAT, Transparent, or Out-of- Path) is a "tagged" VLAN (802.1q) specification. For the rest of the network, there are two ways to configure the switch and devices in order for them to be able to communicate with each other. One way is to make all the devices in the local network use 802.1q VLAN tagging, since only devices using 802.1q VLAN tagging will be able to communicate with each other. However, that option depends on the actual network interface in the device and whether or not it supports 802.1q VLAN tagging. The other option is to leave the network interface configuration on the other devices alone and configure the switch to do the VLAN tagging. This will be the option that we will be using in our example. All manageable switches with VLAN capabilities have these features, but since the switch configuration commands vary from brand to brand, we will only lay out the main configuration concepts and leave it up to you to refer to your switch user manual for specifics.

In the following example, we will be configuring a WebMux in NAT Mode using the "Bond rtr/svr NI" option enabled:

> RTR LAN IP: 192.168.12.21
>
> RTR LAN mask: 255.255.255.0 SVR LAN IP: 192.168.11.21
>
> SVR LAN mask: 255.255.255.0 RTR LAN vlan id: 100
>
> SVR LAN vlan id: 200
>
> Bond svr/rtr NI? YES
>
> SVR LAN gateway IP: 192.168.11.1
>
> External Gateway IP: 192.168.12.1

On the switch, we will be connecting ports 1 and 2 to the "Internet/rtr" port and "Server/svr" ports of the WebMux. We will designate ports 3, 4, 5, and 6 for the "Front/Internet" LAN and ports 7, 8, 9, and 10 for the "Back/Server" LAN.

First you will need to create a "port channel" or "link aggregation group" that includes physical ports 1 and 2. In most switches your real ports are designated by 0/1, 0/2, and so on. When you create a port channel, a new interface may be created designated by something like 1/1, for example.

Next, you will assign the VLAN IDs to the PORT-CHANNEL interface (1/1). First, configure the port-channel interface to "participate" or "include" VLAN 100 and make sure that it is TAGGED. Then, configure the port-channel interface to "participate" or "include" VLAN 200 and make sure that it is TAGGED. The port-channel interface should now be part of both VLAN 100 and VLAN 200 using TAGGED VLAN.

Now, configure the switch to use ports 3, 4, 5, and 6 for the "Front/Internet" LAN. The devices connected these ports will not be using any VLAN configurations. The switch will be configured to accept incoming "untagged" packets and automatically assign a VLAN ID to those packets. In this case, you will be using VLAN ID 100. First, you will configure ports 3, 4, 5, and 6 to "participate" or "include" VLAN 100 and make sure that you specify that it is UNTAGGED. On some switches, that means you have to first issue the command to have the port "participate" on VLAN 100, then you have no issue a "no vlan tagging 100" command. Next, to make this work properly, you must make these ports "accept all frames" AND you must assign them the PVID of 100. If you are unsure where, or how, to set the PVID, then please refer to your switch user manual. This tells the switch that these ports are part of VLAN 100, the data from the devices connected will be untagged and it should accept it anyway, and finally the switch will automatically assign a VLAN ID of 100 to these untagged packets. At this point, assuming that your device has a 192.168.12.0/24 address, you should now be able to ping the WebMux rtr LAN IP address of 192.168.12.21.

Finally, on the "server" side you will configure the switch to use ports 7, 8, 9, and 10 for the "Back/ Server" LAN. Again, the devices on these ports will not be using any VLAN configurations. The switch will be configured to accept incoming "untagged" packets and automatically assign a VLAN ID to those packets. Your "server" side VLAN ID is 200. You will need to configure ports 7, 8, 9, and 10 to "participate" or "include" VLAN 200 and make sure that you specify that it is UNTAGGED. Next you will need to make these ports "accept all frames" AND you must assign them the PVID of 200. Again, please refer to your switch user manual for specific commands. At this point, any device connected to port 7, 8, 9, or 10 (and assuming that it already has a 192.168.11.0/24 address), you should now be able to ping the WebMux svr LAN IP address of 192.168.11.21.

Setting Up the Management Port

The management port on the WebMux is a dedicated interface on its own subnet. If you have a DHCP server on your network, an IP address will automatically be assigned to this interface when you plug it in to the network. To set up a static IP address on this port, hold down the "X" button on the LCD panel for at least 3 seconds. Enter the IP address and netmask you want to use. It is recommended that you do not configure the management port to be on a subnet that already exists on either the Router LAN or Server LAN of the WebMux. Pressing the "check" button will immediately activate the new IP settings. You can set the management port IP from the CLI using the config-mgmt-ip-addr command. If you set a static IP for the management port and you want to go back to using DHCP, use the config-mgmt-ip-addr command and set the IP to 0.0.0.0

Initial Setup Through a Web Browser

Web GUI Initialization Interface:

You may want to change the basic settings for the WebMux through the web Graphical User Interface (web GUI), for example, when the WebMux located in a hosting center across the country. If one has information about the WebMux current basic settings, one could change those parameters through the web GUI. On a web browser, enter the following URL:

http[s]://webmux_ip:webmux_manage_port/cgi-bin/rec

For example, if your webmux_ip is 192.168.12.21, and your webmux_manage_port is 24, your URL will be:

http://192.168.12.1:24/cgi-bin/rec

```
WebMux initialization 14.0.00 . . .
You are not logged in as superuser.
Please enter your WebMux superuser's login name:
[superuser                ]

Please enter your WebMux superuser's password:
[                         ]

current GMT setting:
12:17:18 12/19/2018
If incorrect, please enter correct GMT as hh:mm:ss mm/dd/yyyy. (Use 24 hour time, not a.m. or p.m.)
[                         ]
Set time only?   O YES    ⊙ NO

[ continue ]
```

The first screen in "rec" (reconfiguration) asks for the superuser's password. The default superuser's password is "superuser." However, the actual superuser's password may have been changed by the system administrator. If you could not remember the superuser's password, someone has to go to the keypad to reset the password. For additional information reference the section on Remake Password within this User Manual.

The next question on the screen asks to set the time in the WebMux. The WebMux uses its clock to set the cookie for the management browser. When a WebMux manager is logged in for more than 8 hours without activity, the WebMux will log out the user based on the cookie. If the clock is off by more than 8 hours, the manager will not be able to login in to the WebMux. This section on the "rec"   screen will allow the manager to correct the clock if it is off. After entering proper password and setting the clock information (optional), the "continue" button will bring up this screen:

WebMux initialization 14.0.00 . . .

language	English
WebMux's host name without domain	
WebMux's domain name	
dispatch method	
Router LAN gateway IP address	
WebMux's router LAN IP address	
WebMux's router LAN IP network mask	
WebMux's server LAN IP address	
WebMux's server LAN network mask	
WebMux's router LAN VLAN tag (0 if none)	
WebMux's server LAN VLAN tag (0 if none)	
Bond all server LAN and network LAN interfaces together?	
Remake password file with default passwords?	
WebMux administration HTTP port	
WebMux administration HTTPS port	
Is this WebMux a primary (or solo) WebMux?	
Is this WebMux running solo without a secondary?	
Server LAN gateway IP address on WebMux (not same as server LAN IP address above!) (required for NAT, optional for OOP, use 0.0.0.0 to omit)	
Reinitialize configuration with admin entries only? (destroys existing configuration!)	
Reboot immediately after submitting this form?	
Submit when satisfied or cancel and log out.	submit cancel

Click the mouse into a field or use the TAB key to move the cursor into a field to see the current values. The user may change it based on new information obtained from ISP or network engineers. Once you press on the submit button, the WebMux will save all the changes to its internal solid state storage and reboot itself with the new value.

WebMux Reconfigure Screen (an alternate way):

You can also access these setting from the regular management console in the "reconfigure" screen of the "network" section of the menu.

See SECTION V – Management Console for more details on accessing the regular management console.

Configuration Wizards

The WebMux includes configuration wizards for quick deployment of the WebMux dispatch method and farm configurations. You can access the selection of configuration wizards by going to:

```
https://webmuxIP:webmuxPORT/wizards
```

Or you can log in to the WebMux web GUI and go to the "wizards" screen the "miscellaneous" sections of the menu.

Configuration Setup Wizards

The configuration wizards guide you to set up the WebMux quickly and easily.

After completing and submitting your set up data, the WebMux will reboot taking you to the WebMux login screen. After logging in, you may further customize WebMux through a secured browser user interface (GUI).

If there is no wizard for your application, reference the WebMux Quick Setup Guide for logging directly into the WebMux through a secured browser user interface (GUI) to complete the setup.

Notes and cautions:

1) Wizards are intended as a "one shot" initial configuration tool.
2) You can use the wizards to reconfigure the WebMux for different deployments, applications, and services on your network. However, each time a wizard is run, it will overwrite any existing WebMux configuration (including any configuration done manually or by any previously used wizards).
3) Wizard configuration changes can be adjusted through the WebMux Main Menu after logging in.
4) Once logged into the WebMux, under the Main Menu > Miscellaneous, you have the option to return here to the WebMux Configuration Wizard Menu for reconfiguration.

For additional support, contact AVANU's Technical Support Team at techsupport@avanu.com or by telephone 1.888.248.4900 U.S. Toll Free/1.408.248.8960 International (Ext 202) during normal business hours (Monday through Friday. 8:00am to 5:00pm Pacific Time).

Wizard Menu Selection

Generic Services

HTTP Servers   HTTPS Servers   HTTP/HTTPS Servers

Microsoft® Applications

Exchange 2010   Exchange 2013   Terminal Services   SharePoint   Lync 2013   Skype for Business

Other Applications

RedHat JBoss   Eclipse Jetty   LiteScape   Pexip   Apache Tomcat   Oracle WebLogic   IBM WebSphere

---

The configuration wizards are intended to be for first time setup and one time use. Once you have configured the WebMux via the configuration wizard, additional configuration modifications should be done via the WebMux management GUI. Each wizard will contain its own set of detailed instructions. Running any wizard will overwrite any existing configuration you have on the WebMux.

Current wizards available include:

- Generic HTTP
- Generic HTTPS
- Generic HTTP/HTTPS
- Microsoft Exchange
- Microsoft Lync
- Microsoft SharePoint
- RedHat JBoss
- Eclipse Jetty
- LiteScape
- Pexip
- Apache Tomcat
- Oracle WebLogic
- IBM WebSphere

The wizards are laid out and operate in a significantly different way than the main WebMux GUI. The wizard interface is divided into sections that can be expanded and collapsed in an "accordion" style. By clicking on the section heading, you can expand that section. Be sure to read the information and directions carefully, make your selections, and fill in all the required fields. You will then submit the completed wizard and the WebMux will process the settings and reboot. After the WebMux has rebooted and comes back online, you can log in to the regular WebMux GUI and make modifications to the resulting configurations.

43

Navigating:
- For better browser visibility, you can use the page zoom controls for your browser.
- Mouse click on the menu header to toggle open each section.
- Keyboard tips:
  The Up/Down keys advance you to the next menu header and the Enter key opens up the selected menu header
  The TAB key advances you to the next input field with a menu section.

▼ 1) Select the Network Architecture Mode

Click to highlight and select one of the four network architecture mode configurations. 2-Arm NAT is the default.

| 2-Arm NAT | 2-Arm Transparent |
| 1-Arm Single Network | 1-Arm DSR |

⌐ Network Architecture Definitions

NEXT ▶

▸ 2) Identify the WebMux

▸ 3) WebMux High Availability Configuration

▸ 4) Farm / Virtual IP Address Configuration

▸ 5) Server Health Check Method

▸ Submit Configuration

CANCEL - Wizard Menu Return

CANCEL - Exit

Command Line Interface (CLI)

Accessing the CLI

The CLI commands are intended for main initialization and simple diagnostics. You can use ssh or telnet to access the CLI commands to help troubleshoot network problems or server problems. There are maximum two diagnostic ports. By default they are 77:87. The first one will be SSH and second one will be Telnet. If there is only one port specified, only SSH access is allowed.

For example, to SSH into the WebMux, the following command can be issued from any Linux®/UNIX® computer. For Windows® computers, PuTTY can be used and can be freely downloaded over the Internet.

```
ssh –l superuser –p port_number WebMux_ip_address
```

Once logged into the CLI, the following screen will be shown:

```
Last login: Mon Dec 10 11:49:42 on tty1
WebMux version: 14.0.00 built Dec  3 2018 12:52:54
patch level: none
model: WebMux (part number AVE)
serial number: VX-000XAA0A0 manufactured Dec 09 2018
CPU speed: 2332.880 MHz
CPUs: 1
total memory: 2052176 k
configured as: two-armed server LAN NAT
management interface IP address: 192.168.15.159

Enter "help" for list of commands.
Enter  "cmd --help" give help for the command "cmd".
Enter "exit" or "logout" to end this session.
Enter "cmd —help" give help for the command "cmd".

Enter "exit" or "logout" to end this session.
```

Initialization via CLI

You can use the "rec" command in the CLI to do the same initialization steps that you would see on the LCD on or the web initialization screen.
When you run the "rec" command, you will see:

```
$ rec
(re)configuration utility for WebMux version 14.0.00 ...

Please answer yes/no questions with y or n.  Please supply IP
addresses as dotted quads.  This program runs in a loop until you
agree to reboot with your entered settings or decide to quit.
After the first iteration through the questions, your earlier
answers will be used as the defaults.  Any default value will
appear in brackets in a prompt.  Simply entering a return will
accept the default.
```

```
Please enter WebMux's host name without domain [default
"webmux"]:
```

... and so on.

CLI Commands List

There are more commands available in CLI:

about - displays WebMux model, serial number, and firmware version information.

arp - manipulate the system ARP cache

arping - ping <address> on device <interface> by ARP packets, using source address <source>

arptables - allows you to create custom packet filtering for the WebMux on the MAC address level. The changes made here are not reboot persistent.

authorized_keys - allows you to import your authorized keys for password-less SSH login. Run with --help for usage.

bootroot - There are two bootable partitions on the WebMux. Normally, you should never need to use this. However, in case one partition becomes unusable, this will change the default boot partition to the other one.

brctl - manually manipulate Ethernet bridge properties when the WebMux is in Transparent Mode

checkssl - verifies key and certificate. For example, "checkssl 1" will check the key and certificate in slot 1 (from the SSL Termination Management page of the web GUI). If no messages are returned, the test passed.

chg_pass - use this command to change the passwords for the "webmux" and "superuser" login.

config-mgmt-ip-addr - set the IP address for the dedicated management port. Run with --help for usage.

date - displays current system date and time. Allows you to adjust system date and time.

ethtool - allows you to display the status or manipulate the settings of the Ethernet hardware

eud - runs WebMux self-tests.

factory_reset - reset WebMux settings to original settings, clear all current settings

floodcontrol - displays current blocked sources history of the flood control feature.

getallsettings - save all WebMux settings from WebMux to your PC

46

getconfig - save all farm/server settings from WebMux to your PC

hwclock - displays current hardware date and time. Allows you to adjust hardware date and time

ifconfig - display and configure a network interface(s) ip - TCP/IP interface configuration and routing utility

ip - command for configuring network interfaces and network settings.

ip6tables - allows you to create custom packet filtering for IPv6 addresses for the WebMux. The changes made here are not reboot persistent.

iptables - allows you to create custom packet filtering for IPv4 addresses for the WebMux. The changes made here are not reboot persistent

netstat - display network connections, routing tables, interface statistics, etc.

nwconfig - allows you create additional networks for use in multiple ISP configurations and/or for multiple server subnets in NAT mode. Reference the "Multiple Uplink/VLAN Support" section for details.

openssl - access to the openssl command console

ping - send ICMP ECHO_REQUEST packets to network hosts

ping6 - version of ping command for IPv6

poweroff - initiates the proper shutdown sequence

putallsettings - allows you to import your saved "all settings" files.

putconfig - restore farm/server settings from your PC to WebMux

rdev - verifies current running root partition of the WebMux.

reboot - initiates a soft reboot

rec - allowing configure basic WebMux IP without using pushbutton

restart - restarts the WebMux unit's internal processes without rebooting the hardware.

route - manipulate or display the routing table. Settings made here ARE reboot persistent.

ssh - ssh client for WebMux CLI.

sysinit - allows you to create a custom startup script. (Useful for making custom iptables rules reboot permanent, etc) See the "Adding Commands to WebMux Startup Sequence" section for details.

takeover - utility to temporarily disable secondary WebMux takeover. Useful when doing firmware updates on paired systems. This utility only runs on the secondary unit.

tcpdump - capture and display network traffic traceroute - print the route packets take to network host

telnet - telnet client for WebMux CLI.

traceroute - traceroute utility for network diagnostics.

upgrade - this is the older upgrade command that is only used from incremental patching. It cannot be used for downgrade

upgrade64 - this is the "full upgrade" command to be used for upgrading the firmaware.

uptime - display when the unit has be running since.

vconfig - manipulate VLAN configurations

Most commands can be found on UNIX®, for detailed usage, please refer to any UNIX® man pages. Our support center does not support the usage of these commands.

Additional Command Line Interface Features

Adding Commands to WebMux Startup Sequence

Sometimes there is a need to add commands to the WebMux startup sequence so that certain commands can be reboot persistent. The superuser command "sysinit" is provided for the user to add iptables command or other commands to the startup sequence. Please note that adding a wrong command to the startup sequence may render the WebMux not accessible, thus it is always a good practice to test the commands first before adding it to the WebMux startup sequence.

For example, if you want an SMTP server at 192.168.10.98 always appear to be sent from one of your public IP addresses (i.e. 66.1.1.98) on the WebMux, you can use this iptables command:

```
iptables -t nat -I POSTROUTING -s 192.168.10.98 -d ! 192.168.10.98 \
-m multiport -p tcp —destination-ports 25 -j SNAT —to-source \
66.1.1.98
```

This command works the moment it is issued, but when you reboot the WebMux, it gets lost. To make it reboot persistent, you want to add it to the WebMux startup sequence. You can use the sysinit command to add the above command to the sysinit table in the WebMux, so that it will always be executed during the WebMux startup.

The sysinit command has following syntax:

```
$ sysinit —help

usage: sysinit [—help] [—quiet] [—write]

—help  print help
```

48

```
—quiet   skip prompts and confirmation

—write   write stdin to superuser's sysinit script table
```

(without parameter will read existing table) The superuser's sysinit table may contain any commands that are allowed at the superuser's command prompt. At system startup, it will be run after networking has been started.

If typing or pasting new input, use control-D for EOF.

```
$ sysinit —write

sysinit: Enter new script up to EOF (cntl-D):

echo AAA >/dev/console

sysinit: You entered 23 bytes. [done]


$ sysinit

sysinit: reading sysinit file: echo AAA >/dev/console

sysinit: sysinit file contains 23 bytes. [done]
```

For the purpose of the above example, the echo AAA will be saved in the sysinit table. If you want to add a new command, it is always a good idea to test them before adding to the sysinit table. To clear the sysinit table, use a space and control-D to write a blank table into sysinit table. Please note that sysinit table will not be send over to the backup WebMux. In case the wrong command caused user no longer able to login into WebMux, use the LCD "factory reset" to reset the sysinit table to blank.

Tagged VLAN and WebMux

VLANs may be untagged and tagged. To use untagged VLANs, also known as port based VLANs, no additional configuration of the WebMux is necessary. The VLAN configuration is done on the switches. To the WebMux it appears as if no VLANs are used.

This section covers using tagged VLANs, also known as 802.1q VLANs for the main networks configured on the WebMux.

When you configure the WebMux main network addresses and masks, whether with the front keypad and LCD (see the section under Configuring the WebMux within this User Manual); the web GUI (see the section Initial Setup Change through Browser within this User Manual); or through the superuser's command line interface with the "rec" command (see the "Initialization via CLI" section within this User Manual); you may also specify VLAN tagging for these networks. VLAN tagging is optional. If it is used, the switches to which the WebMux is connected must also be configured correctly to use these tags. (When additional networks are configured for the WebMux using the superuser's command line utility nwconfig, you may also arrange for their VLAN tagging at that time).

Besides configuring the WebMux to use VLAN tags, the switches to which the WebMux is connected must be configured to use these tags. In most switches, there are three items to

be addressed when setting up VLANs: the VLAN name, the port participation, and if it will be tagged or untagged.

First a VLAN must be chosen and named. Choosing a VLAN name on the switch does not automatically determine whether its VLAN is tagged or untagged. It merely an identifier for your own record.

Once the VLAN name has been chosen, you must next select which ports participate in this VLAN. If the port selection does not match the physical connectivity, traffic will not pass.

The third (very important) setting to make sure is that the port on the switch connected to the WebMux will accept correctly tagged VLAN packets only. In some switches, you must first configure the port to use "general" mode and then specify that the port will be tagged. If you plan to use more than one VLAN, you may configure the switch port to be a trunk port, or add multiple VLAN tags to it.

At this point you should be able to access the WebMux from other devices that are also using the same tagged VLAN ID.

There are some specific considerations when configuring VLAN IDs in NAT, Transparent, or Out-of- Path Mode. In NAT mode, you have the option to have a VLAN ID for both the Router (Internet) LAN interface and the Server LAN interface. Even though the WebMux will allow for both sides to have the same VLAN ID, it is still recommended that you have a different VLAN ID for each to ensure complete network separation between both sides.

In Transparent mode, you will only have one Bridge IP address, but you will need to create a VLAN ID on both the Router (Internet) LAN interface and the Server LAN interface. The WebMux will allow you to create the same VLAN ID on both interfaces, but this is not recommended unless each physical side is on physically separate switches, completely isolated from each other. Be wary of routing loops.

In Direct Server Return Mode, you only have one VLAN ID to assign for the original network since the WebMux only uses one network for both incoming traffic from clients and outgoing traffic to the servers. In Direct Server Return Mode, the Internet LAN interface and Server LAN interface are bonded in a Link Aggregation Group, and both interfaces have identical configuration (unless the port bonding is   specifically disabled— reference section on Bond all Interfaces Setup within this User Manual).

Multiple Uplink/VLAN Support

The WebMux supports load balancing multiple uplink capabilities. You can configure this feature using the command line interface command:

nwconfig—additional network configuration add/list/delete/install tool

With multiple uplink, you can configure the WebMux to use multiple ISPs and gateways. The WebMux uses source based routing to be sure that packets that came in from one ISP will return through the same ISP. All uplinks are useable simultaneously. Once you have configured farms on both networks, the WebMux will monitor the default gateways of the different uplinks and failover to any available ISPs should one ISP go down.

To set up multiple uplinks, first log into the command line interface via telnet on port 87 or ssh on port 77. We will refer to the main network configuration of the WebMux (the IP addresses created via the LCD setup or the "rec" page in the web GUI or rec_cmdline from

the CLI) as the "original" network. Networks created with the "nwconfig" command will be referred to as "additional" networks.

nwconfig -A|—add NAME -i|—ipaddr IPADDR [other options] nwconfig -D|—delete NAME

nwconfig -I|—install NAME nwconfig -L|—list [PATTERN …]

nwconfig -R|—replace NAME -i|—ipaddr IPADDR [other options]

nwconfig -U|—uninstall NAME

For the -A or —add option, the -i or —ipaddr option is required, but other options are optional. Whatever information you supply is used, and what information is not supplied is calculated from the supplied information as best as possible. However if an external gateway address for routing is to be used, it must be specified with -g or —gateway.

Options:

-A|—add NAME   add new network configuration NAME

-D|—delete NAME   delete existing network configuration NAME

-I|—install NAME   install network described by network configuration NAME

-R|—replace NAME   like -A, except allows configuration to already exist

-U|—uninstall NAME   uninstall network described by network configuration

NAME

-b|—broadcast BROADCAST   broadcast address is BROADCAST, e.g.,
          192.168.14.255

-g|—gateway GATEWAY   address of gateway/router on the network is GATEWAY, e.g.
          192.168.14.1

—help|—usage   print this usage message

-i|—ipaddr IPADDR   WebMux unit's IP address on the network is IPADDR, e.g.,
          192.168.14.22

-L|—list [PATTERN …] list existing additional network configurations whose name
          match   the given pattern(s). If no pattern is given, list all
          additional network configurations.

-m|—netmask NETMASK network mask for the network is NETWORK, e.g.,
          255.255.255.0

-n|—network NETWORK address of the network is NETWORK, e.g., 192.168.14.0

-r|—router-vid VID   VLAN ID for the network for the router in transparent mode

51

-s|—server-vid VID   VLAN ID for the network for the servers in transparent mode

-p|—prefix PREFIX   network mask as a prefix width is PREFIX, e.g., 24

-v|—vid VID   VLAN ID for the network is VID; default: original VLAN tag

For example:

    nwconfig -A newISP -i 192.168.14.21 -g 192.168.14.1

The IP you specify will be the WebMux unit's main IP on the additional network.

To activate the configuration immediately without rebooting: nwconfig -I newISP

If you need to assign VLAN ID for the additional network use the -v option: nwconfig -A newISP -i 192.168.14.21 -g 192.168.14.1 -v 200

In NAT mode, if you do not specify a gateway IP, the new network will be put on the Server LAN side.

If you will be pairing up WebMux units in a failover configuration, we recommend that you perform these preliminary configurations first before attempting to connect the two units together.

Important Considerations Pertaining Only to Additional Network Configurations.

NAT Mode VLAN and Server LAN Gateway IP:

In NAT mode, the interface assigned for the additional network depends on whether or not you specify a gateway IP. If you specify a gateway IP, the additional network IP will be configured on the Router (Internet) LAN interface for multiple uplink. Otherwise, it will be used on the Server LAN interface to create additional networks for the server LAN side.

We recommend that you set up different tagged VLANs for each additional network you set up for the WebMux.

If you already have a VLAN ID configured for your original network configuration and you do not specify a VLAN ID for your additional network configuration with nwconfig, the additional network will use the same VLAN ID that you specified for your original network configuration. Even though the WebMux allows for this kind of configuration, it is generally not recommended. We suggest that all separate networks be on separate VLAN IDs.

Also, you cannot create an additional network with a VLAN ID unless the original network is also configured with a VLAN ID. This is true for all modes (NAT, Transparent, and Direct Server Return). Generally, it is not recommended that you create additional networks unless you are using VLANs.

If you are pairing up two WebMux units in a failover configuration, you can use the same Router (Internet) LAN and Server LAN IP address for the additional networks in both the primary and secondary units. In NAT mode, the Router (Internet) LAN and Server LAN

interfaces are deactivated when the unit is in standby to eliminate duplicate IP address issues and to allow you to conserve available IP addresses.

In the original network configuration you had to specify a "server LAN gateway IP" to be used as the servers' default gateway IP address. The "server LAN gateway IP" is a floating IP address that is available only on the active WebMux in a WebMux pair. When creating additional network configurations on the server side, you do not have the option to create a "server LAN gateway IP" like the original network configuration. In this case, you will need to configure your additional server networks using the same IP addresses on the secondary as with the primary. The IP address you create for you additional server network will be used as the server's default gateway IP. Since only the active WebMux will have this IP enabled on its interface, you will not have a duplicate IP address between both units. If one unit goes out of service, the IP address becomes available on the other unit and the servers can continue to communicate to the external network uninterrupted.

Transparent Mode VLAN:

In Transparent mode, it is recommended that you assign a different VLAN ID for the physical front and back interfaces with the -r (—router_vid) and -s (—server_vid) flags.

For example:

nwconfig -A tm_vlan -i 192.168.14.21 -g 192.168.14.1 -r 200 -s 300

If you use the -v flag, both the physical front and back interfaces will have the same VLAN ID. It is not recommended that you use the same VLAN ID for the front and back interfaces in Transparent mode.

Direct Server Return Mode VLAN and Server LAN Gateway:

When creating an additional network in Direct Server Return Mode, it is important that your farm IPs are different from the main IP address you create with the "nwconfig" tool. This is important because the main IP address you create will be the IP address the WebMux unit's health checks will appear to come from. You will have problems with Windows® servers if you use a farm IP that is the same as the main IP. This is because Windows® utilizes the MS Loopback Adapter with the farm IP. When the WebMux send its health check request coming from the main IP, the Windows® machine will see that the IP address is on its Loopback Adapter and will not send back a reply since it believes it is coming from itself. The WebMux will mark the server dead since it will not receive a reply. To ensure that this will not occur, do not use a farm IP that is the same as the main IP in Direct Server Return Mode.

It is important to remember that when you are running a setup involving SSL termination that you must point your servers' default gateway back to the WebMux. In the original network configuration, you had an option to create a "server LAN gateway IP." The servers used this IP address as their default gateway IP. This IP is a floating IP that transfers between WebMux units in a failover configuration. Only the active WebMux will have that IP address available on its network interface to avoid duplicate IP address issues.

Additional network configurations do not have the option to create a "server LAN gateway IP" like the original network configuration. In this case, you will need to use the FARM IP as your servers' default gateway IP address. Since the FARM IPs are only available on the active WebMux they will effectively serve as the floating server LAN gateway IP.

SECTION V – MANAGEMENT CONSOLE (WEB GRAPHICAL USER INTERFACE)

After the initial configuration, you should be able to use a web browser to connect to the WebMux. The Web Graphical User Interface (web GUI) is where all of the WebMux management is done.

✍ It is recommended that you first complete the Network Admin setup after logging in the the WebMux web GUI for the first time. More information on the Network Admin screen is found further in this section.

Overview of the Web GUI

This is the web GUI as seen on a desktop web browser:

The web GUI is divided into several sections, or panes:

Pane 1 is the unit information pane. This displays the basic hardware and status information of the WebMux, like the dispatch mode the WebMux is running, the device IP(s), CPU usage, memory usage, link status of the network interfaces, current hardware date and time, and uptime. This pane also contains clickable elements. The "menu" element will hide or show the menu pane (pane 2). Clicking on the "AVANU WebMux" logo will open a new browser window to the www.avanu.com site. The "webmux.avanu.com" element will appear as whatever host and domain name you assigned your WebMux unit. Clicking on this take you to the unit's "about" screen to show more information about the unit such as its serial number and firmware version.

Pane 2 is the menu pane. The menu is divided into sections. Each section heading is marked by a filled triangle. Click on the section heading to expand that section. Or use "open all" or "close all" options to expand or collapse every section of the menu.

Pane 3 is the console pane. This pane will display the various management screens that the menu will navigate to.

Pane 4 is the navigation pane. The navigation pane contains back, forward, and reload buttons that behave like the browser's back, forward, and reload buttons. However, these navigation buttons only affect pane 3 (the console page). Whereas, the browser's navigation buttons might affect the whole browser screen.

The WebMux web GUI is a "responsive" web page. That means the page will arrange itself to accommodate the smaller size of a mobile screen or if the desktop browser window is adjusted to a small enough dimension. The "responsive" web GUI design helps make it easier to administer the WebMux via a mobile interface such as a smartphone or tablet.

The following examples show the rearrangement of the web GUI on a mobile interface as well as the appearance of the mobile interface with the menu hidden:
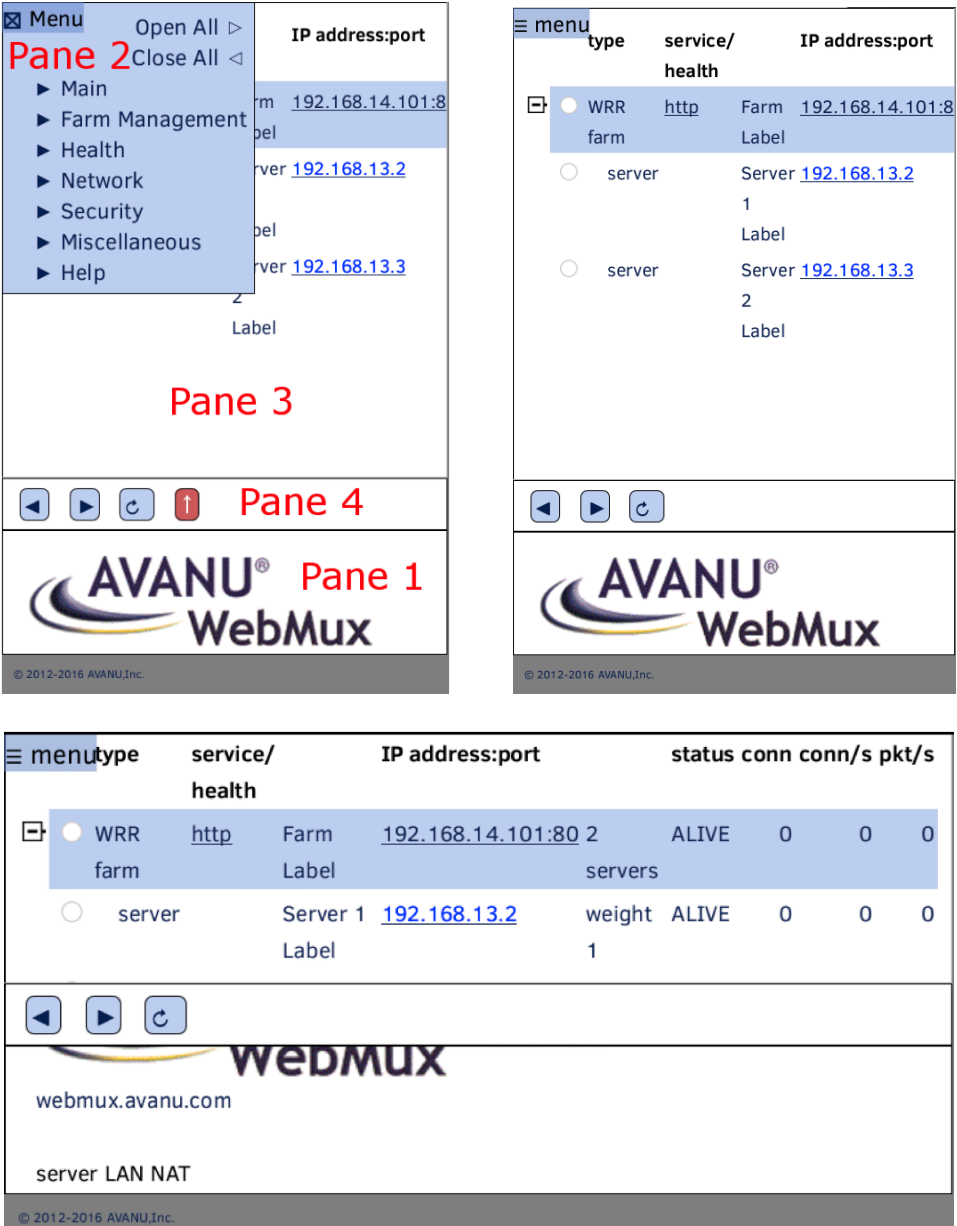
In mobile display, you can swipe to scroll the different panes vertically and/or horizontally as needed.

Logging into the WebMux Web GUI

Login Page:

Start a web browser from your management workstation.
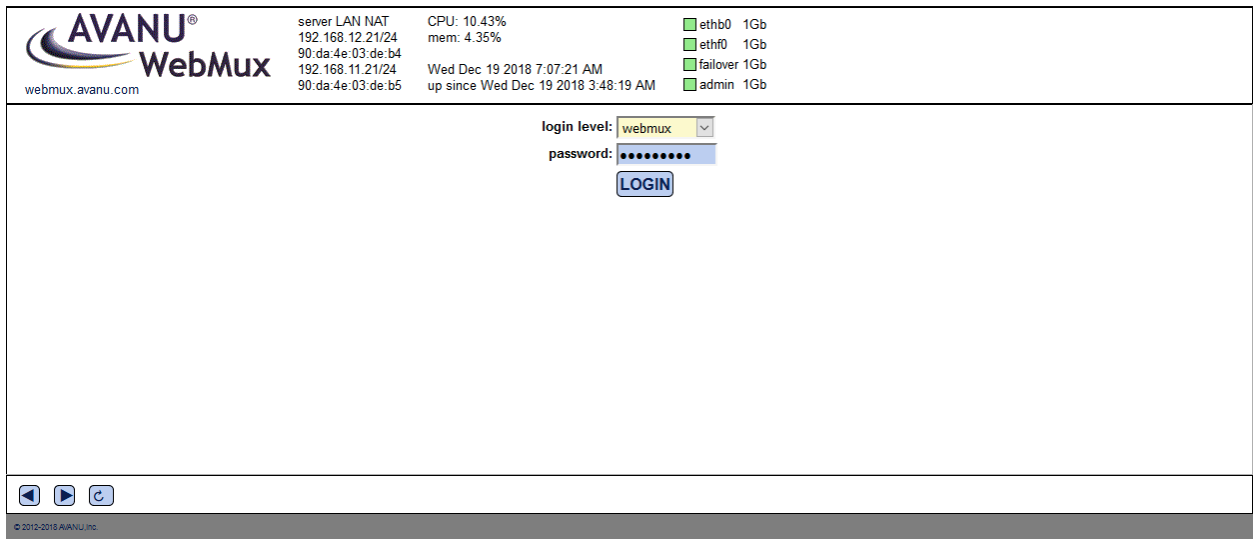
Set URL to https://webmuxip:webmuxport/

webmuxip is the IP address of the WebMux on the server LAN.

webmuxport is the management port address of the WebMux. The default ports are 24 for an unsecured connection, and 35 for the secured connection. Use HTTP instead of HTTPS on the URL line if you decide to use port 24 for unsecured communications. (The port number can be changed per your specification in the "network admin" section of the "network" menu).

The following login page will appear.

✍ In order to use a browser to manage the WebMux, the browser must be set to accept all cookies.

Login Level:

There are two preset user login levels:

1) superuser - Allows access to all screens and functions provided by the WebMux.

2) webmux - For viewing only. Does not allow the user to access or change any settings.

Password:

Fill in the correct password for the selected User ID. The password is case sensitive.

The default passwords are:

ID	PASSWORD
superuser	superuser
webmux	webmux

✍ It is recommended to change the passwords periodically. No new user ID can be added, with exception of using a TACACS+ or LDAP server

Login:

After entering the correct password, click Login.

✍ For first time setup, please login as superuser and go to the Network Admin screen, within the Network menu section. Depending on the dispatch method used, t is important to set up the Server Farm Gateway IP address and network mask first.

If you want to restrict access to the web management console to HTTPS connections only, go to the "network admin" screen within the "network" menu section and change the WebMux HTTP control port number to 0.

✍ For customers who have configured TACACS+ or LDAP support, the login screen will display the TACACS+ or LDAP user login field and password. WebMux will validate the user to the TACACS+ or LDAP server specified in the "Security Management" screen. Please refer to the "security" section further down in this section of the user manual for more details.

Main

Main Status

Once logged in to the web GUI, the main status screen will show by default. If you are logging in the WebMux for the first time, the screen will display the words, "no farms!" If you have not done so already, configure the options in the "network admin" screen before creating your farms. If you already have some farms and servers configured, you can do the following things from the main status screen:

Adjusting Health Check Timeout for Each Service

Clicking on the service type (under the service column) for the farm will take you to the "modify service timeout" screen. In that screen, you can change the timeout value of application level health check for each different service as well as other settings. For example, the default timeout to check the HTTP protocol is 5 seconds. The WebMux will wait 5 seconds for the server to respond. If the server does not repond within the timeout period, it will check again. If the server fails to respond for three consecutive health checks, then the WebMux will declare that server is dead and switch that server out from service and notify the operator through email or pager. Please note that this change is global and will affect all the farms using the same type of service.

✍ WebMux will declare a server dead only if it fails the health check 3 consecutive times.

If your web server is not really dead but for some reason is not responding to the checking request within the given timeout, the WebMux will issue a false alarm. To avoid this, the user can change the timeout value to a larger value.

Many times, servers try to and cannot resolve the IP address of WebMux server LAN interface and could cause the server to not respond to the WebMux unit's protocol checking in a timely manner. Adding the WebMux unit's server LAN IP address and server LAN gateway address to the server's name resolution table will help resolve this problem. Please reference the Frequently Asked Questions section for more information.

See "timeouts" in the "health" menu section in SECTION VI – FARM MANAGEMENT AND HEALTH for more details on the various settings you can configure.

Modify an Existing Farm

Clicking on the IP address/port of the farm the farm will take you to the "modify farm" screen for that farm. See the "Modify Farm" section in SECTION VI – FARM MANAGEMENT AND HEALTH for more details on the various settings you can configure.

Modify an Existing Server

Clicking on the server IP address will take you to the "modify server" screen for that server. See the "Modify Server" section in SECTION VI – FARM MANAGEMENT AND HEALTH for more details.

Unsaved In-Memory Configuration Changes

The "main status" screen will have an "unsaved in-memory configuration changes!" message appear if you make changes to any of your farm or server settings. You can click on the message message itself to save your settings. You can also use the "save" link in the "farm management" section of the menu to save your configuration.

✍ The main status screen updates every 5 seconds. When the mouse is hovered over it or if you touch that part of the screen on a touch screen, the updating will pause until you move the mouse elsewhere or touch another part of the web GUI.

SSL

The second item in the "main" menu section is the link to the SSL management screen. Please see the "SSL keys" section in SECTION VIII – SSL MANAGEMENT for more details about that screen.

Show Graphs

To monitor the traffic history, memory and CPU usage, the WebMux maintains some of its statistics information in the memory during running. The WebMux is able to keep a maximum of 2 weeks worth of activity history. This history of information is able to persist past reboots.
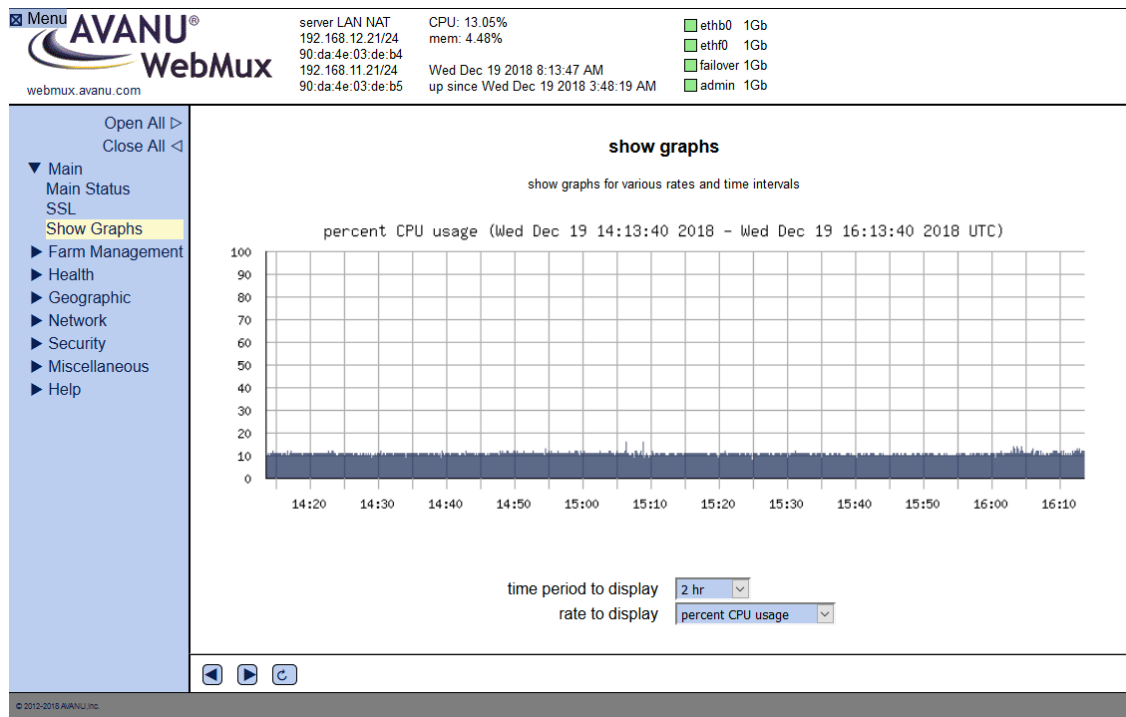
Time Period to Display

Adjust the the time span of the history you would like to view by selecting from the drop down menu:
- 2 weeks
- 1 week
- 1 day
- 12 hr
- 8 hr
- 4 hr
- 2 hr

Rate to Display

Select the information you would like to display on the graph. These are the global metrics for the WebMux unit. The choices are:
- conn/s (connections per second)
- inbound pkt/s (packets per second)
- outbound pkt/s (packets per second)
- inbound bytes/s
- outbound bytes/s
- percent CPU usage
- percent memory usage

Farm Management

See [SECTION VI](#) for details about this menu section.

Health

See [SECTION VI](#) for details about this menu section.

Geographic

See [SECTION VII](#) for details about this menu section.

Network

Network Admin

After completing the initial WebMux configuration, you will want to configure these settings next. These settings can always be changed later in the future as needed. Note that some setting will require a reboot of the WebMux to take effect.

IPv6 96-bit Address Prefix

To load balance in IPv6, you will set the option field of an IPv6 address prefix. The IPv4 addresses will be appended to this prefix. For example, if you assigned 192.168.12.21 for the WebMux unit's server LAN IP and you assigned fec0:: as the IPv6 prefix, the WebMux unit's complete IPv6 address will be fec0::192.168.12.21 (or fec0::c0a8:c15). For additional information reference the section on "IPv6 Considerations" in SECTION III – WEBMUX TOPOLOGY OVERVIEW in this User Manual.

DNS Server(s) IPv4 address(es)

The WebMux will attempt to resolve names for settings such as the email server for email notifications and front network verification (if an FQDN of an external site is used instead of your external gateway/firewall IP). Specifying DNS servers will not have any effect on the network traffic management functions of the WebMux. The DNS server of 8.8.8.8 (Google's public DNS server) is used by default. You can leave the field blank if you do not want to use this feature.

Email Server URL for Notification

The WebMux can send email notifications. Enter the IP address or FQDN of the email server that will forward the notifications.

Enter the email server information as a URL. For example:
    smtps://xxx.xxx.xxx.xxx

SMTP will use port 25. Other protocols you can use are "msa" or "submission", both will default to port 587. If only an IP address is entered, "smtps" is assumed and will default to port 465. Non-standard ports can be specified in the URL using a colon after the IP address.

Email User Name

Enter the user name or login to authenticate on your email server.

Email User Password

Enter the password used to authenticate on your email server.

Addresses for Email Notification

Enter the email addresses to be notified. Separate multiple addresses with a colon. For example: johndoe@anywhere.com:janedoe@anywhere.com

✍ When you have the email server, email user name, email password, and email addresses filled out, you can use the "Email Test" button on the bottom of the page to make sure you are able to receive emails from the WebMux.

UDP Syslog Server IP Address Notification

The WebMux can be configured to send syslog messages to a remote syslogd server. Enter the syslogd server IP address to use this feature. The syslogd server must be configured to accept remote UDP syslog connections. The facility for WebMux syslog messages is LOCAL6.

The notification levels of the syslog messages are as follows:

LEVEL	SEARCH KEY	DESCRIPTION
INFO	STATS	LCD display messages
NOTICE	LOGIN	Successful browser login/logout
NOTICE	SETUP	Significant access and changes to setup and configuration items
NOTICE	EVENT	Same as paper/mail messages
WARNING	LOGIN	Unsuccessful browser login

Server Gateway IP Address

This setting is the same setting from the "server LAN gateway IP" in the LCD and CLI initial setup. Most likely, this field is already filled with the IP that you have configured previously. You can change it here, if needed, instead of going throught the LCD or CLI setup all over again.

This setting only applies for the NAT mode (or for Direct Server Return Mode that requires the WebMux to do SSL termination load balancing. Normally, this is optional for Direct Server Return Mode). In those modes, the WebMux acts as a gateway or router for all the servers in the farms. This is the IP address assigned on the WebMux that should be used as the default gateway IP address on the web (or other) servers. It is highly recommend that it is also added to the /etc/hosts file on your servers.

✍ For first time setup, it is very important to set up this address and the Server Farm network mask (below) first. Also when setting up the servers, you may be asked to fill in the default gateway IP address for the server.

✍ It is important to reiterate that THIS IS NOT INTERNET ROUTER/FIREWALL/ GATEWAY IP/DEFAULT ROUTE IP FOR THE WEBMUX ITSELF. Putting that IP in this field WILL CREATE A DUPLICATE IP ON YOUR NETWORK.

Use this IP address as the default gateway for all the servers behind the WebMux. The network traffic load balancing will not function properly if this IP address is not set correctly for both WebMux and the servers.

WebMux HTTP Control Port

By default, the port is 24. You can change the port to any port that is not being used for any load balancing farms, if so desired. The LCD panel setup can also be used to change this.

✍ Since any IP address on the WebMux (including farm IPs) listen on the control port, a non-standard port has been selected for the management port. If you have a farm IP using port 24 as well, the WebMux will not be able to determine if the incoming connection is destined for the management console or for network traffic management. Therefore, always use a port that will not be used for any farm.

WebMux HTTPS Control Port

65

By default, the port is 35. You can change the port to any port that is not being used for any load balanced farms, if so desired. The LCD panel setup can also be used to change this.

✍   Since any IP address on the WebMux (including farm IPs) listen on the control port, a non-standard port has been selected for the management port. If you have a farm IP using port 35 as well, the WebMux will not be able to determine if the incoming connection is destined for the management console or for network traffic management. Therefore, always use a port that will not be used for any farm.

SNMP UDP Port

SNMP on the WebMux is active on port 161 by default. You can change the port here. Or you can enter "0" or "none" or leave blank to disable SNMP altogether.

SNMP Community String

The WebMux uses SNMP v1 and the community string "webmux" by default. You can change the community string in this field.

WebMux Diagnostic Ports

The WebMux allows diagnostic sessions from remote access for factory technical support or trained network engineers through ssh or telnet. Access is also subject to the restriction of the "Allowed-Host" setting earlier. "superuser" can login with its password using "ssh" to run certain diagnostic tools (help shows the commands). When this entry is blank, any diagnostic access is denied. This entry should remain blank under normal operations. Default port numbers are 77 for ssh and 87 for telnet. If only one port is specified, only ssh login is possible. You will need to notify us the port numbers before obtaining support from us.

WebMux Failover Ports

The WebMux allows configuration of failover ports being used by primary and backup WebMux units. Default port numbers are 2000 and 2001. Do not change this unless you have very specific requirements to do so.

Least Significant Bits in Client IP Address to Ignore for Persistent Connections

This setting allows persistent connections to be handled properly when clients are coming from behind cache servers. With cache servers, the IP address of the cache server is the source address. Since a client can be sent through multiple cache servers; it is possible the requests are actually coming from one client, but network traffic management will see it as different clients and sent the requests to different web servers in the farm. Therefore, applications that require persistent and secure connections, such as shopping carts, will not work properly. This feature will treat a small range of IP differences as one source, thus the WebMux can properly handle the persistent requests from browsers. From customers' feedback, three (3) is good enough for most requests.

The WebMux will use this setting to determine how to load balance the network traffic. It calculates based on two to the power of the setting value as the number of IP addresses to combine. If too large a mask applied, it will defeat the load balancing function of the WebMux.

Act as IP Router

If YES is selected, the WebMux router LAN IP can be used to route IP packets to the private server LAN side. The WebMux will not act as a firewall in this mode.

If NO is selected, the WebMux will NOT route incoming IP packets through the WebMux. Only connections to farms will be able to reach services in the server LAN side. This is the default setting.

Front Network Verification

The WebMux checks the availability of the front network by checking on the IP address you configured as your router IP ("external gateway IP"). The selection here determines the protocol used to check the connectivity of that IP address. It can be "none," "ARP," "TCP Connection," or "ICMP (ping)." Depending on how the front end router responds, this can be changed. For example, most Cisco routers will respond to the WebMux with ARP and TCP Connection; however, most Cisco DSL modems will only respond to the WebMux through ping. Changes to this verification method will take effect after the WebMux has been rebooted. If you have configured a farm on the WebMux and the farm IP address is showing dead, it is an indication that the WebMux is not able to reach the front network gateway IP. It does not, however, mean that incoming traffic to the farm IP is not able to get through. It is only an indication. Please verify that your router responds to the method you have specified in this field.

Front Network Verification IP Address

You can specify a different IP address or the FQDN of an external site (if you have the DNS server field filled in) for the WebMux to use to check the front network. It can be the router in front of the WebMux, or a router in your ISP's WAN. It can be any address that is reachable through your Internet side. The protocol specified in the above field will be used to check. If you see the farm IP turning red, it is an indication that this address failed the check. Leaving this field blank will cause the WebMux to use the IP address you specified as the "external gateway IP" when you first set up the WebMux.

Request for Updating MAC Table for Farms

This option will force the WebMux to periodically send Ethernet level ARP requests to force local machines to update their MAC tables for the farm addresses. Unfiltered network traffic captures will show periodic ARP requests coming from the WebMux. This is very minimal traffic, but some would rather try to eliminate extraneous network chatter altogether. The option here allows one to turn it off. Please keep in mind, however, that this enabling this setting is extremely important especially if a WebMux failover has occurred in a high-availability configuration. When one WebMux takes over the farm IP addresses are the same but the MAC address is changed to the current active unit. If other local machines are unaware of this, they will continue to try to communicate to the old MAC address and will be unable to reach it. The default setting is YES.

Persistence Timeout

The WebMux will keep track of the clients' browser connections if a "persistent" scheduling method for a farm is selected and accessed. The WebMux will send any request from the same browser IP address to the same server if the returning request is done within the timeout time period specified here. Our customer feedback indicates that 5–10 minutes is the best value for most cases. The larger the persistence timeout value, the less chance the

user connection will get sent to a different server. Keep in mind that by keeping a lot of connections in the WebMux memory, the maximum number of available connections for new clients will drop. Also, a large persistence timeout will cause uneven load balancing if the majority of the clients are returning clients.

UDP/NTP Time Server

The WebMux can sync its internal clock with any UDP NTP server. By default it points to a tier 2 NTP server. You can also set it to your Internet NTP server, or wipe out the entry to not sync to any NTP server.

Reset Stranded TCP Connections

When a server fails to function, there could be many TCP connections on the WebMux that are still in the TCP_WAIT state. If this is set to "YES" when client tries to access the failed server, the WebMux will pretend the server is sending TCP Reset to the client, thus freeing all the TCP_WAIT state connections. The default setting is "YES" to conserve resources.

Front Proxy Addresses

By default, the WebMux will use the main IP address you configured in the router/internet LAN interface or Bridge IP as the source IP for outgoing connections (the masquerade IP). You may want to specify a different IP address instead. You can list more than one IP address by separating them with a colon (:). If you have more than one front proxy address, the WebMux will choose a proxy address in a round-robin fashion. This option is not available in One-Armed DSR Mode.

Insert "X-Forwarded-For" (SNAT only!)

When SNAT is enabled for a farm, the WebMux will substitute its own IP address as the originating source. When you enable this option, an "X-Forwarded-For" MIME header will be inserted to the HTTP requests that will contain the original requesting client's IP address. You can use this information for your server logging or if your application server requires it.

X-Forwarded-For ports (SNAT only!)

By default, the WebMux will insert the X-Forwarded-For MIME header for port 80 traffic. If you want the WebMux to insert the MIME headers for HTTP requests on non-standard ports, you can add them here. You can add multiple ports separated by a colon (:). For example, 80:8080:8081.

Routing Table

You can add static routes to the WebMux using the Web GUI or through the Command Line Interface (CLI). From the Web GUI menu, expand the "network" section and click on "routing table".

You should see this screen:

Routes displayed that are "grayed out" cannot be modified. To add a route, make sure "make indicated changes" is selected in the drop down menu, click the "add" checkbox, and fill in the remaining fields. Click the "submit" button. Your new route should appear along with a "delete" checkbox. You can check on the "delete" checkbox and click submit to delete the selected route. Please remember that even though a new route is immediately active once you click the "submit" button, it is not automatically saved and will get lost if the WebMux is rebooted or powered off. To save your settings, select "save displayed table" from the drop down menu and click the "submit" button.

If you made unsaved changes and want to quickly revert back to your previously saved settings, select "restore last saved table" from the drop down menu and click the "submit" button.

To get to the CLI, you can either telnet or ssh in to the WebMux diagnostic port. By default it is port 77 for ssh and port 87 for telnet. Log in as "superuser." Issue the "route" command to modify the routing table. The network interfaces are as follows:

    ethf0 — "Internet" / Router LAN interface(s)
    eths0 — Interface labeled "Backup"
    ethb0 — "Server" LAN interface(s)

    In Single Network or Transparent modes, the main interface is br0.

Modifications to the routing table issued through the CLI are automatically saved after issuing the command.

✍ If you are running a backup WebMux unit, you need to make sure you also click the save button on the main console screen in order to propagate the changes made to the backup unit.

Reconfigure

The Reconfigure button will bring you to the initial network settings page. Additional details about this can be found under the "Initial Setup Through a Web Browser" section in SECTION IV – CONFIGURING THE WEBMUX in this User Manual.

Security

Security

Allowed Remote Host IPs

The WebMux Web Management Administrative Console only allow logins from these IP addresses to establish a management session. You can allow access from more than one IP address by specifying all the allowed IP addresses separated by a ":" (except use "," as the separator for IPv6 addresses). You can put the netmask following the IP address to specify the range of hosts that can access the management console. For example, 192.168.12.0/24 will allow all hosts in 192.168.12 network to access it. Omitting the "zero" octet is allowed. For example, 192.168.12 will be allowed for Class C allowed host. If this field is left blank, you can access the Web Management Administrative Console from any IP address that is configured. It is recommended to set this up for security reasons. If the wrong IP addresses are entered, the Web Management Administrative Console login might not be possible.

Use the setup mode on the LCD panel to clear the allowed host list. This field is blank by default.

TACACS+ Server Configuration

The WebMux allows you to control the user/passwords for the "superuser" group logins with a TACACS+ server so that password changes can be administered to several WebMux machines instantly through a central authentication server. In this field you will need to specify the TACACS+ server IP with "server=xxx.xxx.xxx.xxx." Other arguments include "secret=" (if the TACACS+ server requires a password to be accessed) and "encrypt." Each argument must be separated with a space.

If for some reason the TACACS+ server is not working, the WebMux will default back to the passwords configured in its password setup screen.

71

LDAP server IPv4 URL

Access to the WebMux GUI or CLI can be authenticated by an OpenLDAP server. Enter the LDAP location as a URL, such as ldap://192.168.12.1:389.

LDAP domain

Enter the LDAP domain in this field.

Connection Warning Threshold

The WebMux monitors the number of connections established. When the number of connections is greater than the value entered, the WebMux will page the designated numbers. For example, if a DoS attack is occurring, the number of connections to the site would be extremely high. Assuming they exceeded the value set for the "connection warning" threshold, the designated numbers would be paged.
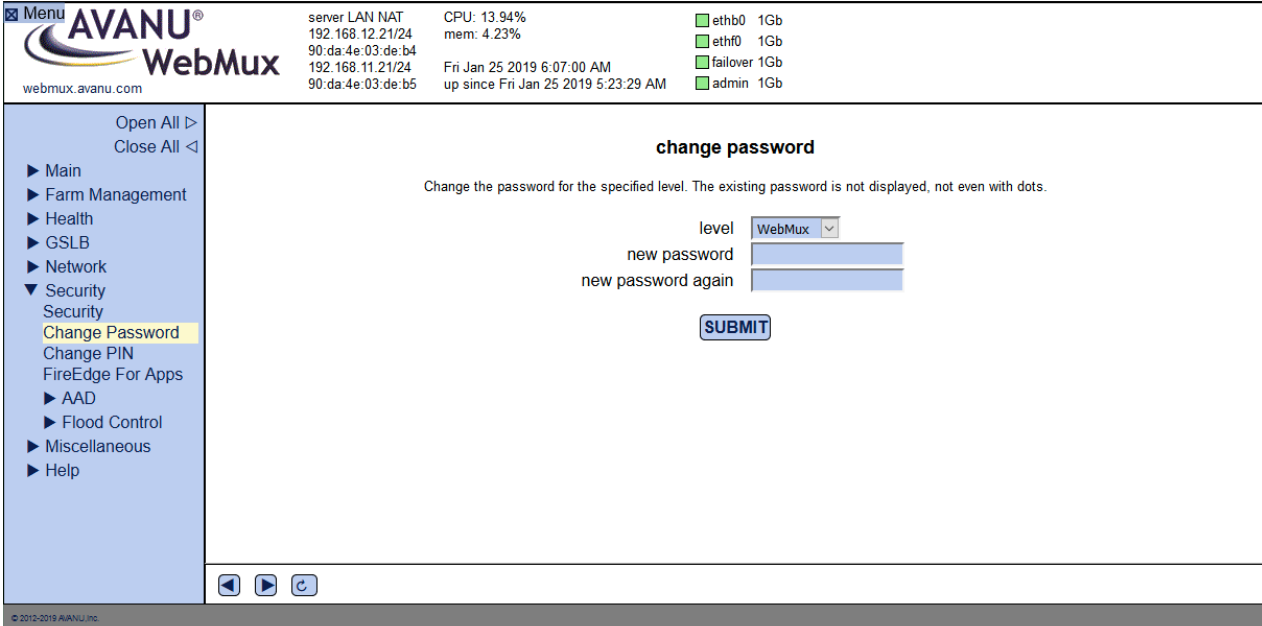
ICMP Packet Input Policy

Accept: The WebMux will allow all ICMP packets to travel through the WebMux or to IPs on the WebMux itself. For CLI arp commands to work properly, this must be set to accept.

Deny: The WebMux will NOT allow any ICMP packets to travel through the WebMux.

✍ During installation, having the ability to ping the other hosts on the networks is typically useful when the installation is complet, setting the "ICMP packed policy" to DENY is recommended as a security precaution.

Change Password

Level

Select the login level for which the password is to be changed.

New Password

Enter the new password for the selected login level.

New Password Again

Enter the same password as in the previous box. If this does not match the password entered in the previous field, you will get a notification page stating so and you will need to try again.

Submit

Click "submit" to execute the change.

Change PIN

To protect the WebMux from unauthorized changes from the front LCD panel, a PIN can be entered here to prevent saving any changes from the front LCD panel. By default, there is no PIN. You can unset the PIN by submitting blank fields. If a PIN was set and you want to remove it, you can set this to 0000.

FireEdge for Apps – Powered by ModSecurity

ModSecurity is an open source Web Application Firewall from Trustwave Spiderlabs. As of version 13.1.00, ModSecurity and OWASP Core Rule Set 3 has been integrated into the WebMux for our FireEdge for Apps Web Application Firewall feature. This screen is the global setting to select the rules to enable or disable. You can make multiple selections by holding down the control key and clicking the left mouse button. Use the single arrow button to move the rules into the active or inactive box. The double arrows functions the same have having selected all the rules and moving them to the desired box. Actives rules will be applied to all farms that have FireEdge enabled from the "Add Farm" screens.

Press the submit button to complete the changes.

AAD (Automatic Attack Detection)

The Automatic Attach Detection (AAD) security feature controls how many concurrent open TCP connections from a single source IP address is allowed to connect.

Management

TCP Connection Attack Threshold

This will set the maximum number of concurrent connections a client can make before the WebMux will consider it an attack. You do not want to set this value too low because most of the time, servers will experience several concurrent connections during normal operations. Usually a DoS or DDoS connection attack comes in by the hundreds. Set this value according to your needs.

Client Whitelist for TCP Attacks

It may be necessary to allow certain IPs to make connections that may appear to be attacks. For example, if you have a third party company that regularly benchmarks your services for maximum load handling, you will need to allow that company uninterrupted access. You can use a specific IP address or specify a network range (i.e. xxx.xxx.xxx.0/24). Separate each entry with a colon (:). Use the appropriate IPv4 and/or IPv6 fields for IPv4 and/or IPv6 addresses.

Client Blacklist for TCP Attacks

If you have specific IPs you want to block, you may enter them in the appropriate IPv4 and/or IPv6 fields for the Client Blacklist for TCP Attacks. Just like the whitelist, you can use specific IP addresses or a network range (i.e. xxx.xxx.xxx.0/24). Separate each entry with a colon (:).

Duration to Block Attackers

This sets the amount of time to block attacker IP addresses. It may not be desirable to block specific IP addresses indefinitely because of the dynamic nature of IP addresses used by the general public. You may end up blocking out potential customers in the future. Therefore, this setting allows you to set the IP blocking duration that suite your needs.

Changing the settings in this page will not require a reboot and is effective once you click the confirm button.

AAD Display

The AAD Display screen will show you the list (if any) of source IP addresses that are currently being blocked because of excessive activity.

AAD Download

This link will download a text file copy of your whitelist and blacklist

Flood Control

The Flood Control security feature limits the maximum allowable packet transfer rate for any single IP address connecting through the WebMux.

Packet Rate

This will control the packets per second rate that will be allowed.

Packet Threshold

Some attacks are done in bursts rather than large streams. While the packet rate parameter will control the maximum allowable steady rate of packets, the packet threshold detects the maximum allowable packet bursts.

Timeout in Seconds

This setting will control duration in seconds that the connection blocking will be upheld.

Flood Control Display

The Flood Control Display screen will show you the list (if any) of source IP addresses that are currently being blocked because of excessive activity.

Flood Control History

The Flood Control History screen will show all the past and current blocked and released IP addresses.

Miscellaneous

Show Events

This page will show you the history of WebMux events such as detection of server dead status. Events will be saved past reboots. You can clear the events history by clicking on the "Delete" button.

AVANU®
WebMux
webmux.avanu.com

server LAN NAT
192.168.12.21/24
90:da:4e:03:de:b4
192.168.11.21/24
90:da:4e:03:de:b5

CPU: 13.25%
mem: 4.39%

Fri Jan 25 2019 6:37:58 AM
up since Fri Jan 25 2019 5:23:29 AM

☐ ethb0   1Gb
☐ ethf0   1Gb
☐ failover 1Gb
☐ admin   1Gb

Open All ▷
Close All ◁
▶ Main
▶ Farm Management
▶ Health
▶ GSLB
▶ Network
▶ Security
▼ Miscellaneous
　Show Events
　Backup/restore
　Set Clock
　Banner
　Upgrade
　Show Connections
　Wizards
　Tcpdump
　Login
　Logout
　Reboot
　Shutdown
▶ Help

WebMux events

Jan 25 07:35:39 2019: server failure:"Server 1 Label" 192.168.11.114:*, http port 80 in http farm "Farm Label" 192.168.12.200:80, communication error: Resource temporarily unavailable

Jan 25 07:35:55 2019: server failure:"Server 2 Label" 192.168.11.115:*, http port 80 in http farm "Farm Label" 192.168.12.200:80, communication error: Resource temporarily unavailable

[DELETE]

◀ ▶ ↻

© 2012-2019 AVANU,Inc.

Backup/Restore

Backup

This feature allows the saved configuration to be saved as a file on the local computer you are using to access the WebMux web interface. Be sure you have saved your farm configurations from the main screen before exporting your configuration to ensure that you are getting your most recent changes.

There are two levels of backup: 1) farm and server information only, and 2) all settings.

The "farm/server information" backup will save only the farm and server configurations and settings to a plain text file. Click on the Click Here link to display the configuration. Choose 'File->Save As' from the browser menu to save it as a text file. It is possible to make changes to this file and uploaded back to the WebMux to make instantaneous bulk changes to the farm and server configuration. DO NOT change the first comment line.

The "all settings" backup is an encoded plain text file that not only includes the farm/server configurations and settings, but all other settings just as the units main IP addresses, settings from the network administration, and so forth. This file cannot be edited.

Restore

Restore allows a configuration file that has been saved at the browser workstation to be uploaded to the WebMux. Enter the full path of the configuration file, or click on Browse to search for the file. Click Upload to upload the file to the WebMux. This file will immediately

become the saved and active configuration. Upload ALL Settings to WebMux will actually upload settings including IP addresses, farms, and information you entered in the Network Admin screen. If you want to replace the WebMux with a new unit, you could save the configuration and upload all settings to the WebMux, so that you do not need to go through step by step configuration. Only restore an all settings backup to a unit running the same firmware version. Restoring to different firmware versions may not carry over setting from old to new firmware, or vice versa, correctly and can cause unpredicatable behavior.

Set Clock

Click the "set clock" link in the drop down menu and proceed to the page that controls the clock settings. The time and date of the WebMux can then be set. Please note that the WebMux internally uses GMT time zone, not your local time zone, per W3C/HTTP protocol. If the time zone is not set correctly, the browser access could be denied due to "cookie" time out. If the UDP NTP server is set up correctly, there is no need to set the clock anymore, since the WebMux automatically sets its clock periodically.

You have 3 ways to set the clock on the WebMux.

1. Automatic will use the WebMux unit's own predetermined NTP server to set the clock.

2. Use the NTP server specified in the "Network Management" page:

3. Set the time manually using the form:

Month

Enter the number of the month, 1 through 12. Leading zeroes are not necessary.

Day of the Month

Enter the day of the month, 1 through 31.

Year

Enter the year. Enter all 4 digits.

Hour

Enter the hour of the day. Use the 24 hour clock (military time).

Minute

Enter the minute of the hour.

Time Zone

Select the time or hour offset to the UTC (GMT) time. You can set the WebMux to your local time, if your time zone is selected here.

Submit

Click "submit" to execute the date and time change.

✍ It is recommended to set the WebMux clock to UTC (GMT) time

Banner

This screen will allow you to customize the login banner that will be seen on the telnet and SSH login prompts.

Upgrade

To upgrade the WebMux firmware, you will first need to contact WebMux support at techsupport@avanu.com and request for the latest firmware image. Save that image to your local computer and use the Browse button to find that file. After you have selected the file, click the "Submit" button. The text box below will show the progress of the upgrade.

Show Connections

This screen will let you track the connections going through the WebMux

show connections through webmux

Show connections filtering and sorting as specified. Unspecified or IP addresses are not compared. Comparison addresses are IPv4 dotted quads. For IPv6 addresses, the least significant four bytes will be compared to the given IPv4 addresses. Most browser will allow changing file name if "save?" is specified.

client address	
client port	0
farm address	
farm port	0
server address	
server port	0
sort by client	○
sort by farm	○
sort by server	○
do not sort	◉
save?	NO

SUBMIT

Wizards

This will take you to the configuration wizards index page:

The configuration wizards are intended to be a first time and one time use feature. These wizards will set all the main settings for the WebMux (IP addresses, dispatch method, farm and servers, etc.) all in one shot. Running a configuration wizard will always overight any existing WebMux configuration.

The wizards interface is slightly different from the regular WebMux interface. Each wizard is a single form with the sections done in an "accordion" style interface. Each heading will expand a section. Each section will contain specific instructions. Please read carefully the instructions. Select and fill in the appropriate fields. Once you have gone through all the sections, you will need to supply the superuser password (by default it is "superuser"). The wizard form will be submitted and the WebMux will automatically reboot. After the WebMux is back online with the new configurations, you can log in to the main WebMux interface and see the farms created by the wizards. You can modify the existing farms; or add or delete farms as needed.

TCPdump

The tcpdump page allows you to do a simple packet capture session through the web interface. Tcpdump is a useful utility for network traffic diagnotics. You can use this to check if hosts are passing through the WebMux or to check if the WebMux is sending packets to the proper distination, among other things. For more advanced tcpdump options, use the tcpdump utility from the CLI. Tcpdump is a linux utility. You can search online for the tcpdump manpage for detailed information.

IP address

Specify the IP address of the host you want to capture.

Port number

Specify the port you want to filter for.

Count

This will stop the capture when this number of packets have been reached

Timeout in seconds

This will stop the capture when the timeout period (in seconds) has been reached.

Login

This will bring you back to the login screen should you wish to quickly switch user accounts. THIS DOES NOT LOG OUT YOUR CURRENT SESSION. When you log in as a different user, the old session will end. However, we normally recommend that you correctly end your current session by using the Logout from the drop down menu.

Logout

It is not recommended to leave the management browser logged in unattended. Click the "confirm" button to close the session. The "Login" screen will re-appear.

Reboot

Changes to "TACACS+ server configuration," "server gateway address," "server farm network mask," "WebMux http control port," "WebMux https control port," "WebMux SNMP UDP Port," "WebMux SNMP Community," "WebMux diagnostic ports," "least significant bits," "forwarding policy," "front network verification," and "persistence timeout", many other fields that are marked with an asterisk (*) require a reboot for the new configuration to take effect. You can use the Reboot button to reboot the WebMux remotely. Reboot button will require confirmation before proceeding with reboot.
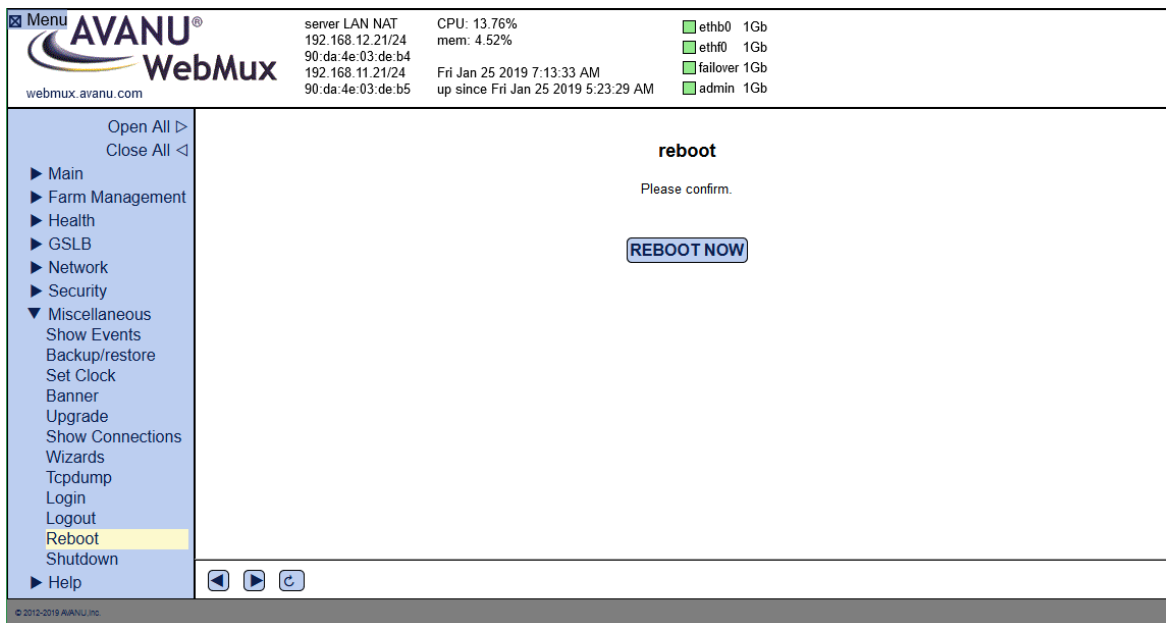
Shutdown

The shutdown button will bring you to a confirmation screen to power off the WebMux.

90
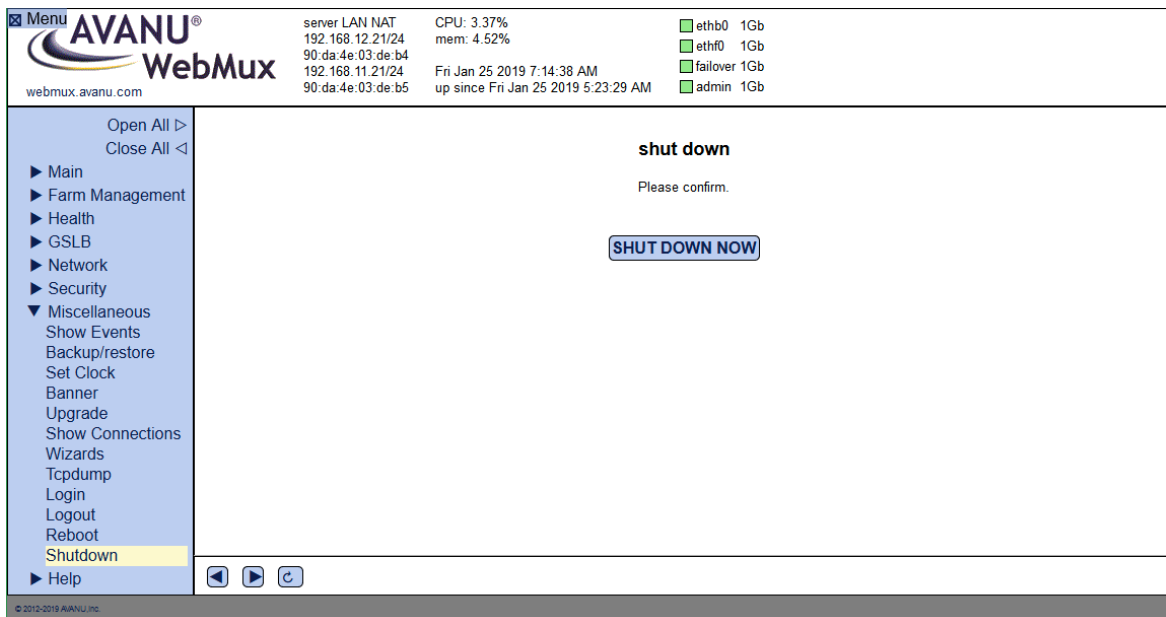
Help

Online Manual

This will open a new windows to take you to the www.avanu.com support pages.

About WebMux

This will take you to the "about" screen of the WebMux. Here you will see information about your WebMux unit, such as the firmware version, the model number, the serial number, etc.

SECTION VI – FARM MANAGAMENT AND HEALTH

Farm Management

Add Farm

This screen is where you create your farms and select your options for load balancing. Some fields may be displayed or hidden depending on what options you might select.

Label

This is for your visual reference to be displayed on the main console for the farm entry. It can be any alphanumeric text.

Farm IP Address

This is the IP address of the new farm.

For SSL terminated traffic, each farm must have its own IP address.

If your WebMux is on the public Internet the farm address could be an Internet known address. Or, if the WebMux is behind a firewall, the address can be an IP that is NAT'ed by your firewall. For example, if you want to create an HTTP farm for www.mydomain.com, the

farm IP address will be the IP address for www.mydomain.com from your DNS record. If the IP address of www.mydomain.com is 205.188.166.10, then the Farm IP address is also 205.188.166.10. The WebMux will then forward requests to the farm address to the web server address in your DMZ or internal network.

Virtual Host Name

For web servers that are serving name based virtual hosts, this field will be important for the WebMux to perform a correct health check. The WebMux uses the data in this field as the host name for the HOST mime header in its HTTP health check requests to the servers. In some cases, name based virtual hosts have a default site that will still respond with a 400 OK even if a HOST MIME header is not specified in the request. In that case, leaving this field blank may not have a negative effect. However, in other cases, a request that does not have a specified HOST MIME header will end up receiving response from the server such as 503 Service Unavailable. In which case, the WebMux will mark the server dead. Therefore, it is important that you specifiy the correct host name of the site you are serving for the farm in order for the WebMux health check to reach the correct site and get a valid response from the server.

The format for the virtual host name field should be the site host name (i.e. www.xyz.com), max length 75 bytes. Without a virtual host name specified, a 401 (Unauthorized) error code is still considered a live server. If you have a virtual host name specified and the server returns error code 401, then the WebMuxwill consider that server dead. For both Microsoft® IIS and Apache® servers doing virtual hosting, the virtual host name field must be an existing web site name on the server.

Virtual Hosting Issues

Servers serving more than one web site may do virtual hosting. The WebMux supports virtual hosting by checking the virtual server's response. There are three different situations for the WebMux to handle.

WebMux supports health checking HTTPS servers with SNI (server name identification) capability. If the web server supports SNI, the WebMux will be able to supply the virtual hostname specified in the virtual host name field in order to do the HTTPS health check for that specific host name.

For servers that do not have SNI support, there is no way to do virtual hosting on the same IP address with HTTPS. The reason that each HTTPS server must have its own IP address is because the web server cannot see the host name in URL of the HTTPS packets, since they are encrypted. The server only decrypts the URL after the packet is sent to a particular process. In those circumstances each HTTPS farm can be on a different IP address on the same server.

If the service is HTTP, then any web server software, Microsoft® IIS or Apache®, can host almost unlimited virtual farms on each IP address. Many hosting centers handle this situation by putting all the servers serving each virtual host on a server farm on the WebMux. The WebMux will load balance the traffic for all the incoming traffic for that IP address to different servers in that farm. During farm setup, the virtual host name for the farm could be one of the virtual farm's base URL, say www.mydomain.com, the WebMux actually periodically reads a page from this URL. If the server that serves that URL does not response correctly, the WebMux will mark that server dead. Since every server in that farm serves all the virtual farms, the WebMux expects the problem with one server in one URL will affect all the URLs in that farm.

Another situation: the server that serves HTTP virtual sites is using a single private IP address already before load balancing. After adding a load balancer, some of the sites want to have their own IP addresses. The WebMux allows the set up of a separate farm for each site having its own public IP address, but each farm will have the same sets of servers in the private network. In this situation, each separate farm could have its own label as www.site1.com and www.site2.com, etc. The WebMux will actually do a health check on each URL by periodically reading a default page from that site.

In the virtual hosting situation, the virtual host name field and response from the web servers are critical for reliable services. The WebMux checks the server for its health situation based on the virtual host name supplied in the field. If the server response is 500 or, which is an error code indicating server internal error, the WebMux will exclude that server from serving the farm. If server responses 402, which indicates access is denied for that virtual farm, the WebMux will mark that server dead. We have checked with Microsoft® IIS server and Apache® server sertups and they both follow the same rules.

Port Number

This is the listening port for the farm. If you are choosing one of the known services (see below), you do not have to specify anything in this field. However, if the service you choose is not listed in the list below, you will need to specify a port number here. For example, for Microsoft® Terminal Services, use port number 3389.

If you enable SSL termination (see "Enabling SSL Termination" section), you can specify port 80 for the farm and servers in the farm. Choosing "HTTP—hypertext transfer protocol will automatically specify port 80 for the farm. You can also specify non-standard ports for the clear traffic port, if needed. There is a separate field to specify the SSL port. By default, the WebMux will terminate all SSL traffic on port 443 and send them to port 80 on the servers, unless you specify different ports.

Scheduling Method

The scheduling method is the way in which traffic is distributed among the servers in the farm. Ten (10) different methods are supported. Persistent scheduling methods track the client IP in order to return them to the same server upon reconnection within a given timeout period. For example, if you are using a shopping cart service, a persistent scheduling method is recommended.

- Least connections

- Least connections—persistent

- Round robin

- Round robin—persistent

- Weighted least connections

- Weighted least connections—persistent

- Weighted round robin

- Weighted round robin—persistent

- Weighted fastest response

- Weighted fastest response—persistent

- HTTP to HTTPS redirect (see SECTION X for more information about this feature)

Service

Select the service the type of that is running on the servers in the farm. This selection determines the method which the WebMux will check the server health status. The service type selection will automatically assign a well-known listening port for the farm. You generally will not need to specify the port number if the service protocol is on the list. However, you can manually modify it if your service is using a different port number, but you still want to use the type of health check determined by the service selection. If your service is not listed, then choose one of the "Generic" selections and enter the port number in the PORT NUMBER field. The WebMux has level 7 protocol checks for the known ports in the list. For Custom Defined TCP Service (custom health check), please specify the URL for the CGI code in the Administration Setup screen.

Warning! Once a farm is created, the port number cannot be changed. Like the IP address, the farm must be deleted and a new one created in order to change farm settings.

✍ Please choose "Generic TCP" and specify port number, if service is not listed below. If multiple ports to be used, please also select "Generic TCP" and specify port number "0."

SERVICE	PROTOCOL	COMMON PORT #
DNS – Domain Name Service	TCP	53
FTP – File Transfer Protocol	TCP	21
HTTP – Hypertext Transfer Protocol	TCP	80
HTTPS – Secure Hypertext Transfer Protocol	TCP	443
HTTP/HTTPS Combined Ports		80/443
LDAP – Lightweight Directory Access Protocol	TCP	5050
NNTP – Network News Transfer Protocol	TCP	119
NTP – Network Time Protocol		123
POP3 – Post Office Protocol		110
SMTP – Simple Mail Transfer Protocol	TCP	25
SNPP – Simple Network Paging Protocol	GCP	444
Generic	TCP	User Specify
Generic	UDP	User Specify
Generic	TCP/UDP	User Specify

Generic – No Health Check	TCP	User Specify
Generic – No Health Check	UDP	User Specify
Generic – No Health Check	TCP/UDP	User Specify
Custom – Defined Services	TCP	User Specify
Custom – Defined Services & Generic	TCP	User Specify
Custom – Defined Services	UDP	User Specify
Custom – Defined Services	TCP/UDP	User Specify
Custom – Defined Paired HTTP and HTTPS Services	TCP	User Specify

SNAT

Enable SNAT for the farm. SNAT means that all requests being load balanced through the farm will have the source IP that comes from the WebMux rather than the original requesting client.

Farm Will Use MAP

If the Multiple Address/Ports feature is going to be used, this must be selected upon creation of the farm. This cannot be set or disabled once the farm is created. You will need to delete and recreate the farm to change this. Also, the MAP feature cannot be enabled in conjunction with any Layer 7 features or the Compress HTTP Traffic feature.

SSL Termination

You must first import your private key and certificate in the SSL Key Management screen. Please see SECTION VIII – SSL MANAGEMENT for detailed information on importing or generating your keys and certificates.

Selecting an SSL key in this section will enable SSL termination for this farm.

The HTTP service and POP3 service terminate to ports 443 and 995, respectively, and will allow you to choose any port for the clear traffic to the servers.

When using the generic or custom services, specifying the clear traffic port for the service in the
"port number" section causes the WebMux to automatically assume the secure port for the following services:

CLEAR TRAFFIC PORT	SECURE PORT	SERVICE
80	443	HTTP
110	995	POP3
23	992	Telnet
25	465	SMTO

119	563	NNTP
143	993	IMAP
194	994	IRC
389	636	LDAP

Any of the port assignments can be manually overridden.

SSL Port

If the SSL traffic is not standard secure port listed above, user can specify his own.

Block Non-SSL Access to Farm

Block non-encrypted incoming traffic so that only encrypted traffic can reach your server. This might be useful when you only want encrypted connections.

Tag SSL-terminated HTTP Requests

If the "Servers are HTTPS Servers, Re-encryption" setting is set to "No", traffic between the WebMux to your servers will be unencrypted traffic. Your servers will not be able to tell if the originating connection was HTTPS or HTTP. This may be important if the application on the server requires that kind of information. You can turn on "tag SSL-terminated HTTP requests." By selecting "Yes," the decrypted traffic to the servers will have the added MIME header "X-WebMux-SSL-termination: true" and "X-Forwarded-Proto: https". It is up to you how you want the server to process this information. For example, you can write a script on your server to identify if the original traffic was HTTPS or HTTP, and then properly redirect the traffic to the HTTPS.

The WebMux allows SSL termination for any farm port. If your SSL/TLS traffic is other than the standard HTTPS traffic, you can specify the SSL port in the "SSL port" field.

Servers are HTTPS Servers, Re-encryption (Layer 7)

This is only allowed on a farm doing SSL termination. When it is not enabled the forwarded client connections between the WebMux and the real servers are unencrypted. With this option enabled, the WebMux will use a secure, encrypted connection between itself and the real servers. Microsoft® Lync® and Exchange® servers may need this feature.

Servers Only Serve IPv4, Not IPv6 (Layer 7)

If the incoming traffic is IPv6, WebMux can map them into IPv4 servers.

Health Check Port Number (for generic TCP and custom TCP services)

By default, the WebMux will do its custom service check on port 80 no matter what port you set up for the farm. If you wish to change this, you can specify a port here. This is a global setting and will be used for all farms using the custom health check service.

Compress HTTP Traffic

Selecting "yes" to this option will activate the WebMux HTTP compression. If the client web browser sends out a MIME header that states that it accepts compressed data, the WebMux will compress HTTP data to the client browser. If the WebMux detects that the servers in the farm are already compressing the data, the WebMux will not perform compression. Instead, it will let the compressed data from the servers pass through without additional processing. When enabled the MIME header "X-WebMux-Compression: true" will be appended to the server response MIME header.

The WebMux will also automatically disable compression should its CPU usage reach 50%.

✍ The MAP feature cannot be used in conjuction with the compression feature.

HTTP Caching

When HTTP caching is enabled, the WebMux will cache web pages and serve them on the server's behalf. This alleviates server load the best when the site is mostly static pages. Dynamic content is not cached. The WebMux reserves 2GB of internal SSD space for cache storage and will automatically remove old cached pages when space is needed. Cache storage is cleared upon reboot.

HTTP Server Response Comparison String

When a string is entered in this field, WebMux HTTP Health Check will search the first 1024 bytes in the HTML content. String is a case sensitive match.

HTTP Server URI

By default, WebMux health check checks default page loading. If specifying a URI here, the WebMux will use this URI instead of the default page do health check.

Layer 7 Cookie MIME Header Perl Regex Match

When a string is entered in this field, the cookie MIME header of the HTTP request is examined for a match. Only matching requests will continue through to be forwarded to the servers in this farm.

Layer 7 Host MIME Header Perl Regex Match

When a string is entered in this field, the host MIME header of the HTTP request is examined for a match. Only matching requests will continue through to be forwarded to the servers in this farm.

Layer 7 Request URI Path Perl Regex Match

When a string is entered in this field, the request URI (the part after the domain name) will be examined for a match. Only matching requests will continue through to be forwarded to the servers in this farm.

Layer 7 Load Balancer Cookie Name

Text entered into this field will be used as the load balancer cookie name that the WebMux will generate. This field will only be visible if you select persistent scheduling method.

Use FireEdge

In order for this option to be available, you will need to enable a Layer 7 feature for the farm. You can enable Layer 7 without doing any actual match pattern testing by using the "wildcard" pattern: .* (a period followed by an asterisk). Once you have entered something in any of the Layer 7 match pattern fields, the 'use FireEdge' field will appear. Selecting "YES" will enable the FireEdge Web Application Firewall for this farm. The web application firewall rules that are applied can be can be selected in the FireEdge section of the GUI.

Add Server

In the Modify Farm screen click on the "Add Server" button to add a new server to this farm. Or you can select the radio button of the farm from the main screen and click on the "Add Server" button on the left.

Server IP Address

Enter the IP address of the real server to be added to the farm.

Warning! Once the server is added, the IP address cannot be changed. To correct the IP address, the server must be deleted and a new one be created.

Server Port Number

If the port number specified in the farm setup is the same as the real server's port number, you can leave this as "same." In NAT mode, the WebMux can perform port forwarding from the farm IP port to the server IP port if you specify a server port that is different from the farm port.

Warning! Like the IP address, once created, the port number cannot be changed. To correct the port number, the server needs to be deleted and a new one to be created.

Label

Add a label to each server's IP address. The purpose of labeling a server is only to help identify the server in the farm. It has nothing to do with the name resolution of the server. Although a label can be anything, it is always better to have a meaningful and unique label for each server.

100

Weight

This is for scheduling priority weight. Valid integer numbers are between 1 and 100. A server that has a weight of 2 will be directed twice as much traffic as a server with a weight of 1.

A special zero weight setting is provided for a graceful shutdown of a server. When the weight is changed to zero, the WebMux will not send new connections, but will maintain all current connections to the server. The connections will gradually reduce to zero as current clients' sessions terminated. When there are no connections, the server is functionally "dead" or off line until the weight is changed back to a valid number. Then the server can then be shutdown or taken out of service without affecting any users.

> **Warning!**   Unlike a server that can go down unexpectedly, the WebMux will not move a STANDBY server to ACTIVE when one or more server's weight is set to zero. If the weight of all the servers in a farm were set to zero, then the farm would be "down" because none of the servers are accepting new connections.

> ✍   If your scheduling method is of the "persistent" type, be aware that the WebMux will continue to honor those existing persistent sessions. If you have clients that continue to return before the persistence timeout has expired, then you will continue to see connections coming in.

Run State

Active - The server will be put into service immediately after it is added. If there are servers in the farm in Standby, the WebMux will activate a Standby server in its place if it goes out of service. When the original server comes back in service, it will stay in Standby mode until manually setting its run state to Active again through the browser interface. This will give the system administrator time to fix the system or reboot the server once some software/hardware update is completed.

Favorite Active - The server will be put into service immediately after it is added. If a Favorite Active server failed, once it is operational, the WebMux will automatically put it back to the Active state.

Standby - The server will be put into STANDBY, or backup, mode after it is added. The WebMux will change a STANDBY server to ACTIVE when one or more ACTIVE servers fail. The weights will also have an effect on the number of standby servers that are activated. If the failed active server had a weight of 20 and there are two standby servers with the weight of 10, the WebMux will activate the two standby servers to make up the difference.

Last Resort Standby - The server will be put into STANDBY state. Unless all other servers are out of services, this server will not be switch in. This will allow the last server to show a different web page from others.

Modify Farm

The "Modify Farm" screen can be invoked from the main management console screen by clicking on the farm IP address or selecting a radio button of a farm and clicking the "Modify Farm" button on the left side of the screen.

The "Modify Farm" screen looks like this. Some of the fields will be hidden or displayed depending on some of your selections.

Farm IP Address and Port Number

The farm IP and port that is being modified will be displayed. These fields are set in the "Add Farm" screen. Once set, they are not changeable. If they must be changed, delete the farm and then add a new one.

Label

This is for your visual reference to be displayed on the main console for the farm entry. It can be any alphanumeric text.

Virtual Host Name

For web servers that are serving name based virtual hosts, this field will be important for the WebMux to perform a correct health check. The WebMux uses the data in this field as the host name for the HOST mime header in its HTTP health check requests to the servers. In some cases, name based virtual hosts have a default site that will still respond with a 400 OK even if a HOST MIME header is not specified in the request. In that case, leaving this field blank may not have a negative effect. However, in other cases, a request that does not

102

have a specified HOST MIME header will end up receiving response from the server such as 503 Service Unavailable. In which case, the WebMux will mark the server dead. Therefore, it is important that you specifiy the correct host name of the site you are serving for the farm in order for the WebMux health check to reach the correct site and get a valid response from the server.

Scheduling Method

Ten (10) different methods are supported:

- Least connections

- Least connections - persistent

- Round robin

- Round robin—persistent

- Weighted least connections

- Weighted least connections—persistent

- Weighted round robin

- Weighted round robin—persistent

- Weighted fastest response

- Weighted fastest response—persistent

SSL Termination

You can enable or change the SSL key/certificate pair used for this farm. All current connections for this farm will be reset if you change the key/certificate pair selection.

SSL Port

This is this is the SSL port for the farm that clients will connect to. Standard ports will automatically be chosen for certain standard services. Otherwise, you can specify your own. This does not necessarily need to correlate to the SSL port of the servers behind the farm, unless their ports will be configured as "same" when adding them.

Block Non-SSL Access to farm

If you do not want to allow non-encrypted traffic connecting to the farm, select "Yes."

Tag SSL-terminated HTTP requests

If SSL termination is active for this farm, choosing "Yes" for this option will add "X-WebMux-SSL-termination: true" and "X-Forwarded-Proto: https" MIME headers in the decrypted HTTP request going to the real server.

Servers are HTTPS Servers, Re-encryption (Layer 7)

This is only allowed on a farm doing SSL termination. When it is not enabled the forwarded client connections between the WebMux and the real servers are unencrypted. With this option enabled, the WebMux will use a secure, encrypted connection between itself and the real servers. Microsoft® Lync® and Exchange® servers may need this feature.

Servers Only Serve IPv4, Not IPv6 (Layer 7)

If the incoming traffic is IPv6, WebMux can map them into IPv4 servers.

Compress HTTP traffic

Enable or disable HTTP compression. When enabled the MIME header "X-WebMux-Compression: true" will be appended to the server response MIME header. (NOT supported in Direct Server Return Mode, except when used in a Layer 7 Farm; or with farms that have MAP enabled).

HTTP Server Response Comparison String

When a string is entered in this field, WebMux HTTP Health Check will search the first 1024 bytes in the HTML content. String is a case sensitive match.

HTTP Server URI

By default, the WebMux health check checks default page of the server. If specifying a URI here, the WebMux will use this URI instead of the default page do health check.

Layer 7 Cookie MIME Header Perl Regex Match

When a string is entered in this field, the cookie MIME header of the HTTP request is examined for a match. Only matching requests will continue through to be forwarded to the servers in this farm.

Layer 7 Host MIME Header Perl Regex Match

When a string is entered in this field, the host MIME header of the HTTP request is examined for a match. Only matching requests will continue through to be forwarded to the servers in this farm.

Layer 7 Request URI Path Perl Regex Match

When a string is entered in this field, the request URI (the part after the domain name) will be examined for a match. Only matching requests will continue through to be forwarded to the servers in this farm.

Layer 7 Load Balancer Cookie Name

Text entered into this field will be used as the load balancer cookie name that the WebMux will generate. This field will only be visible if you select persistent scheduling method.

Use FireEdge

You will only see this field if FireEdge was enabled when the farm was originally created. You can disable it by selecting "no".

Delete

Click this button to delete the entire farm.

Warning!   This function also deletes **ALL** the servers under this farm

Delete Farm

This link carries out an action that requires you to first select a farm using the radio button for the farm in the Main Status screen. Once you have selected a farm radio button, you can click on this link to delete the farm. If you click on this link and you have not selected a farm from the main screen, you will see a notification instructing you to select a farm. If you click on this link while in a different screen. You will see a notification and will be redirected back to the Main Status screen, where you can select a farm you want to delete.

You can also detele the a farm by clicking on the the farm IP:port link on the Main Status screen which will take you to the "Modify Farm" screen. From there, you candelete the farm using the "Delete Farm" button.

Modify Server

This link requires you to first select a server using the radio button from the Main Status screen. Once you have selected the server, you can click on this link to get to the "Modify Server" screen. You can also get to this screen by clicking on the the server's IP address from the Main Status screen.

Destination server IP address and port number:

The IP and port of the selected server is displayed. These parameters are set in the "Add Server" screen. Once set, these fields cannot be modified. To correct this setting, delete the server and add a new one.

Label:

The label can be changed at any time. The change will not affect how the server functions in the farm. It is for description purpose only.

Weight:

This is for scheduling priority weight. Valid integer numbers are between 0 and 100. Changing the weight to zero will stop the incoming connections while all existing connections continue until time out or connection is terminated by client and server. Although all numbers from 1 to 100 will allow traffic to go through, using a smaller weight number in each server will have the best load-distributing result.

Run State:

Active - The server will be put into service immediately after it is added. If there are servers in the farm in Standby, WebMux will activate a Standby server in its place if it goes out of service. When the original server comes back in service, it will stay Standby mode until manually setting its run state to Active again through the browser interface. This will give the system administrator time to fix the system or reboot the server once some software/ hardware update is completed.

Favorite Active - The server will be put into services immediately after it is added. If a Favorite
Active server failed, once it is operational, the WebMux will automatically put it back to the Active state.

Standby - The server will be put into STANDBY, or backup, mode after it is added. The WebMux will change a STANDBY server to ACTIVE when one or more ACTIVE servers fail. The weights will also have an effect on the number of standby servers that are activated. If the failed active server had a weight of 20 and there are two standby servers with the weight of 10, the WebMux will activate the two standby servers to make up the difference.

Last Resort Standby - The server will be put into STANDBY state. Unless all other servers are out of services, this server will not be switch in. This will allow the last server to show a different web page from others.

Delete Server

This link carries out an action that requires you to first select a server by clicking on the radio button for the server in the Main Status screen. Once you have selected a server radio button, you can click on this link to delete it from the farm. If you click on this link and you have not selected a server from the Main Status screen, you will see a notification instructing you to select a server. If you click on this link while in a different screen. You will see a notification and will be redirected back to the Main Status screen, where you can select a server you want to delete.

You can also detele a server by clicking on the the server IP link on the Main Status screen which will take you to the "Modify Server" screen. From there, you can delete the server using the "Delete" button.

Add MAP™

This option will only be available if the "Farm will use MAP" was set to YES and "HTTP compression" is set to NO when the farm was originally created.

Use the MAP feature to create additional IP address/port protocol combinations for the farm. When using a persistent scheduling method, the same client will also be sent to the same server no matter which port it accesses within that MAP.

Click on the radio button next to the farm you want to modify and click on the "add MAP" button on the left. Or click on the farm IP address and click on the "add addr/port" button in the modify farm screen.

You will see this screen:

Farm IP and Port

This displays the current farm you are modifying. These fields are set in the "Add Farm" screen. Once set, they are not changeable. If they must be changed, delete the farm and then add a new one.

IP Address

Add an IP address to the current farm configuration. The IP address can be the same as long as the port number does not duplicate any existing IP/port combinations.

Label

This is for your visual reference to be displayed on the main console for the farm entry. It can be any alphanumeric text.

Virtual Host Name

107

For web servers that are serving name based virtual hosts, this field will be important for the WebMux to perform a correct health check. The WebMux uses the data in this field as the host name for the HOST mime header in its HTTP health check requests to the servers. In some cases, name based virtual hosts have a default site that will still respond with a 400 OK even if a HOST MIME header is not specified in the request. In that case, leaving this field blank may not have a negative effect. However, in other cases, a request that does not have a specified HOST MIME header will end up receiving response from the server such as 503 Service Unavailable. In which case, the WebMux will mark the server dead. Therefore, it is important that you specifiy the correct host name of the site you are serving for the farm in order for the WebMux health check to reach the correct site and get a valid response from the server.

Port Number

Specify a port number that doesn't duplicate any existing IP/port combinations. A port number of "all" will enable all port ranges, but excluding any already existing ports associated with the specified IP address. Please see the note at the end of this section regarding the behaviors of the additional IP/port in conjunction with SSL termination.

Service

This allows you to specify the type of health checking you want the WebMux to perform for this MAP instance.

SSL Termination

You can enable the WebMux to do the SSL termination of this MAP instance.

SSL Port

The known secure port for the type of service you selected will be automatically filled in. You can manually change it if you are using a different port for that service.

Block Non-SSL Access to Farm

Prohibits non-SSL connection to this MAP instance.

Tag SSL-terminated HTTP Requests

This will enable the WebMux to add an "X-WebMux-SSL-termination: true" and "X-Forwarded-Proto: https" MIME headers in the decrypted HTTP request sent to the server.

✍ NOTE: If your farm is already SSL terminated and you create an additional IP/ port combination that is not SSL terminated using the main farm IP and specifying the same secure port (or "all"), the SSL termination by the WebMux will be bypassed and SSL passed directly to the server.

Modify MAP™

This link will require you to first select the radio button of a MAP entry from the Main Status screen. You can also get to this screen by clicking on IP:port link for the MAP entry.

Refer to the previeous "Add MAP" section for details about the fields.

Delete MAP™

This link carries out an action that requires you to first select a MAP by clicking on the radio button for the MAP in the Main Status screen. Once you have selected a MAP radio button, you can click on this link to delete it from the farm. If you click on this link and you have not selected a MAP from the Main Status screen, you will see a notification instructing you to select a MAP. If you click on this link while in a different screen. You will see a notification and will be redirected back to the Main Status screen, where you can select a MAP you want to delete.

You can also detele a MAP by clicking on the the MAP IP link on the Main Status screen which will take you to the "modify additional IP address/port" screen. From there, you can delete the MAP using the "Delete" button.

Add Gateway Farm

Gateway Farms allow you to load balance outgoing traffic between multiple external gateways. The gateways can be routers, proxy servers, firewalls or edge servers. The gateways will be balanced in a Weighted Round Robin Persistent fashion. By default, incoming traffic will be replied through the gateway it came from.

To create a gateway farm, click on the "Add Farm" button from the main status screen. In the "Add Farm" screen, click on the "Add Gateway Farm" button on the left:

IP Address:

The main WebMux IP address will automatically used if you leave this field blank. This address will be what the WebMux will use as its source IP when checking the health status of the gateway IP address.

Label:

You can enter a label for reference purposes. This is optional.

Click the "Submit" button to create the gateway farm. Your status screen will look something like this:

Your original default external gateway will be automatically added to the gateway farm. Click on the gateway farm IP on the grey line above the router IP to add more gateways to the gateway farm in the "Modify Farm" screen. You can also get to the "Modify Farm" screen by selecting the radio button for the farm IP on the grey line and clicking on the "Modify Farm" link on the menu pane.

Click on the "Add Gateway" button to add more gateways IPs to your gateway farm.

IP Address:

Enter the IP address of your gateway.

Label:

The label here is used only for reference purposes.

111

Weight:

This is for scheduling priority weight. Valid integer numbers are between 1 and 100.

Run State:

Active - The gateway will be put into service immediately after it is added. If there are gateways in the farm in Standby, the WebMux will activate a Standby gateway in its place if it goes out of service. When the original gateway comes back in service, it will stay Standby mode until manually setting its run state to Active again through the browser interface. This will give system administrators time to fix the system or reboot the gateway once some software/hardware update is completed.

Favorite Active - The gateway will be put into service immediately after it is added. If a Favorite Active gateway failed, once it is operational, the WebMux will automatically put it back to the Active state.

Standby - The gateway will be put into STANDBY, or backup, mode after it is added. The WebMux will change a STANDBY gateway to ACTIVE when one or more ACTIVE gateways fail.

Last Resort Standby - The gateway will be put into STANDBY state. Unless all other gateways are out of services, this gateway will not be switched in.

Back at the main status page of the web GUI, you will notice that the farm IP addresses are now shown in grey. Before creating a next hop gateway farm, the farm IPs were shown in blue with the ALIVE status, or red with the DEAD status. The farm IP status was an indication of the availability of the default external route of your WebMux. Now that you have created a gateway farm, the status of your external route is determined by the availability of any one of the gateways in your gateway farm. As with a single default gateway the type of health checking done on the router IPs is determined by the "front network verification" protocol setting in the Network Admin section of this User Manual.

If you click on the "nh" link under the "service" column, you will get to the "modify service timeout" page.

The setting in this page will determine how long or how short the WebMux will wait to be able to verify if the gateway IP is still valid or not. You can disable the checking altogether by setting the timeout value to 0 or you can set the "front network verification" protocol to "none" in the Network Admin section within this User Manual.

Modify Service

This link requires you to first select a farm using the radio button from the Main Status screen. Once you have selected the farm, you can click on this link to get to the "Modify Service Timeout" screen. You can also get to this screen by clicking on the the service name, under the service/ health column from the Main Status screen.

113

The "service timeout" is the amount of time the WebMux will wait to receive a reply from the servers during a health check probe. If a server does not reply within the given timeout, it is considered a failure. The WebMux will mark the server dead if it fails three consecutive health check probes.

Save

This link will be highlighted when you have made a configuration change that has not been saved. Clicking this link also forces a paired set of WebMux in HA configuration to synchronize your saved settings. A message will also be displayed and highlighted in the Main Status screen to let you know that an "unsaved in-memory configuration" has be made. You can click on that message or the save link in the menu to save your configurations.

Health

Timeouts

User may change the health check behavior by modify and enable custom health check, modifying the HTTP server respond code behavior, and change the health check TCP timeout value.

Modify Timeouts will allow you to change the health check timeout period (the amount of time the WebMux will wait for the server to reply to its health check probe).   Note that the WebMux will mark a server dead after three (3) consecutive failed health checks.

Service

This is the service type as selected in the farm configuration. Select the service you want to modify from the dropdown menu.

New Timeout

Enter the new timeout period for the selected service. This is a global setting. All farms using this service type will use the given timeout period.

Existing Timeout

This displays the existing timeout period for the selected service that is currently saved in memory.

114

Default Timeout

This displays the factory default timeout period for the selected service as a reference.

Frequency

The health check frequency is the interval in which the WebMux sends out health check probes. In some cases, you might find that the WebMux is probing your servers too often. You can modify the frequency period here. Note, however, that increasing the frequency too much will make the WebMux take longer to mark a server dead or alive.

Custom

Use this screen to modify your Custom Health Check settings

URL for Custom Service Check

Sometimes the WebMux built-in server health check is not enough for special needs. When an ASP/JSP server's output depends on the database server and the database server connection is down, one might want to reduce the incoming traffic to the server, suspend new traffic to the server, or totally redirect incoming traffic to a different server. To accomplish that, the WebMux allows a farm set up using "custom defined service." It will

115

then call the CGI's URL on the server defined in this field. This will involve a custom developed CGI code by your software developer on your server and place it on the path. Upon success the page should return HTTP response code 200 and a plain text page beginning with one of the allowed responses. The URL is truncated to 255 bytes (to be a string of at most 256 bytes with a terminating null). The response from the server must fit in 4k, including all non-display tag and headers etc. This custom CGI code must complete within 15 seconds or the server is considered dead. The custom defined service also allows for CGI code responses that allow the server to change its own weight and announce such change to a remote syslog daemon.

✍ Sample Custom CGI Code

The custom cgi-bin checking program may be written in Java, VB, C, or Perl, for example, or it may be a WB or shell script. Here is a sample script written for the Linux® shell -BASH- which sees if an SSH daemon is running as its check criterion.

```
#!/bin/bash

echo "Content-type: text/plain"

echo # blank line

if ps -C sshd &>/dev/null ; then

   echo "OK" # response from server goes here, see list below.

   echo "SSH service available"

else

   echo "NOT OK"

   echo "SSH daemon not running"

fi
```

The following is a list of valid CGI code responses:

OK   server/service is alive, no weight change

NOT OK   server/service is dead

OVERLOAD   set weight to 0, to quiesce (same as "WEIGHT=0")

QUIESCE   set weight to 0, to quiesce (same as "WEIGHT=0")

WEIGHT=n   set weight to integer n

WEIGHT-=n   subtract integer n from the weight

WEIGHT+=n   add integer n to the weight

The response must be in all capitals to be recognized. The changes in weight count as an unsaved configuration change. It is not automatically saved. Anything

116

not matching the above list will cause the WebMux to believe the server is not responding properly, thus the server will be taken out of service.

When the WebMux sends its health check, it will provide information in a query string that can be passed to your custom health check script. For example, the actual request from the WebMux will include the query string:

```
  /custom?
farm=<IP>:<PORT>&server=<IP>:<PORT>&alive=1&standby=0&favorite=0&la
stresort=0&weight=1
```

"farm" and "server" each consist of a dotted quad IP address followed by a colon and a port number (a server port of 0 means the port is the same as what is specified on the farm IP). "weight" is the numerical weight. The remaining items are either 0 for false or 1 for true.

You can have your script access the query string elements for further processing.

Also, the MIME header of the custom health check request will include the "Host:" and   "User-Agent:." The "Host:" MIME header will be the label you used for the farm (not the label you use for the server). The "User-Agent:" MIME header will show "WebMux health check for <farm IP>:<port>."

✍   The HTTP server will also have its own environment variables that you can utilize for your custom health check script. Please refer to your HTTP server manual and the manual for your scripting language for more information about environment variables.

If you select "Custom Defined + Generic TCP" service for a farm, the health checking process is a bit different. The health check script will pass for the following responses:

OK	server/service is alive, no weight change
OVERLOAD	set weight to 0, to quiesce (same as "WEIGHT=0")
QUIESCE	set weight to 0, to quiesce (same as "WEIGHT=0")
WEIGHT=n	set weight to integer n
WEIGHT-=n	subtract integer n from the weight
WEIGHT+=n	dd integer n to the weight

However, if the custom health check script returns an unknown response or if it is missing altogether, the WebMux will fall back to Generic TCP port checking. If the port for the custom check is different from the server port in the farm configuration, the
WebMux will do Generic TCP port check on the server port. As long as the port is open and responding to TCP connect, the server will be considered alive.

The conditions where the WebMux is consider the server dead will be if the custom health check script explicitly returns "NOT OK," or if the service port goes completely offline.

Ignore Contents of Custom Check Page

This option will disable checking the output of your custom health check script and merely checks if the script file exists on your server. If you have this setting set to yes, you can bypass creating any kind of scripting altogether and just make sure you have a valid file at the location specified in the URI for custom service check field.

HTTP

By default, HTTP servers return code 200 to indicate a successful result. Sometimes a different return code or groups of numbers are desirable.

To modify the HTTP respond code, click the "HTTP check" button on the left. You can modify the acceptable valid HTTP return codes in this screen:

You can list individual numbers separated by commas, or specify a range with a hyphen.

SECTION VII – GLOBAL SERVER LOAD BALANCING

WebMux Geographic Server Load Balancing (GSLB) can be thought of as a "smart DNS". Just like a DNS, the function of the WebMux GSLB is to resolve site names to IP addresses. However, the WebMux GSLB allows you to associate more that one IP address to a single name. Which IP address will be resolved to the client is determined by several possibilities:

1) All IPs are determined to be ALIVE through site health checks and the IP is chosen in a round robin fashion.
2) DEAD IP addresses are effectively taken out of service so that clients can reach the active site. Since IP addresses can be in different geographic locations, this will allow you to have a disaster recovery site that is far away from a site that may be experiencing natural disasters.
3) Each IP address can be associated with a specific geographical location. IP geolocation will determine where a client IP is coming from and the WebMux GSLB will return an IP address that is closest to the client's geographic location. This helps minimize lag between the site and the client.

Configure

The geographic server load balancing configuration screen has three main sections:
1) Data Centers
2) Rules
3) Zones

Each section has a "+", "scissor", "up triangle", and "down triangle" buttons. The "+" button adds another row underneath. The "scissor" button will delete that row. The "up triangle" moves the row before the row above it. The "down triangle" moves the row after the row below it.

Data Centers

This section is where you will put IP address to resolve names to. The mandatory fields to fill are the "name" and "ip addr list" fields. The "name" field can be anything to help designate a site, such as: DC1 for data center site 1. The "ip addr list" field can be a single IP address or multiple IP addresses separated by a space. The use of multiple IP addresses in this field will cause the WebMux GSLB to perform a round robin selection among the available IPs.

The priority field allows you to set a priority weight for the data center in case you want certain data centers to handle more traffic than others.

The latitude and longitude fields allow you to specify a geographic location by coordinates in case the location (or approximate location) is not in the list of locations in the Rules section.

Rules

This section is where you assign the geographic location of the data center. You must give a name to a rule. For example, area1. The location box is a list of locations sectioned by continent. Within each continent are specific countries. If you select a continent, you are effectively selecting all the countries within that continent. If you only want associate an area to specific countries, you can select multiple countries by holding down the ctrl key and clicking the mouse on your selection. Likewise, you can select multiple continents the same way. If you assigned latitude and longitude coordinates to a data center, you can select "(lat,long)" for the location.

The data centers field will be auto-populated with all the data center names you created in the section above. If you did not specify exact coordinates to a datacenter, you can select multiple data centers in a single geographic rule.

Zones

This section is where you input the domain name of a site just like in a regular DNS. The important fields are the domain name, rules, and check. The rules field will be auto-populated with the area names you created in the rules section above. Select the rule you want to associate with the domain name. Then, select the type of health check you want the WebMux to perfom for the site in the check field.

Empty Form

This button will clear all the settings in the screen.

Restore Config

If you have previously saved a configuration and cleared the screen with the Empty Form button, but have not yet clicked the Save Config button, you can retrieve the previous configuration with this button.

Save Config

This will commit your configuration to memory.

Stop DNS

This will stop the DNS daemon. DNS requests will not be answered.

Start DNS

If you stopped the DNS daemon, you can start it again with this button.

DNS Status

This button will show you if the DNS daemon is running or not.

Load Check

When the DNS daemon starts, it prints system messages. You can display those messages by clicking on this button. This is only helpful if something is not working and the system message might show what went wrong.

Clear Diagnostics

This will clear the messages displayed below the buttons.

Stats

This stats screen will show the current status of the different site IP address you have configured.

Database Update

IP geolocation is maintained by MaxMind. As IPs and geographic designations change from time to time, it is recommended that you update the database occasionally to maintain accurate IP geolocation.

AVANU®
WebMux
webmux.avanu.com

server LAN NAT
192.168.12.21/24
90:da:4e:03:de:b4
192.168.11.21/24
90:da:4e:03:de:b5

CPU: 0.00%
mem: 4.69%

Fri Feb 08 2019 7:50:30 AM
up since Fri Feb 08 2019 7:38:57 AM

☐ ethb0 1Gb
☐ ethf0 1Gb
☐ failover 1Gb
☐ admin 1Gb

Open All ▷
Close All ◁

► Main
► Farm Management
► Health
▼ GSLB
  Configure
  Stats
  Database Update
► Network
► Security
► Miscellaneous
► Help

GeoLite2-City update

Update the WebMux's GeoLite2-City data base from MaxMind.

UPDATE NOW

◄ ► ↻

SECTION VIII – SSL MANAGEMENT

SSL Keys

This screen is where you can manage your SSL keys and certificates that are used for SSL termination. This is also where you can specify cipher restrictions.

The WebMux supports SSL V2, SSL V3, and TLS V1 with RSA key length from 512, 1024, 2048, 4096, and 8192-bit. Each WebMux™ can hold 100 SSL key and certificate pairs. The key and certificate pair is activated by selecting in in the "add farm" or "modify farm" screens. The first line of the private key is a comment line. This will be displayed in the description on the main SSL termination management screen and in the key/certificate selection in the "add farm" or "modify farm" screens. If there is no comment line in the key, it will be blank. If there is no key, it will display "(key and certificate unset)."

Key length can be from 512 to 8192. RSA key length 1024 is also called 128 bit strong encryption.

At the bottom of the screen you will see the option to choose encryption protocols allowed. This will enable you to restrict SSL connections that do not follow the minimum protocol. If there are already active farms using SSL Termination, then changing this setting will require you to reboot the WebMux to activate changes. If you decide not to reboot, existing farms will run under the previous criteria and new farms will follow the new criteria. Rebooting the WebMux will ensure that ALL the farms with SSL Termination will adhere to the new protocol requirement.

Click a key number to go into the key management page. In this page, use the drop down menus to generate keys or copy and paste your existing keys and signed certificates:

You should back up your private key and save in a secure place. Each private key and public key pair must match to be able to work properly.

Generating a CSR

If you plan to generate new keys, click on the drop down box above the private key window to select the "use newly generated" item with the desired key length, and then click on the "Submit" button. This process is also known as "generating a CSR" or "generating a Certificate Signing Request."   This is the process where you generate a key pair and send the public key to the CA for "signing." Once your public key is signed and pasted into the key management screen, browsers over the Internet will accept it without complaint during the lifetime assigned to the key. You can visit www.thawte.com or www.verisign.com for more information

After submitting the selection, you will see this next screen:

Enter all the necessary information. Click on the "Confirm" button to complete the key generation. A certificate request will be generated. **Be sure to copy and save this before you continue.**

When you are done saving the certificate request, you can click on the "Confirm" button. You will be taken back to the dialog boxes that will display the newly created private key. You should make a backup copy of that as well.

Submit the certificate request to the CA of your choice to sign. Once they send you back the signed certificate, you will need to paste that into the certificate dialog box, select "use new certificate pasted in" and click on the "Confirm" button to save it into the WebMux.

You will receive two certificates. One will be the site certificate. The other might be called the CA bundle. Please paste your site certificate first, followed the CA bundle. Keep the BEGIN and END headers and footers for each certificate intact as you paste one after the other.

If you have existing signed keys from a Windows® IIS server or a Linux® server, you can transfer them into the WebMux and continue using them until they expire. You should be able to directly transfer your existing key and certificate from your Linux® server. For Windows® IIS keys and certificates, you will need to convert them to PEM format.

Please refer to our support site for instructions:

   http://www.avanu.com/webmux_ssl_certificate

You can get OpenSSL for Windows® at:

   http://www.slproweb.com/products/Win32OpenSSL.html

Contact the AVANU technical support department at techsupport@avanu.com for further assistance if problems should arise or for help with executing this process.

   ✐ The CA certificate field is only for Client Side SSL authentication. It is not for the intermediate certificate.

Importing Your Existing Private Key and Certificate

If you already have an existing key and certificate in PEM format, importing them into the WebMux is as easy as cutting and pasting the text into the proper fields.

Select an unused key number from the SSL termination management page, for example:

Open your key PEM file in a text editor and copy the text starting with `-----BEGIN RSA PRIVATE KEY-----` all the way to `-----END RSA PRIVATE KEY-----` (be sure to include BOTH the header and footer). Paste the text into the private key text box. From the dropdown selection to the right of the text box, select "use new private key pasted in".

Next, open your certificate PEM fil in a text editor. Copy the text starting with `-----BEGIN CERTIFICATE-----` all the way to `-----END CERTIFICATE-----`. Paste the text into the certificate text box and select "use new certificate pasted in".

If you were given an intermediate certificate, you will need to chain that into the certificate text box as well. Paste your intermediate certificate, including its header and footer, after the `-----END CERTIFICATE-----` footer of the previous certificate.

DO NOT paste any text into the CA certificate text box. The CA certificate field is for a completely different function known as Client Side SSL Authentication. For normal farm SSL Termination, you do not need this.

Submit the page to complete the import. You can now select the corresponding key/certificate slot for your farm configuration.

SECTION IX - HOW TO ADD A LOOPBACK ADAPTER

For Direct Server Return Mode, a loopback adapter (Windows) or setting of similar function (*nix OS) is required.

Installing the Microsoft® Loopback Adapter (pre-Windows 8/Server 2012)

Click Add Hardware -> Add a new device -> No, I want to select the hardware from a list, and select Microsoft® Loopback Adapter from the list and click OK.

At the Microsoft® Loopback Adapter Card Setup screen hit OK to the default of 802.3

You should be prompted for the path to the NT setup files. Click Continue once the path is correct.

Click Close. Reboot maybe necessary. Go to step below for Configuring the Microsoft® Loopback Adapter.

Configuring the Microsoft® Loopback Adapter (pre-Windows 8/Server 2012)

If not there already, go to Start > Settings > Control Panel > Network > Protocols tab

Select TCP/IP and click the Properties button

You should be at the Microsoft® TCP/IP Properties dialog box. Be sure the Microsoft® Loopback Adapter is the Adapter selected. Enter your farm IP address for IP address (The subnet mask should match your servers, change it if not). Make sure not to enter Default Gateway or DNS for this loopback adapter.

Click Apply, then OK, then "Yes" when prompted to restart the computer

For Microsoft® Windows® 2003 Server, make sure the metric is the highest number in the routing table, stop here.

✍ The highest number meaning 1000 is higher than 100. You need to make sure that the Loopback Adapter has the highest number in the routing table. Giving a lower number means a higher priority. You want the Loopback Adapter to have the lowest route priority, therefore a higher number value.

If you are noticing that the Loopback Adapter is picking up or creating NetBIOS chatter, you will need to turn off anything related to Client for Microsoft® Networks, File and Printer Sharing for Microsoft® Networks, and WINS. Right click on the Loopback Adapter icon, and click on Properties. In the Networking tab, unselect "Client for Microsoft® Networks" and "File and Printer Sharing for Microsoft® Networks." Next click on "Internet Protocol Version 4 (TCP/IP)" then click the Properties button. In the General tab, click the Advanced button. Click on the WINS tab and unselect Enable LMHOSTS lookup and select Disable NetBIOS over TCP/IP. Click OK in the various windows to make all the changes permanent.

Installing the Microsoft® Loopback Adapter (Windows 8/Server 2012 and newer)

Open Device Manger.

Highlight the root device (the PC name). Under the "Action" menu, select "Add legacy hardware".
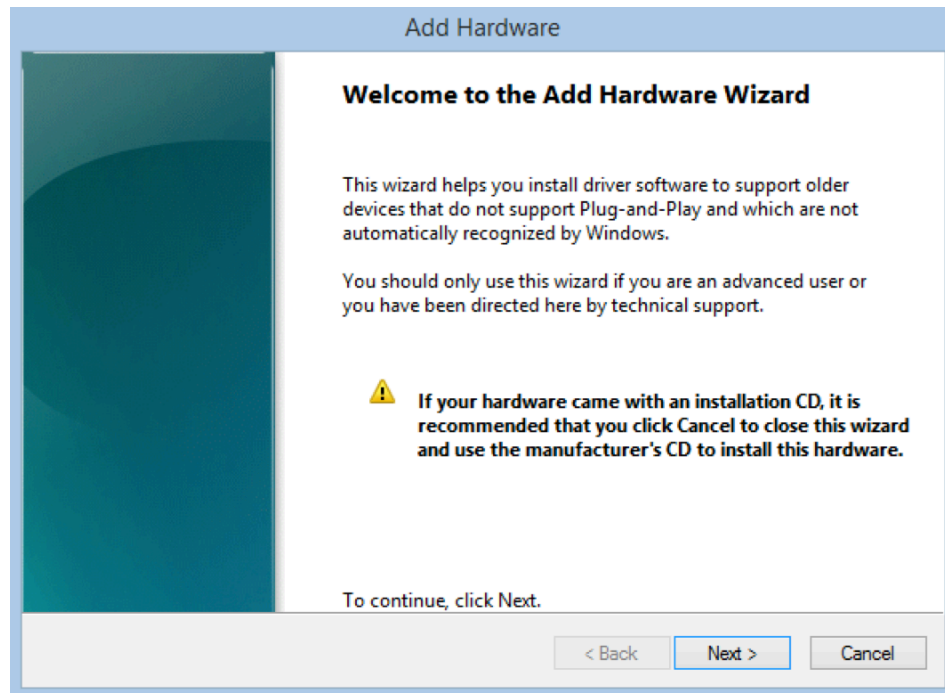
On the next screen, select "Install the hardware that I manually select from a list (Advanced):
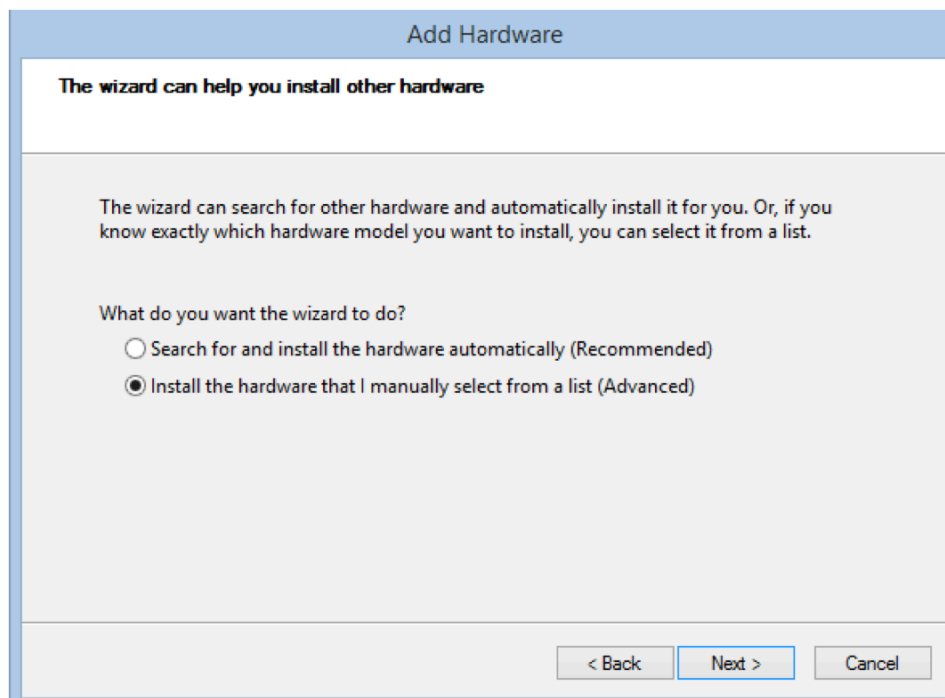
Then, select "Network adapters" and click the Next button:
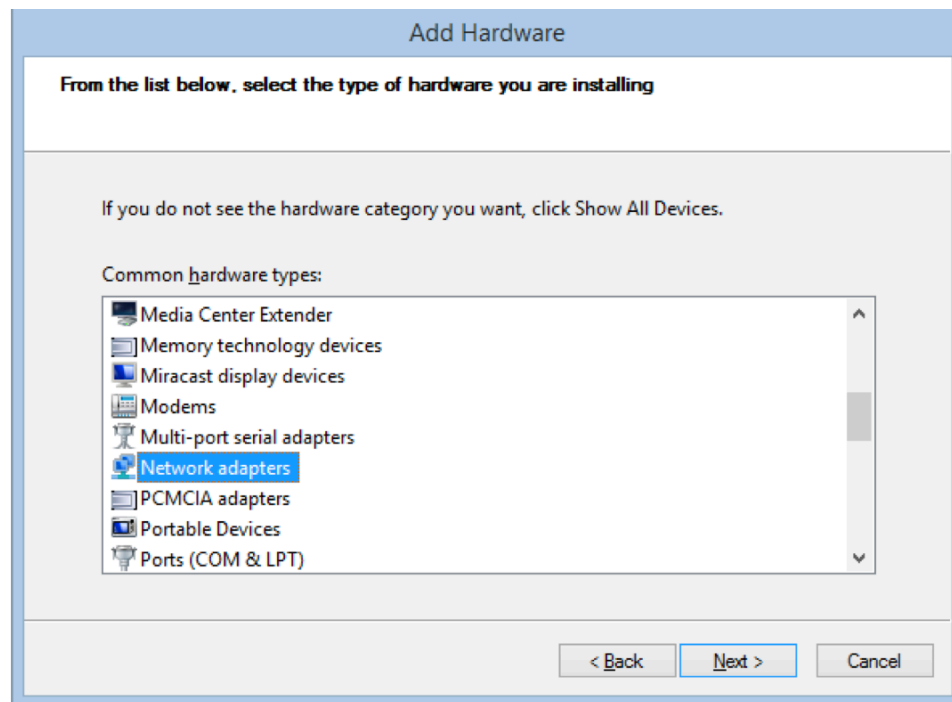
On the next screen, select "Microsoft" on the left pane and "Microsoft KM-TEST Loopback Adapter" on the right pane:
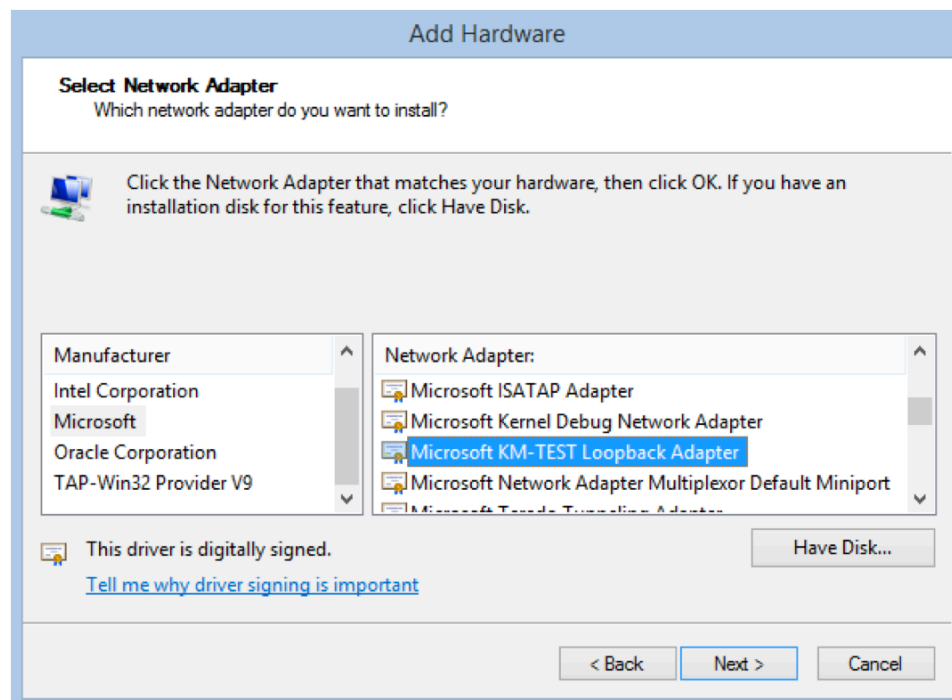
Proceed throught the installation process:
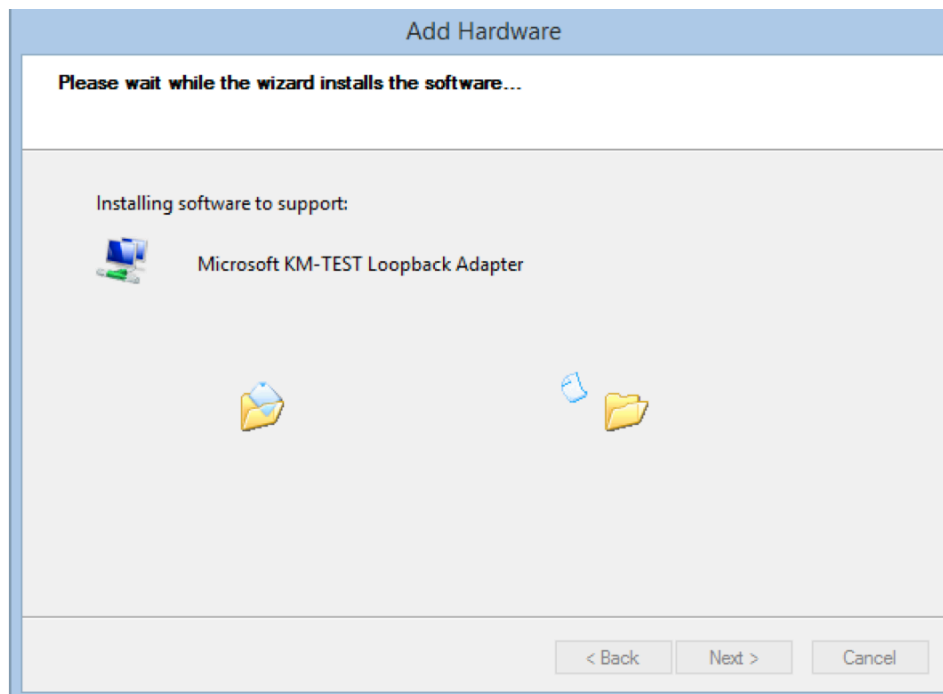
Click the "Finish" button when complete:
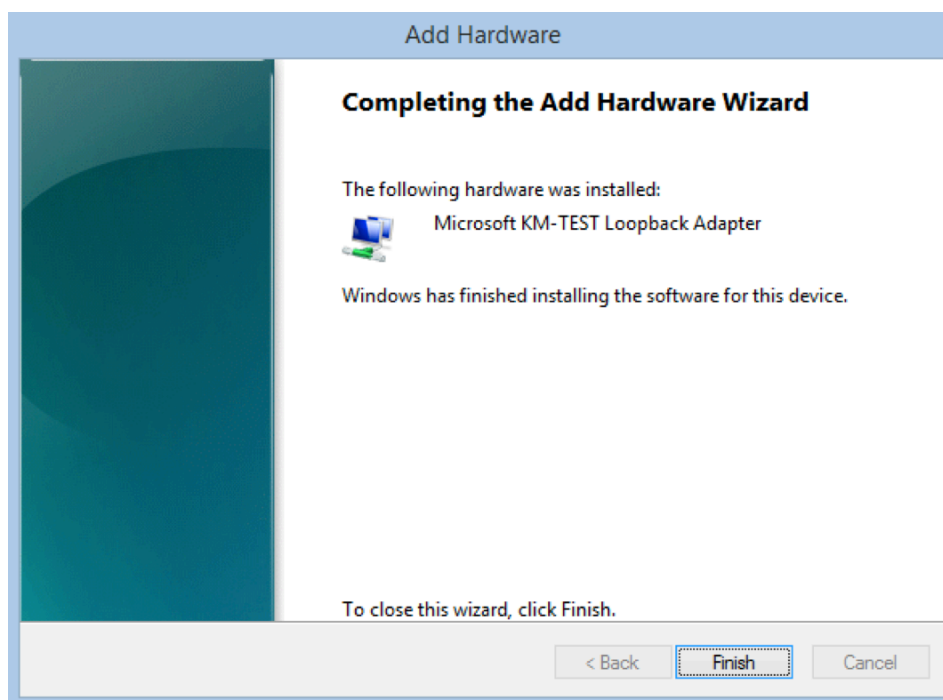
Configuring the Microsoft® Loopback Adapter (Windows 8/Server 2012 and newer)

Open the "Network and Sharing Center" from the Control Panel.

Find the "Change adapter settings" link on the left side of the window.

In the "Network Connections" window, right click on the Virtual Loopback Adapter (Microsoft KM-TEST Loopback Adapter) and select "Properties". In the next window, highlight "Internet Protocol Version 4 (TCP/IPv4)" and click on the "Properties" button.
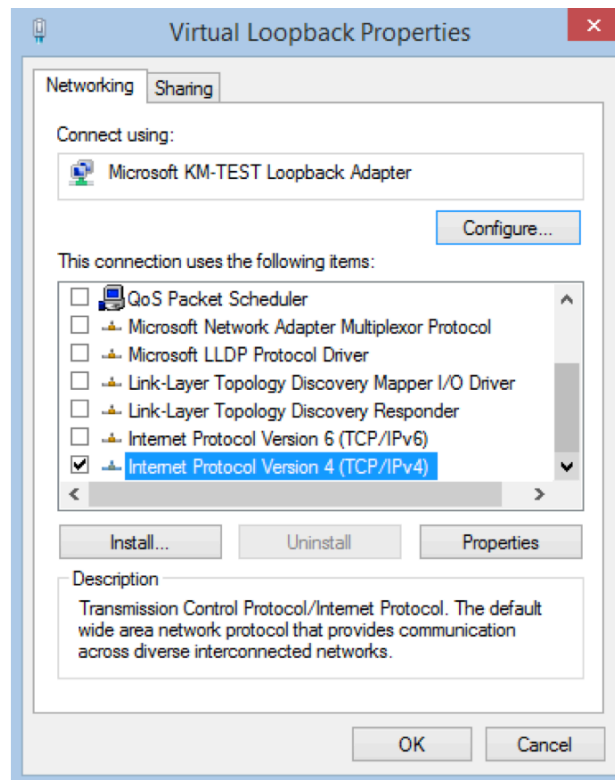
In the "Internet Protocol Version 4 (TCP/IPv4) Properties" screen, enter the FARM IP that the server belongs to and the subnet mask. Do not put anything in the gateway or DNS fields.
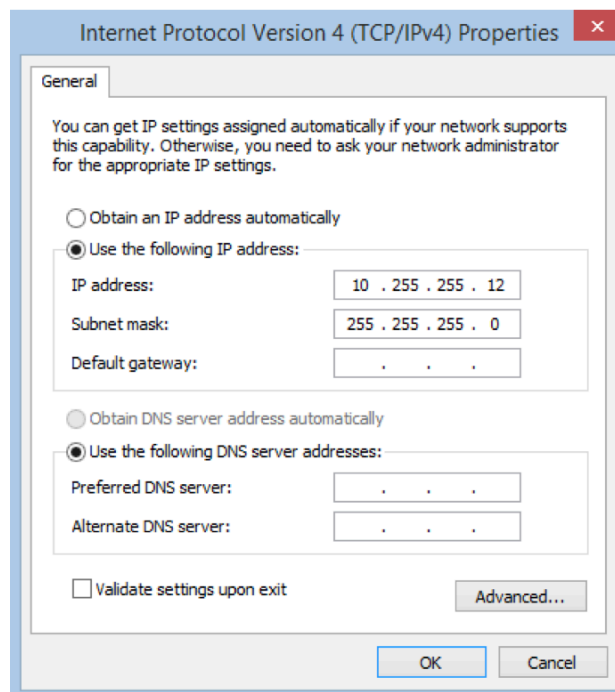
Click on the "Advanced" button, then open the "WINS" tab. Make sure "Enable LMHOSTS lookup" is not selected and "Disable NetBIOS over TCP/IP" is selected.
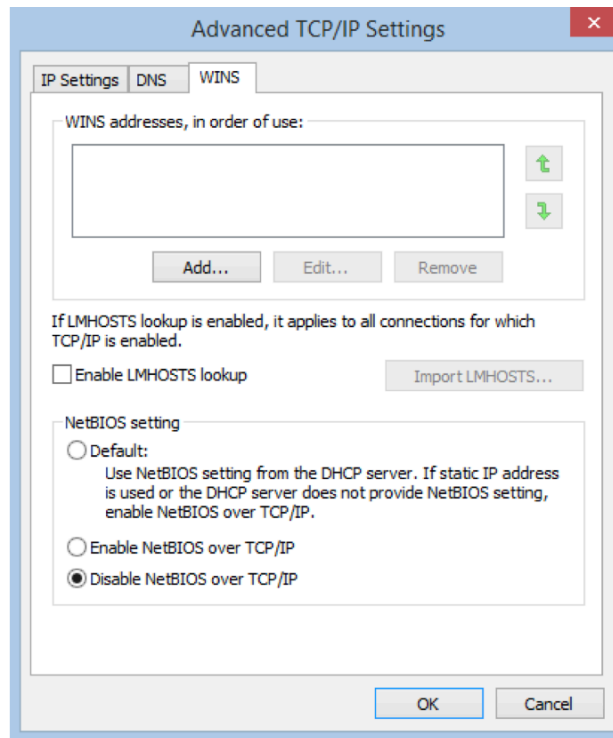
Click the OK buttons to submit the changes.

Finally, set the Weakhost Settings to complete the installation.

Weakhost Settings for Windows Server 2008 and Newer

Beginning with Windows® Server 2008, the default networking has moved to the "strong host" model as outlined in RFC 1122.

You need to use the following command line:

netsh interface ipv4 set interface "net" weakhostreceive=enabled

netsh interface ipv4 set interface "loopback" weakhostreceive=enabled

netsh interface ipv4 set interface "loopback" weakhostsend=enabled

Refer to the Windows "Network Connections" settings to get the names of the interfaces. You can rename them for better identification instead of just "Local Area Connection", etc.

To verify the status of your interfaces:

    netsh interface ipv4 show interfaces level=verbose

For Linux®, SUSE® Enterprise Linux®, Hewlett Packard® HP/UX®, FreeBSD®, Oracle® Solaris®, and Apple® Servers perform the following for:

Linux® 2.4/2.6 Systems:

Log in as root, and add this command to the bootup script:

    iptables -t nat -A PREROUTING -d <farm_ip> -j DNAT --to-dest <server_ip>

For IP-based virtual hosting with multiple IPs, repeat the command for each farm IP on all   the servers. Don't forget to add the proper farm IP to each virtual host configuration. With IPv6 addresses, add the IPv6 address of the FARM to "lo" adaptor. Also, be sure that the routing table has an IPv6 entry for the network and a default gateway entry for the real interface of the server. You can check by issuing the "route —inet6" command. Reference the IPv6 section of this User Manual for additional information.

If your server application requires that you have an actual IP address on an interface to bind to, then you can use this method (requires arptables):

    ip addr add <farm_ip> eth0   # add farm IP address on "eth0"

    arptables -t filter -A IN -d <farm_ip> -j DROP # keep it from responding to ARP

SUSE® Enterprise Linux® 9:

You can use YAST to set up a Virtual Interface and add the farm IP.

Log in as root, and add this command to the bootup script:

iptables -t nat -A PREROUTING -d <farm_ip> -j DNAT —to-dest <server_ip>

134

Hewlett Packard® HP/UX® 11.00 and 11i:

Please make sure PHNE_26771 and related patches applied first. Login as root, and   add this command to the bootup script:

ifconfig lo0:1 farm_ip_address up

FreeBSD®:

ifconfig l®o0 inet farm_ip_address netmask 255.255.255.255 alias

Oracle® Solaris®:

ifconfig lo0:1 FARM_IP_ADDR

ifconfig lo0:1 FARM_IP_ADDR

FARM_IP_ADDR ifconfig lo0:1 netmask

255.255.255.255 ifconfig lo0:1 up

Apple® Servers:

ifconfig lo0 inet farm_ip_addr netmask 255.255.255.255 alias route

delete gateway ip farm_ip_addr netmask

Where lo0 is the loopback adapter.

SECTION X – HTTP TO HTTPS REDIRECT

In some cases, you may need the WebMux to redirect a client coming in via HTTP to HTTPS without having to create rewrite rules on the real servers.   The way this feature works is you first have one farm (the "redirect" farm) that accepts the incoming HTTP connection. The "redirect" farm replies to the client with a "301 Permanent Redirect" response pointing to the rewritten HTTPS URL. The rewritten URL will include also append a suffix and prefix, if any are specified.

Creating an HTTP to HTTPS Redirect "Farm"

Creating an HTTP to HTTPS redirect "farm" is the same as creating any other farm entry. The most important thing is to select "HTTP to HTTPS redirect" as the scheduling method.

Label

This is for your visual reference to be displayed on the main console for the farm entry. It can be any alphanumeric text.

IP Address

This is the IP address for the incoming HTTP connection. Keep in mind that when HTTP to HTTPS redirect occurs, the original domain name is not changed. Therefore, the domain will be resolved to the same IP, but going to HTTPS instead. Therefore, this IP address must also be used for when creating the separate HTTPS farm that will contain the real servers.

Scheduling Method

You will be selecting "HTTP to HTTPS redirect".

URI Redirect Prefix

The prefix will be appended to the front of the original domain name. For example, if you specificy the prefix as "hostname." and the original URI is http://domainname.com, the rewritten URI will be https://hostname.domainname.com.

URI Redirect Suffix

The suffix will be append to the end of the URI. For example, if you specify the suffix as "location" and the original URI is http://domainname.com, the rewritten URI will be https://domainname.com/location

Completing the HTTP to HTTPS Redirect Configuration

After you have created this HTTP to HTTPS redirect "farm", it is important that you remember to create the HTTPS farm that will be accepting the HTTPS connection. Because the domain name will be resolving to the same IP address, your HTTPS farm should be the same IP as what you have used for the HTTP to HTTPS redirect farm.

For example if the HTTP to HTTPS redirect farm is listening on 192.168.12.200 port 80, you will need to create an HTTPS farm that is listening on 192.168.12.200 port 443.

You should then have two farms working in conjuction with each other:

137

SECTION XI – SAMPLE CONFIGURATIONS AND WORKSHEETS

Initial Configuration Worksheets

Configuration Before WebMux Installation

EQUIPMENT	IP ADDRESS
Internet Router (or Firewall) Address	
Webserver(s) Default Gateway	
Web Site IP Addresses	

Configuration After WebMux Installation

QUESTION	ENTRY	
	PRIMARY	SECONDARY
Host Name		
Domain Name		
NAT, Transparent, Single Network, or Direct Server Return		
Router LAN Information (NAT ONLY)		
Router LAN WebMux Proxy IP Address		
Router LAN Network IP Address Mask		
Router LAN VLAN ID (optional)		
Server LAN Information (NAT and OOP)		
Server LAN WebMux IP Address		
Server LAN Gateway IP Address (optional for OOP)		
Server LAN Network IP Address Mask		
Server LAN VLAN ID (optional)		
Bridge Settings (For Transparent Mode Only)		
WebMux Bridge IP Address		
WebMux Bridge IP Network Mask		
Router LAN VLAN ID (optional)		
Server LAN VLAN ID (optional)		

Administration Setup Information		
External Gateway Address		
Remake /home/WebMux/conf/passwd	Y/N	Y/N
Administration HTTP Port Number		
Secure Administration HTTP Port #		
Is this WebMux primary	Y	N
WebMux running solo without backup	Y/N	
Reboot?	Y/N	Y/N

Sample Configuration Worksheets

Standalone WebMux NAT Mode

Configuration Before WebMux Installation

EQUIPMENT	IP ADDRESS
Internet Router (or Firewall) Address	205.133.156.1
Webserver(s) Default Gateway	205.133.156.1
Web Site IP Addresses	205.133.156.200

Configuration After WebMux Installation

QUESTION	ENTRY
Host Name	webmux
Domain Name	avanu.com
NAT, Transparent, Single Network, or Direct Server Return	NAT
Router LAN Information	
Router LAN WebMux Proxy IP Address	205.133.156.200
Router LAN Network IP Address Mask	255.255.255.0
Router LAN VLAN ID (optional)	101
Server LAN Information	
Server LAN WebMux IP Address	192.168.199.251
Server LAN Gateway IP Address	192.168.199.1

Server LAN Network IP Address Mask	255.255.255.0
Server LAN VLAN ID (optional)	102
Administration Setup Information	
External Gateway IP address	205.133.156.1
Remake /home/WebMux/conf/passwd	Y
Administration HTTP Port Number	24
Secure Administration HTTPS Port Number	35
Is this WebMux primary	Y
WebMux running solo without backup	Y
Reboot?	Y

You will also need to change the Web server IP address to 192.168.199.10, and its default gateway to 192.168.199.1. Add a farm for 205.133.156.200 and add a server to the farm at 192.168.199.10. You can then add more servers at 192.168.199.20 and 192.168.199.30. You can also add additional farm at 205.133.156.210, and add above three servers to the 2nd farm.

Standalone WebMux Transparent Mode

Configuration Before WebMux Installation

EQUIPMENT	IP ADDRESS
Internet Router (or Firewall) Address	205.133.156.1
Webserver(s) Default Gateway	205.133.156.1
Web Site IP Addresses	205.133.156.200

Configuration After WebMux Installation

QUESTION	ENTRY
Host Name	webmux
Domain Name	avanu.com
NAT, Transparent, Single Network or Direct Server Return	Transparent
Bridge Information	
Bridge IP Address	205.133.156.210
Bridge IP Network Mask	255.255.255.0
WebMux farm IP Address	205.133.156.200
(front) Router LAN VLAN ID (optional)	101
(back) Server LAN VLAN ID (optional)	102
Administration Setup Information	
External Gateway IP address	205.133.156.1
Remake /home/WebMux/conf/passwd	Y
Administration HTTP Port Number	24
Secure Administration HTTPS Port Number	35
Is this WebMux primary	Y
WebMux running solo without backup	Y
Reboot?	Y

Direct Server Return Installation of WebMux

Configuration Before WebMux Installation

EQUIPMENT	IP ADDRESS
Internet Router (or Firewall) Address	10.1.1.1
Webserver(s) Default Gateway	10.1.1.1
Web Site IP Addresses	10.1.1.200/255.255.0.0

Configuration After WebMux Installation

QUESTION	ENTRY
Host Name	webmux
Domain Name	avanu.com
NAT, Transparent, Single Network or Direct Server Return	Direct Server Return
WebMux Server LAN Information	
Server LAN WebMux IP Address	10.1.2.254 (any)
Server LAN WebMux IP Address Mask	255.255.0.0
Server LAN WebMux farm IP Address	10.1.1.200
Server LAN VLAN ID (optional)	102
Server LAN gateway IP address Necessary for WebMux SSL termination and for Layer 7 load balancing. Each server's default gateway needs to be set to this IP	10.1.1.253
Server Configuration	
Server IP address	No Change
Server NetMask	No Change
Server Default Gateway	No Change
Server Default Gateway (If using WebMux for SSL Termination Load Balancing)	10.1.1.253
Server add loopback adapter	10.1.1.200
Route Deletion	10.1.1.200

Administration Setup Information	
WebMux External Gateway IP address	10.1.1.1
Remake /home/WebMux/conf/passwd	Y
Administration HTTP Port Number	24
Secure Administration HTTPS Port Number	35
Is this WebMux primary	Y
WebMux running solo without backup	Y
Reboot?	Y

There is no change to each server's IP address, netmask and gateway address (except if using the WebMux for SSL termination. See next paragraph). You will need to add a loopback adapter to each server, and assign the farm address to the loopback adapter. For Microsoft® Windows®, it always adds a route for the loopback adapter, which will need to be removed. In the virtual farm, add each server using its real IP address.

For SSL termination, you must set server LAN gateway IP address and set the servers' default gateway to that IP.

If using multiple VLAN configuration, please note the VLAN IP address cannot be used for FARM address. FARM address must be an address within that VLAN and other than the VLAN IP address.

Redundant WebMux Installation

Configuration Before WebMux Installation

EQUIPMENT	IP ADDRESS
Internet Router (or Firewall) Address	205.133.156.1
Webserver(s) Default Gateway	205.133.156.1
Web Site IP Addresses	205.133.156.200

Configuration After WebMux Installation

QUESTION	ENTRY	
	Primary	**Secondary**
Host Name	webmux1	webmux2
Domain Name	avanu.com	avanu.com
NAT, Transparent, Single Network, or Direct Server Return	NAT	NAT

Router LAN Information		
Router LAN WebMux Proxy IP Address	205.133.156.200	205.133.156.200
Router LAN Network IP Address Mask	255.255.255.0	255.255.255.0
Router LAN VLAN ID (optional)	101	101
Server LAN Information		
Server LAN WebMux IP Address	10.1.1.10	10.1.1.20
Server LAN Gateway IP Address	10.1.1.1.1	
Server LAN Network IP Address Mask	255.0.0.0	255.0.0.0
Server LAN Network IP Address	10.0.0.0	10.0.0.0
Server LAN Network Broadcast Address	10.255.255.255	10.255.255.255
Server LAN VLAN ID (optional)	102	102
Administration Setup Information		
External gateway IP address	205.133.156.1	205.133.156.1
Remake /home/WebMux/conf/passwd	Y	Y
Administration HTTP Port Number	24	24
Secure Administration HTTPS Port	35	35
Is this WebMux primary	Y	N
WebMux running solo without backup	N	
Reboot?	Y	Y

SECTION XII – FREQUENTLY ASKED QUESTIONS – FAQs

I can't log in with my browser. It always says you are not logged in.

To use your browser to manage the WebMux, it must be set to accept all cookies. Because the cookie is set to expire in 8 hours, you also need to make sure your system clock set correctly using GMT.

The message is an indication that your system clock is off. Please refer to the "Miscellaneous Settings" "Set Clock" section on how to set the system clock of the WebMux.

I can't login with my browser because the WebMux does not respond.

Your IP address is not on the allowed host list, or the wrong IP addresses were entered by accident.

Use the LCD panel setup to clear that list.

If I have multiple servers assigned as STANDBY, how does the WebMux choose which server to use if an ACTIVE server goes down?

The WebMux checks the standby servers in order and activates each one until their total weight meets or exceeds the server that is unavailable

Will a server with weight 0 act as a STANDBY?

No. A weight of 0 indicates that the server will not accept any new connections. The state is considered neither ACTIVE nor STANDBY. This is to quiet the new connections for the server so that it can be taken out of service. Setting a server to STANBY will immediately disconnect current connections.

Is the Server LAN and the Router or Front LAN required to be on separate IP subnets?

It is required that the server LAN and the router LAN be separate IP subnets.

What notification services are compatible with the WebMux?

Any SMTP server can be used for sending email notifications.

If I'm running a UNIX®-based FTP, such as wuftp, how can I get the ftp server in the farm to resolve the WebMux IP addresses?

The IP addresses typically will not be able to be resolved since the servers in the farm are typically using non-routable or private network addresses. In order for wuftp to resolve the IP addresses and stop complaining, place the non-routable IP address entries in the /etc/hosts file on those servers.

How come my servers in the farm are showing in red color from time to time, even though the servers are okay?

Your servers are trying to resolve the WebMux unit's IP address to a name so it could log them into log file. This may delay the server's ability to reply to the WebMux health check probes. To avoid

this problem, set the servers not resolve the IP addresses. You can also try adding all the IP address to the /etc/hosts file on your servers. For example,

www.mydomain.com	1.2.3.4	// use your real IP address
Webmuxgw	192.168.199.1	// server lan gateway

How many browsers can simultaneously access the WebMux management console?

The limit is 4.

I have added a new farm/server, but the changes are not showing up on the STATUS screen.

The web browser cache may be the cause of this. If the new configuration does not appear after clicking on Reload or Refresh, then clear the cache or temporary files on the browser.

Will my web server be able to communicate to a credit card validation service, like CyberCash?

Yes. For any communication initiated from the internal or private network, the WebMux will substitute the IP address of its router LAN interface for the IP address of the host initiating the conversation. For any service that requires a specific IP address to allow communication into their network, the IP address of the router LAN interface must be the one provided. We have had CyberCash engineers work with us to test this.

Can I use the WebMux as a proxy server for other hosts in my internal network?

Yes. The function that allows the web servers to talk to services such as the credit card validation allows the WebMux to function as a proxy server for any host in the internal network. The WebMux will translate all internal addresses to the IP address of the "first farm" defined. This is the farm that is created when answering the question: WebMux Router LAN IP address:.

Configuring other computers using the WebMux unit's proxy function is easy—just point the gateway

IP address to the WebMux backend IP address.

Do I need to have a firewall in front of the WebMux?

In most cases, no. In NAT mode, the WebMux blocks all the incoming traffic from router LAN to your internal network. Unless there is a farm defined for a port number, the outside traffic will not be able to reach to any server or computers behind the WebMux. The WebMux does not have the management functionality for restricting which IP address or services an internal host can reach to the outside. If such restriction is desirable, then additional firewall is needed. A firewall is recommended if running the WebMux in Transparent Mode or Direct Server Return.

What can I do if the service that I want to load balance is not in the list?

The WebMux already supports many different services. If your service is not in the list, you could use generic TCP and/or UDP to set your farm. If this is not ideal, you may contact us for developing a special service aware module for you for a modest fee in most cases.

Why didn't the secondary WebMux take over when I powered down Primary WebMux?

Possible reasons: 1) The two WebMux units are not running on the same version of firmware, or 2) The secondary WebMux not only monitors the primary WebMux, but a few other things as well. Before it takes over, it makes sure it can reach to the router LAN gateway, as well as at least one server defined in any farm. If the secondary WebMux cannot reach to the front router LAN gateway, or if it cannot see any server in any farm, then it will consider that the primary was disconnected or powered down purposely by operator.

Why can't VLAN IP address be used as farm IP in Direct Server Return WebMux?

WebMux uses VLAN IP to forward the packets to the servers in Direct Server Return mode. If that VLAN IP address is also the farm address, then the loopback adapter on the server will have the same IP address. During a health check from WebMux, a server will not be able to send the reply back to WebMux, since the server finds the same IP address on itself.

SECTION XIII – LIMITED PRODUCT WARRANTY AND SUPPORT

About the Performance Guarantee

The "Performance Guarantee" is an expression of the confidence we have in our products and services.

AVANU Limited Product Warranty and Support

WebMux comes with the following coverage *:

- Two (2) year limited product warranty (Parts and Labor; Customer is responsible for freight and carrier insurance coverage and for any damage or loss during transit time until received by AVANU's Service Center)
- One (1) year product firmware updates (Monday to Friday except US Holidays; 8:00 am to 5:00 pm Pacific time)
- One (1) year product technical support by telephone and email (Monday to Friday except US Holidays; 8:00 am to 5:00 pm Pacific time)
- * 90-days product configuration support

AVANU has a thirty-day (30) money back guarantee

- Money back guarantee claims must be processed through the original point of purchase

- Restocking fees may apply

- Customer or point of purchase must contact AVANU to disclose reason for return prior to thirty-days (30) of receiving product

- Upon approval, a RMA number will be issued by AVANU's Customer Service for the return and must be visible on the outside shipping container

- Customer is responsible for freight and carrier insurance coverage and for any damage or loss during transit time until received by AVANU's Service Center.

- Product must be received in a brand new condition. Customer will be responsible for any other costs incurred due to product and/or packaging damage (internal components and external including scratches or dents) or missing components. Any damage or missing components will be charged to customer according to current repair or replacement costs along with a 15% restocking and handling fee.

- Delinquent returns received beyond ten-business days (10) of the thirty-days (30) period will not be honored for return.

- Product purchase refunds (less applicable freight charges, restocking and handling fee, repair or replacement cost) are issued to original AVANU point of purchase in the same payment method as original purchase. AVANU has the option to refund with a company check or credit memo after product inspection and diagnostic testing.

Extended Warranty and Support Programs (Optional purchase)

Standard Annual Service Program for continued or extended coverage. Renewals must be within 1-year of support expiration period coverage to prevent additional lapsed period coverage costs; lapsed periods beyond 2-years is not eligible for renewal.

- Product firmware updates (Monday to Friday except US Holidays; 8:00 am to 5:00 pm Pacific time)

- Product technical support (Monday to Friday except US Holidays; 8:00 am to 5:00 pm Pacific time)

Gold Annual Service Program for continued or extended coverage. Renewals must be before the original warranty expiration period coverage to prevent additional recertification cost; any renewal post-expiration will be backdated to begin coverage from the original expiration date; any lapsed periods beyond the 1-year of expiration is not eligible for renewal. Contact your representative or reseller for current recertification costs.

- Limited Product Warranty (Parts and Labor; Customer is responsible for freight and carrier insurance coverage and for any damage or loss during transit time until received by AVANU's Service Center)

- Product firmware updates (Monday to Friday except US Holidays; 8:00 am to 5:00 pm Pacific time)

- Product technical support (Monday to Friday except US Holidays; 8:00 am to 5:00 pm Pacific time

Premium Annual Service Program (First year must be purchased with the WebMux product or within the first 30-days of purchase. AVANU has the right to request a proof of purchase document. Renewals must be before the expiration period coverage to prevent additional recertification cost; any renewal post-expiration will be backdated to begin coverage from the original expiration date; any lapsed periods beyond the 1-year of expiration is not eligible for renewal. Contact your representative or reseller for current recertification costs.

- 24x7 product technical support

- Product firmware updates

- Limited Product Warranty (Parts and Labor; Customer is responsible for freight and carrier insurance coverage and for any damage or loss during transit time until received by AVANU's Service Center)

- Advanced replacement option available

Recertification

Any WebMux received for recertification must be in working condition upon receipt. A complete diagnostic test will be conducted to determine the WebMux condition and eligibility for renewal coverage under one of AVANU's Extended Warranty and Support Programs. The diagnostic testing includes a complete hardware test, small part replacements if required (such as battery, memory); major parts are not covered (such as power supply, motherboard). Customer is responsible for freight and carrier insurance coverage and for any damage or loss during transit time until received by AVANU's Service Center).

About the Limited Warranty Disclaimer

AVANU warrants to the end-user customer that the WebMux products will be free from defects in material or workmanship under normal use during the Limited Warranty period. AVANU shall have no obligation to repair or replace until the customer returns the defective WebMux unit to AVANU's Service Center. AVANU will, at its sole discretion, repair or replace any component or hardware product that manifests a defect in materials or workmanship during the Limited Warranty period.

All component parts or hardware products removed under this Limited Warranty become the property of AVANU. In the unlikely event that the WebMux product has recurring failures, AVANU, at its sole discretion, may elect to provide you with a replacement unit selected by AVANU provided that it has functionality at least equal to the product being replaced.

The Limited Warranty is a specified, fixed period commencing on the date of purchase from AVANU. The date on the sales receipt is the date of purchase unless AVANU or your point of purchase informs you otherwise in writing.

Customer Responsibilities

In order to avoid the risk of charges for issues not covered by your limited warranty (issues that are not due to defects in materials and workmanship on AVANU WebMux products), you will be asked to assist AVANU as follows:

1) Verify configurations, update and install most recent firmware

2) Implement temporary procedures or workarounds provided by AVANU while AVANU works on a permanent solution

3) Allow AVANU remote support where applicable. If you choose not to deploy available remote support capabilities, it may result in delays or you may incur additional costs due to increased support resource requirements.

4) Cooperation with AVANU in the attempt to resolve the problem by method of telephone, email or other form of mutually agreed communications. This may involve performing routine diagnostic procedures, installing additional firmware updates or patches.

5) Make a backup copy of your WebMux product configuration file as a precaution against possible failures.

6) Perform additional tasks as requested that AVANU may reasonable request in order to best perform the warranty support.

Limitations

IF YOUR WEBMUX PRODUCT FAILS TO WORK AS WARRANTED ABOVE, THE MAXIMUM LIABILITY OF AVANU UNDER THIS LIMITED WARRANTY IS EXPRESSLY LIMITED TO THE LESSER OF THE PRICE YOU HAVE PAID FOR THE PRODUCT OR THE COST OF REPAIR OR REPLACEMENT OF ANY HARDWARE COMPONENTS THAT MALFUNCTION IN CONDITIONS EXCEPT AS INDICATED ABOVE, IN NO EVENT WILL AVANU BE LIABLE FOR ANY DAMAGES CAUSED BYE THE WEBMUX PRODUCT OR THE FAILURE OF THE PRODUCT TO PERFORM, INCLUDING ANY LOST PROFITS OR SAVINGS OR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES. AVANU IS NOT LIABLE FOR ANY CLAIM MADE BY A THIRD PARTY OR MADE BY YOU FOR A THIRD PARTY.

THIS LIMIATION OF LABILITY APPLIES WHETER DAMAGES ARE SOUGHT, OR A CLAIM MADE, UNDER THIS LIMIED WARRANTY OR AS A TORT CLAIM (INCLUDING NEGLIGENCE AND STRICT PRODUCT LIABILITY), A CONTRACT CLAIM, OR ANY OTHER CLAIM. THIS LIMITATION OF LIABLITY CANNOT BE WAIVED OR AMENDED BY ANY PERSON. THIS LIMITATION OF LIABLITY WILL BE EFFECTIVE EVEN IF YOU HAD ADVISED AVANU OR AN AUTHORIZED REPRESENTATIVE OF AVANU OF THE POSSIBLITY OF ANY SUCH DAMAGES. THIS LIMITATION OF LIABLITY, HOWEVER WILL NOT APPLY TO CALIMS FOR PERSONAL INJURY.

Exclusions

AVANU DOES NOT WARRANT THAT THE OPERATION OF THIS PRODUCT WILL BE UNINTERRUPTED OR ERROR-FREE. AVANU IS NOT RESPONSIBLE FOR DAMAGE THAT OCCURS AS A RESULT OF THE CUSTOMER'S FAILURE TO FOLLOW THE INSTRUCTIONS INTENDED FOR THE WEBMUX PRODUCT.

About the Support Disclaimer

The Support provision covers product configuration and basic remote installation support up to the first sixty-days (60) from purchase date (AVANU has the right to request a proof of purchase document). Technical support applies to WebMux performance only and current version firmware updates.

There will be a fee for any firmware version request other than the current available version and any request for support outside of our normal business hours if not covered under a Premium Annual Support Program.

For assistance beyond our basic remote product configuration, installation and product-specific support, professional consulting with our engineers is available based on our current professional services fee structure. Contact AVANU or your point of purchase representative for current fee schedule.

Technical Support Contact

Monday to Friday excluding US Holidays; 8:00am to 5:00pm Pacific time

Email: techsupport@avanu.com
Online Form Request: Technical Support Request Form
1.888.248.4900 US Toll Free (Extension 202)
1.408.248.8960 International (Extension 202)

Service Center
AVANU®
2122 South Grand Ave Ste H
Santa Ana CA 92705
United States

Note: AVANU approval and an issued RMA number are required for all warranty repair, service, or sales returns. AVANU has the right to refuse any shipment without a RMA number.

* AVANU has the right to offer promotional programs at any time where the Limited Product Warranty and Support coverage may differ.