AVANU®

WebMux Network Traffic Manager

Virtual WebMux™ Edition
AVANU®
Virtual WebMux™ Network Traffic Manager
Software Appliance for Virtualized Platforms
AVANU® WebMux
POWER
AVANU WebMux 13.0.01
BACKUP
FAIL
RESET

Application Delivery Network and Global Server Load Balancing with FireEdge™ for Apps

avanu.com

Notices and Contact Information

Copyrights

Trademarks and Service Marks

AVANU, AVANUAdvantage, Flood Control, FireEdge, MAP, WebMux are trademarks or registered trademarks of AVANU, Inc.

'It is all about the user experience on your network and keeping everyone connected' is a service mark of AVANU, Inc.

This document identifies product names and services known to be trademarks, registered trademarks, or service marks of their respective holders. They are used throughout this document in an editorial fashion only. Use of a term in this document should not be regarded as affecting the validity of any trademark, registered trademark, or service mark. AVANU, Inc. is not associated with any product or vendor mentioned in this document.

Update Information

All products and specifications are subject to change without notice. Contact AVANU, Inc. for the latest information.

August 2019 Rev A

Contact Information

AVANU, Inc.
1.888.248.4900 U.S. Toll Free
1.408.248.8960 International
Email: info@avanu.com
Web Site: https://avanu.com

Table of Contents

WebMux Network Traffic Manager Introduction

Evolving transitional changes in the computer world are posing many challenges to networks. Network infrastructures are highly sophisticated and complex.

High availability is critical when it comes to your network's ability to run smoothly, overcoming network disruption. Performance, scalability, and redundancy/fault tolerance along with reducing site maintenance downtime all are important factors.

A network infrastructure hosts and processes applications residing on the back end servers where it serves both internal and external users. Common applications include accounting, emails, database record management, web services, e-commerce, FTP services, Internet gaming, POP services, IoT device services, mobile device services, call centers, social media, terminal servers, video streaming, etc.

On the horizon is a new era of explosive network traffic growth that will test a network's handling ability.

To successfully manage and control user data traffic, a network traffic manager in the infrastructure is required. The network traffic manager plays a vital role in load balancing the data traffic to provide uses real-time interaction and high availability of services.

Network traffic managers that load balance network data traffic within the core network, regional Edge computing sites, and failover sites are fundamental requirements for high availability. Preserving a network's stability and security are of utmost important priorities.

This paper introduces AVANU's WebMux Network Traffic Manager ("WebMux"), a full-featured load balancing solution. It is an all-inclusive enterprise-class solution that integrates application delivery network (ADN) load balancing and global server load balancing (GSLB) with its built-in FireEdge™ for Apps Web Application Firewall (WAF).

In development since 1987, WebMux features are based on the powerful 64-bit architecture platform. It manages, controls, and secures local data traffic for high availability of applications assuring reliable peak performance with geographic disaster recovery and affinity services and enhanced applications security firewall features.

Using intensive algorithms, WebMux is designed to benefit sophisticated network infrastructures that require full-featured load balancing flexibility to meet and manage the most stringent network traffic demands.

The user-friendly menu-driven interface makes WebMux fast to deploy and easy to manage. It meets the U.S. Federal Information Processing Standard Publication (FIPS) 140-2 Levels 1 & 2 validated encryption computer security standard, Trade Agreements Act (TAA), and Payment Card Industry (PCI) compliance.

WebMux Network Traffic Manager scalable models are available as software appliances for virtualized platforms or reliable high-performing network hardware appliances for fast plug-and-run deployment ease that are quality built to last.

About AVANU, Inc.

AVANU® designs and develops quality products for the IT infrastructure and data center environments that are full-featured, high in performance, and cost-effective for all business sizes.

AVANU founded in 1997, started as a computer network supplier for Internet Service Providers (ISP) and is now a privately held network infrastructure product developer with R&D, manufacturing, and production in the United States. Graduated from the U.S. SBA 8(a)/SDB program in 2015.

AVANU®

WebMux™ Network Traffic Manager

Overcoming Network Disruption with High Availability

© Copyright 2019 AVANU Inc

WebMux Advantages for the Network

Performance

The traffic to servers are distributed among the server farm so that a site can handle more than a single server alone. Other features, such as SSL Offloading and HTTP cache, help reduce impact on server resources.

Scalability

After a farm has been created, more servers can be added to handle the workload as needed without interruption to the network.

Redundancy/Fault Tolerance

A farm contains several servers that serve the same site. If a server should fail, the WebMux health check will detect the failed server and send requests to the remaining servers. Therefore, keeping the site online.

Reduce Site Maintenance Downtime

Servers in a farm can be taken offline for maintenance without interrupting the site.

WebMux Application Delivery Network (ADN)

Local Network Load Balancing Service

Application Delivery Network (ADN) is a core function of WebMux. It manages, controls, and securely delivers local Layers 4-7 traffic reliably to the back-end servers of the network infrastructure. This is where applications and services are processed providing reliable high performance and availability for your users.

These are some common applications requiring local network traffic load balancing:

Web Services • E-Commerce • FTP Servers • Internet gaming • POP servers • IoT device services
Mobile device services • Call centers • Social media • Terminal servers • Video streaming
Internal operations (accounting, database record management, etc.)

WebMux Network Topologies - Arms and Architecture

WebMux accommodates four (4) different load balancing methods or operation modes. Each has its advantage in a network. The term Arm's use refers to the number of physical networks. There are one or two LAN connections (typically External and Internal). Both IPv4 and IPv6 are supported and work in all operation modes.

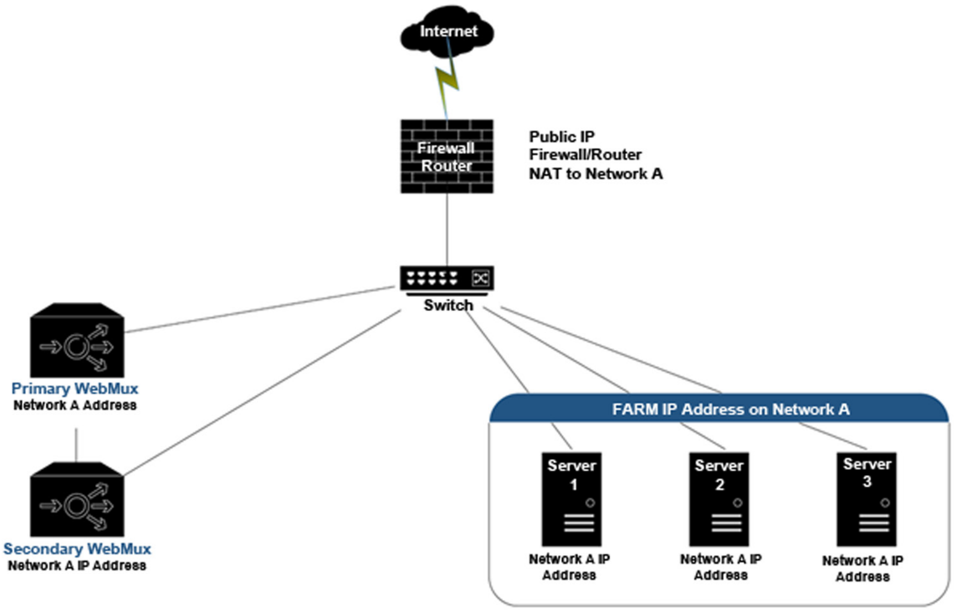
One-Arm Single Network

This configuration is a Network Address Translation (NAT) where WebMux is connected to the network using a single interface. For higher network throughput capacity, a set of interfaces can be bonded together.

Notes:

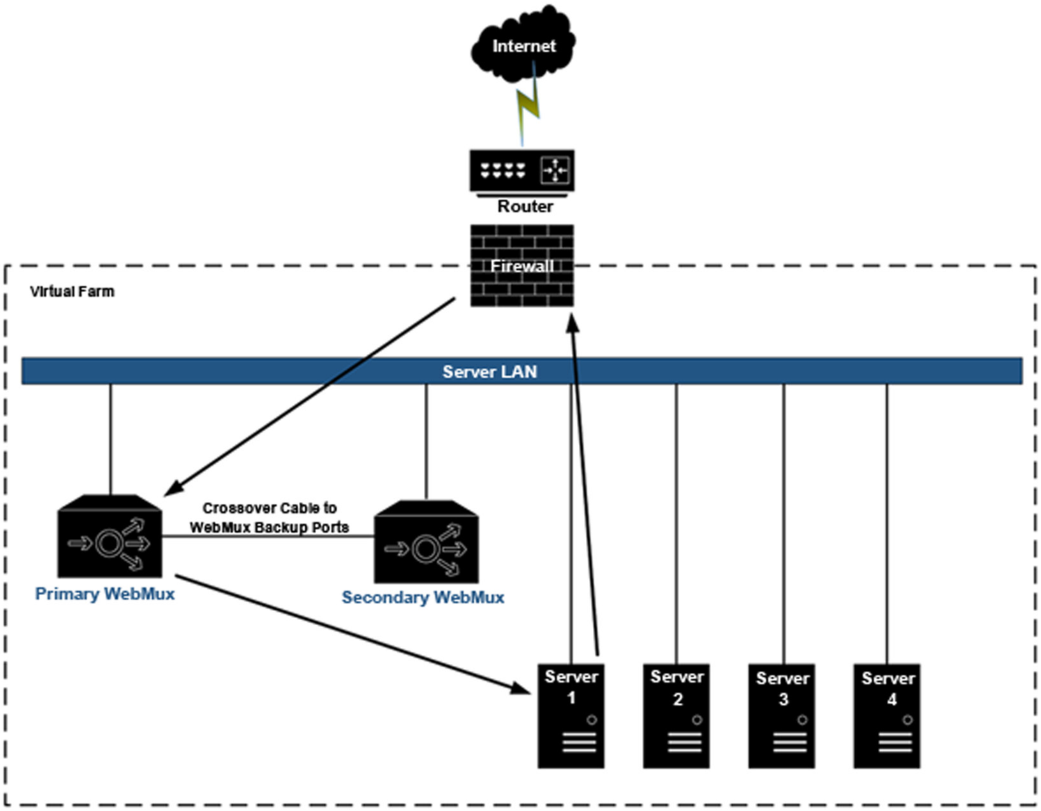
All traffic is Source NAT'd (SNAT) where WebMux becomes the client and the server does not see the client's IP address.

An additional WebMux IP address must be assigned for each 65,000 simultaneous connections due to the SNAT configuration and client-server relationship.



One-Armed Direct Server Return (DSR)

This configuration is also know as Direct Routing or Out-of-Path (OOP) and is the highest performance configuration. WebMux becomes the traffic director for incoming traffic while the return traffic can route back bypassing the WebMux (unless WebMux is configured to do SSL termination).



Notes:

This configuration requires a simple configuration of a “loopback adapter” on the servers.

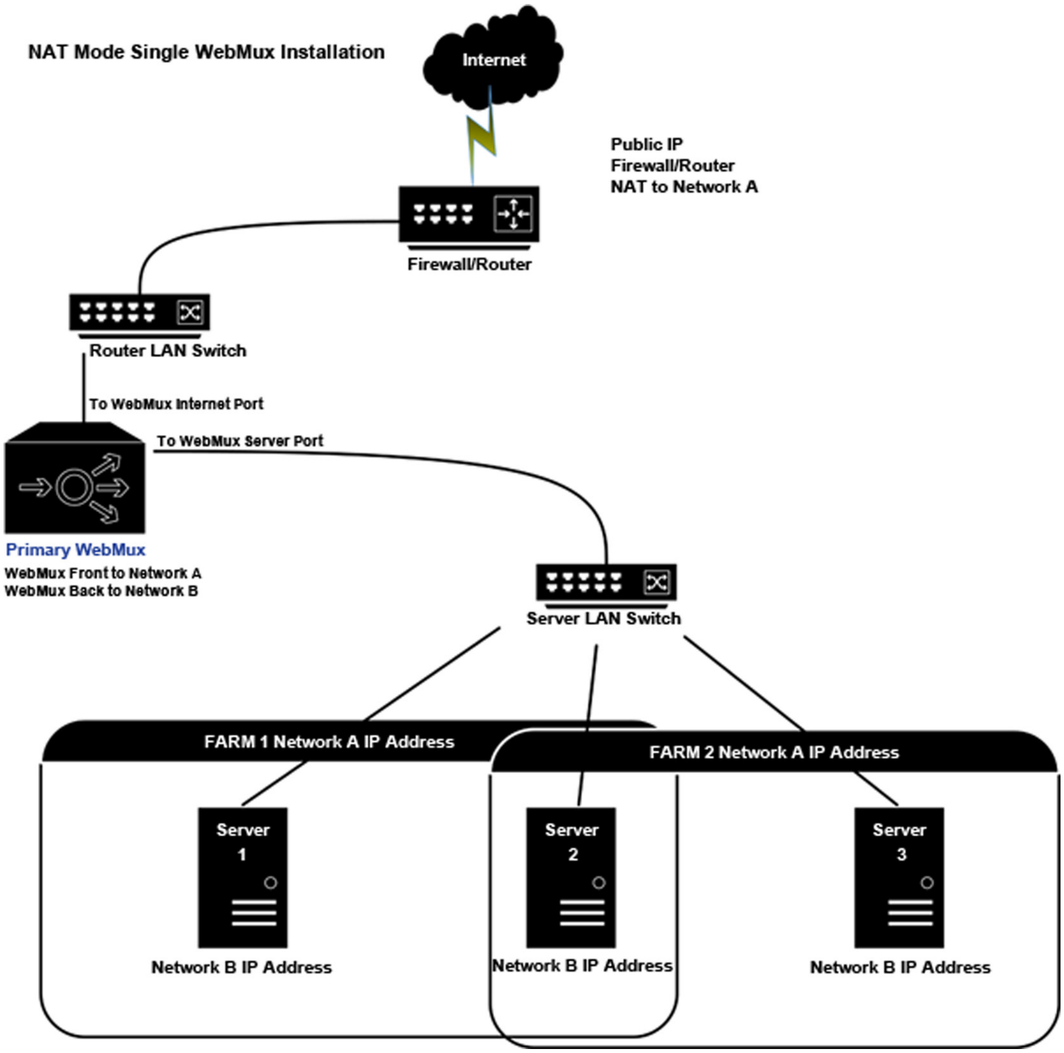
There is no performance advantage if SSL or TLS termination is required as WebMux becomes the endpoint for the SSL/TLS security relationship.

Two-Armed Network Address Translation (NAT)

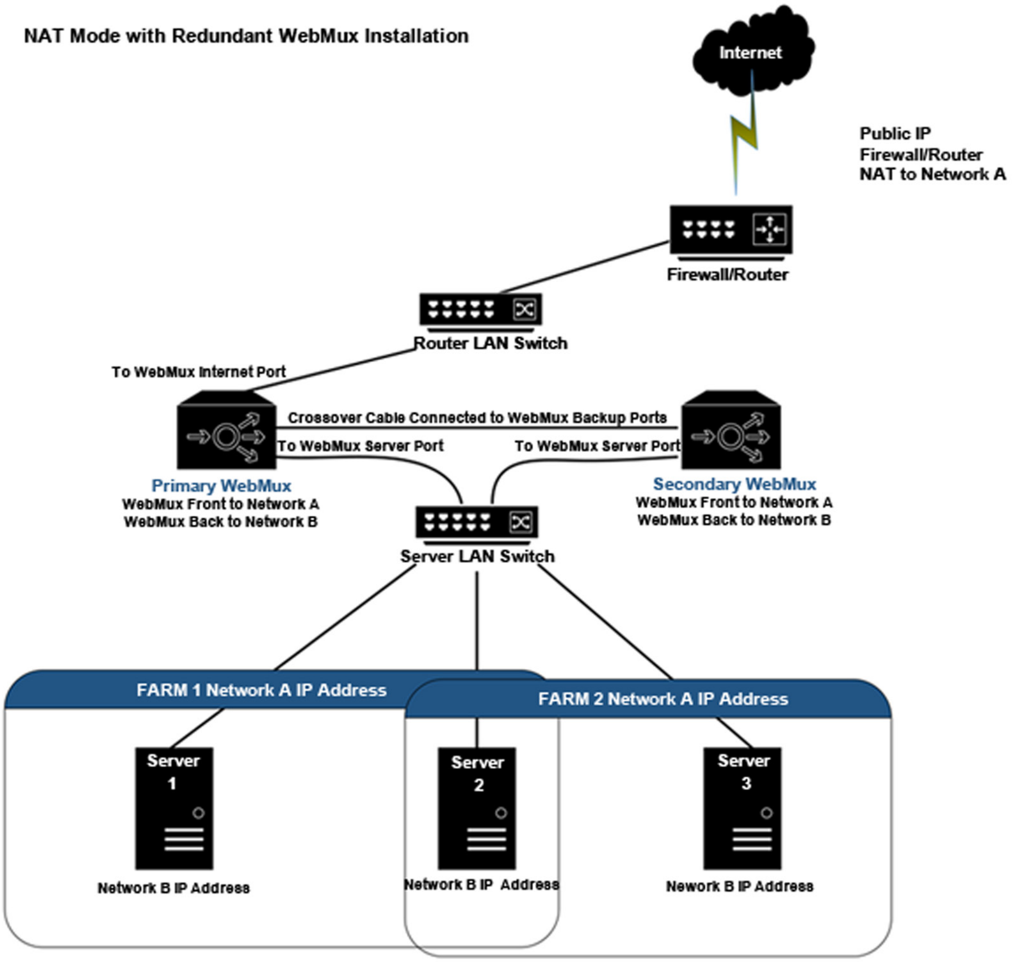
This configuration requires that you have two (2) subnets. It is the common "Destination" NAT configuration where clients connect to a WebMux IP address which WebMux proxies to the back-end servers.

The servers see the clients IP addresses as if the WebMux was not there.

This configuration is required when there are two IP subnets (Internet-side and Internal).



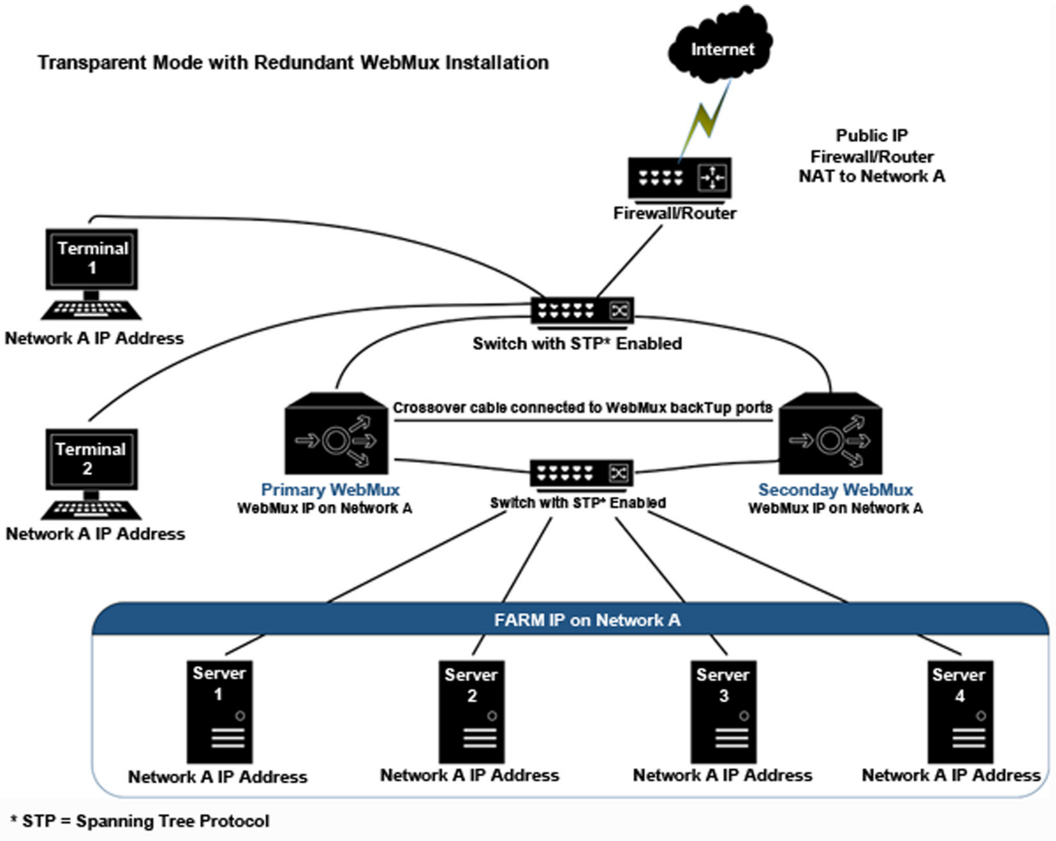
NAT Mode with Redundant WebMux Installation



Two-Armed Transparent

This configuration allows WebMux to act as an Ethernet bridge, with WebMux being inline and Two-Armed. Load balanced and non-load balanced traffic flows through the WebMux.

Note:
With WebMux acting as a bridge, avoid any bridge loops having a circular path through interconnected bridges.



WebMux Load Balancing Scheduling Methods

There are three (3) primary load-balancing scheduling method algorithms that WebMux offers.

Least Connections
Round Robin
Weighted Fastest Response

Along with these primary scheduling methods, there are additional options that include Weighted, Persistent, and combined Weighted and Persistent that give WebMux a total of ten (10) different load balancing behaviors to choose from.

Both Least Connections and Round Robin have the Weighted and Persistent along with combined Weighted and Persistent options. The Weighted Fastest Response has the Persistent option.

WebMux Scheduling Options

Weighted

Weighted scheduling is when a value can be assigned for the amount of network traffic sent to each server. A farm may consist of a variety of servers built with different amounts of memory or CPU speeds. Thus, the network traffic capacity handling and performance from each server will be different from each other within the server cluster.

This option prevents any one server within the farm from being overwhelmed from requests. The weighted value of a server is a ratio of the total weight of all the servers in the farm.

For example, assigning a weight of 100 to one server and 50 to another server will have the same effect as setting the weight of 2 to one server and 1 to another server. In both cases, the ratio between the servers is 2:1 and the server with the highest weight will be favored to get twice as many connections than the lower weighted server.

Persistent

Persistent instructs WebMux to send a returning client back to the original server it connected to, as long as the client reconnects to the server farm within the set Persistent timeout period. This is regardless of the base scheduling method used. The timeout period is set or changed in the WebMux Network Administration settings.

This is beneficial in cases where the servers do not track sessions and clients might disconnect and reconnect expecting to continue a session. Without the Persistent option, the client can be sent to a different server upon returning.

For example, in the case of HTTP services, a client may disconnect immediately after retrieving a resource from a web page, but may make several reconnections to retrieve other resources on the same web page. Although the duration of time could be very minimal between a user's disconnection and reconnection, each connection could potentially send the client to a different server for each of the retrieval.

This would not be a problem for a basic HTTP site, where all the servers in the farm have the same exact copy of the site. However for session dependent services, the Persistent option would be essential to maintain an uninterrupted service rather than sending a client to a different server mid-session that would cause interruption to the user's experience.

Many modern services may already have a means of tracking sessions within a server cluster. With these service types, the Persistent option is not necessary.

WebMux Different Load Balancing Behaviors

Least Connections

With the Least Connections scheduling method, WebMux will send new clients to servers with the least amount of active connections. There will be occasions when clients remain connected to a server for an extended amount of time where other servers may accumulate more client connections than others.

As with any of the load balancing scheduling methods, one cannot always expect to see a leveling of distribution. As connections come and go or remain connected, different servers may gain or lose connections sooner than others. But, the selection of servers to send a client to will continue to be a dynamic decision according to the servers with the Least Connections at the time a client connects to a farm.

Least Connections/Persistent

The Least Connections/Persistent scheduling method instructs WebMux to direct clients that disconnect and reconnect within the persistent timeout period back to the same server they originally connected to, bypassing the load balancing algorithm. New client connections are distributed to the servers according to the Least Connections algorithm.

Weighted Least Connections

When WebMux is configured with the Weighted Least Connection scheduling method, the server weight ratio will prioritize and take precedence over the Least Connections scheduling algorithm. The load balancing schedule then prioritizes between servers of equal ratio.

Weighted Least Connections/Persistent

When WebMux is configured with the Weighted Least Connection/Persistent scheduling method, servers are first prioritized by weight ratio. Then for new connections, WebMux uses the Least Connections scheduling algorithm to prioritize between servers of equal ratio. If a connection is a reconnect within the persistence timeout period, the WebMux will bypass the server weight and load balancing algorithm where it sends the clients' connection directly to the server it was previously connected to.

Round Robin

In a Round Robin scheduling method, WebMux sends client connections to the next available server in a sequential manner. If all connections are of equal in duration and activity, it would be reasonable to expect Round Robin to result in the most even distribution of connections to the servers. However, it must be considered that in real world scenarios not all connections will have equal activity and duration. So, even with

Round Robin, there may be some servers carrying more connections than others; especially in cases where clients tend to remain connected for long periods of time.

Round Robin/Persistent

With Round Robin/Persistent, WebMux distributes new connections to the servers in a sequential manner according to the Round Robin algorithm. However, connections that disconnect and reconnect within the persistence timeout period are sent back to the same server they originally connected to, bypassing the load balancing algorithm.

Weighted Round Robin

When WebMux is configured with the Weighted Round Robin scheduling method, the server weight ratio will prioritize and take precedence over the Round Robin scheduling algorithm. The load balancing algorithm then distributes connections in a sequential manner between servers of equal ratio.

Weighted Round Robin/Persistent

Servers are first prioritized by weight ratio when WebMux is configured with the Weighted Round Robin/Persistent scheduling method. Then, for new connections, the Least Connections algorithm distributes connections in a sequential manner between servers of equal ratio. If a connection is a reconnect within the persistence timeout period, it will bypass the server weight and load balancing algorithm and is sent directly to the server it was previously connected to.

Weighted Fastest Response

The WebMux Weighted Fastest Response scheduling method calculates a value based on the number of current connections, divided by the server weight. The server with the lowest value is determined to be the server that can provide the fastest response.

Weighted Fastest Response/Persistent

With the WebMux configured using the Weighted Fastest Response/Persistent scheduling method, WebMux will distribute new connections to the servers according to the Weighted Fastest Response scheduling algorithm. However, connections that disconnect and reconnect within the persistence timeout period are sent back to the same server they originally connected to, bypassing the load balancing algorithm.

WebMux Network Traffic Manager Security

Access Control List System

This restricts or allows specified source IP addresses to connect to WebMux web GUI.

Authentication - LDAP, TACACS+

This allows you to add additional admin users for the WebMux web GUI.

Automatic Attack Detection (AAD)

WebMux restricts the maxiumum number of TCP connections coming from a single IP source. Additional IP address filtering with whitelist and blacklist for known sources.

Flood Control™ - Advanced Denial of Service (DoS) and Distributed Denial of Service (DOS, DDoS) Protection

Limits the maximum bandwidth a single connection is allowed to have. If that limit is reached, Flood Control will block that connection for a period of time.

Flood Control differs from network firewalls. Firewall rules and protocols are set where it is either 'on' or 'off'. If the settings are wrong, it could block legitimate traffic to the network servers.

SSL Acceleration

WebMux SSL/TLS acceleration is a method of offloading processor-intensive public-key encryption and decryption for Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), to a hardware accelerator.

SSL Certificates (Third Party Support)

SSL certificates signed by any third party Certificate Authority can be used on the WebMux as long as you have the corresponding private key as well.

SSL Certificate Signing Request (CSR)

The SSL Certificate Signing Request is an encoded block of text that is sent to the Certificate Authority to be digitally verified and signed. A signed certificate will allow the web browser to display an indication that the certificate being used on the site has been validated by a trustred Certificate Authority.

SSL Encryption

WebMux supports 1024, 2048, 4096, and 8192 bit encryption. The certificate encryption strength is a measure of number of bits in the key used to encrypt data during an SSL session. The bigger the number, the longer it takes for computer(s) to decrypt enciphered data.

SSL/TLS TCP Protocols Support

Support for TLS 1.0 and TLS 1.2

SSL FIPS 140-2 Levels 1 and 2 compliant - Federal Information Processing Standard

WebMux complies with FIPS 140-2 Level 2 regulatory requirements with its digital monitoring and built-in physical intrusion protection.

SSL Termination/Offloading

SSL termination is supported on all WebMux – WebMux' SSL termination rating is based on actual SSL transactions per second

Web Application Firewall (WAF)- FireEdge™ for Apps

FireEdge™ for Apps is WebMux integrated Web Application Firewall (WAF). It adds web application security by monitoring HTTP traffic to and from the back-end network servers, detecting and blocking malicious activities.

FireEdge for Apps features ModSecurity and comes complete with the Open Web Application Security Project (OWASP) Core Rule Set 3, protecting the servers against OWASP Top 10 most dangerous Web application security flaws:

Unvalidated Input

If web requests used by a web application are not validated before reaching the web application, flaws can be used to attack backend components through a web application.

Broken Access Control

If restrictions on what authenticated users are allowed to do are not properly enforced, flaws can be exploited to access users' accounts, view restricted files, and other unauthorized functions.

Broken Authentication and Session Management

If account credentials and session tokens are not properly protected, then password, keys, session cookies, or other tokens can override session restrictions and assume other users' identities.

Cross Site Xcripting (XSS) Flaws

This exploit uses the Web application as a mechanism to transport an attack to an end user's browser and can disclose the end user's session token, attack the client machine, or spoof content to fool the user.

Buffer Overflows

CGI, libraries, drivers, and Web application server components that do not properly validate input can be crashed and, even possibly, be used to take control of a process.

Injection Flaws

An attacker can embed malicious commands in the parameters Web applications send to external systems or the local operating system.

Improper Error Handling

If error conditions that occur during normal operation are not handled properly, an attacker can cause errors to occur that the Web application does not handle. They can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.

Insecure Storage

Cryptographic functions in Web applications used to protect information and credentials can be difficult to code and integrate properly, resulting in weak protection.

Denial of Service (DoS)

Attackers can consume Web application resources to the point where legitimate users can no longer access or use the application. Users can be locked out of their accounts or even cause the entire application to fail.

Insecure Configuration

Servers have many configuration options that affect security and are generally not secure by default.

WebMux Network Traffic Manager Protocols

ASP – Active Server Pages
Server-side scripting engine for Microsoft's IIS Web Server for dynamically generated web pages
Basic Layer 2 Protocols (i.e., STP, MSTP, RSTP...)
Layer 2 protocols are the link level protocols.

DNS – Domain Name Server
A directory server that resolves domain names to their corresponding IP address.

FTP – File Transfer Protocol
A service for sending and receiving files.

HTTP – Hypertext Transfer Protocol
This the application level protocol of the World Wide Web.

HTTPS (SSL/TLS)
WebMux supports and does health checks using the Server Name Indication (SNI) TLS extension.

IMAP – Internet Message Acces Protocol
Internet standard for email clients to retrieve messages from an email server.

LDAP – Lightweight Director Access Protocol
An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

NNTP – Network News Transfer Protocol
An application protocol used for transporting Usenet news articbetween news servers and for reading and posting articles by end user client applications.

POP3 – Post Office Protocol
POP3 is a protocol for receiving email by downloading all your messages to your computer from a mailbox on the server of an Internet service provider, unlike IMAP which only retrieves messages as needed.

RDP (Terminal Services)
Remote Desktop Protocol is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.

SMTP - Simple Mail Transfer Protocol
An Internet standard for electronic mail (email) transmission.

SNMP - Simple Network Management Protocol
An Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

SSH – Secure Shell

Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. The best known example application is for remote login to computer systems by user.

Streaming Media

Streaming media is video or audio content sent in compressed form over the Internet and played immediately, rather than being saved to the hard drive. With streaming media, a user does not have to wait to download a file to play it. Because the media is sent in a continuous stream of data it can play as it arrives.

TCP/UDP-based Services - Transmission Control Protocol and User Datagram Protocol

Services that do not fall under any specific protocol, but operated within IPv4 and/or IPv6.

TFTP - Trivial File Transfer Protocol

An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required.

WebMux Other Operation Modes

Active/Passive Redundant Operation

Primary WebMux is active while secondary WebMux is in standby mode for high availability failover mode. Requires two (2) WebMux Virtual software licenses or hardware appliances.

Active/Active WAN

Multiple gateway network failover - The WebMux can be configured with multiple default gateways allowing the WebMux to maintain Internet connection should one Internet gateway go down.

Application GUI and Wizard Setup

Application specific templates are available to quickly deploy WebMux in just a few steps.

Application Health Checking

Health checks for specific application services are checked for actual application level server responses, not jus a ping to a port.

Adaptive Balancing

Load balancing options that factor in current number of connections or distribute connections according to server weight preferences.

Bonding/Teaming Ports (802.3ad/LACP)

Port Bonding/Teaming (also known as Link Aggregation Group, LAG) allows you to combine two or more ports together to act as a single network interface with a combined bandwidth of all the ports in the LAG.

Content Encoding (HTTP Compression)

HTTP compression improves transfer speed and bandwidth utilization. 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.

Digital Monitoring

The WebMux front LCD panel displays network activity, CPU, and memory usage.

IP Persistence

Connections that disconnect within a time period are returned to the same server they originally connected to in order to preserve client sessions.

Link Interface Bonding

Combine the bandwidth of two (2) or more network interface to work as a single, larger data pipe.

Multiple Address and Port (MAP™)

The WebMux MAP feature binds multiple addresses and ports as a single service, thus one client will be sent to the same server across all those addresses and ports. This is useful for making audio/video calls, or in complex database configurations.

REST API – Representational State Transfer: Application Programming Interface

Provides flexible and versatile configuration and query access with RESTful API. Responses are in the easily parsed JavaScript Object Notation (JSON) format.

Reverse Proxy

Network address translation with port redirection. A reverse proxy server retrieves resources on behalf of a client from one or more servers. WebMux performs the reverse proxy function for Microsoft Lync Server at the external edge where WebMux is always proxying as part of the load balancing operation.

SSL Termination/Offloading

Centralize key and certificate management on the WebMux rather than needing to have keys and certificates on each individual server. The WebMux will take care of the encryption and decryption so the servers can maintain more of their resources.

Multiple VLAN Trunking (IEEE 802.1Q)

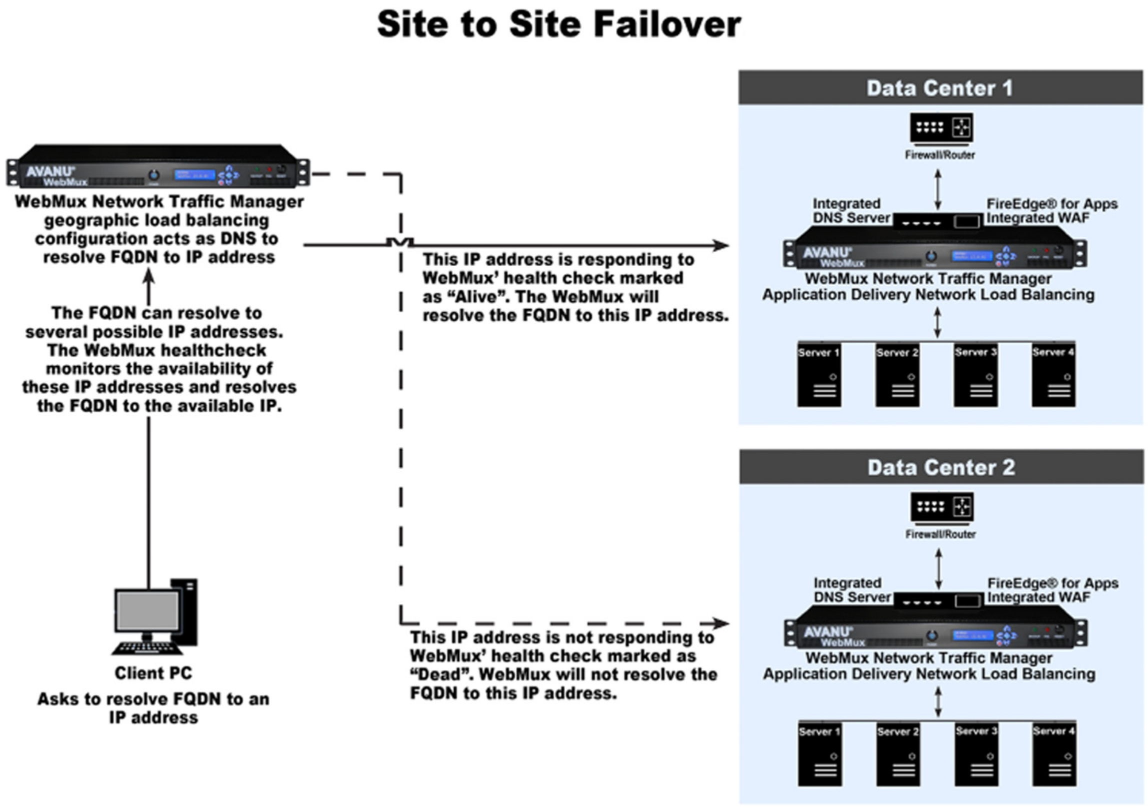
The WebMux load balance ports can be configured to participate in 802.1q Tagged VLANs.

Web-based GUI

WebMux management can be done using any of the common available web browsers, including web browsers on mobile devices.

WebMux Global Server Load Balancing (GSLB)

WebMux provides additional high-availability with its built-in intelligent Domain Name Service (DNS) server features that add Global Server Load Balancing (GSLB) capabilities. The GSLB feature lets you easily set up disaster recovery sites in case of a catastrophic occurrence that brings you main site down and geographic affinity capabilities that determine the geographic location of clients where it resolves the site name to an IP address that is nearest to the client.



Site to Site Failover

WebMux Network Traffic Manager geographic load balancing configuration acts as DNS to resolve FQDN to IP address

The FQDN can resolve to several possible IP addresses. The WebMux healthcheck monitors the availability of these IP addresses and resolves the FQDN to the available IP.

Client PC

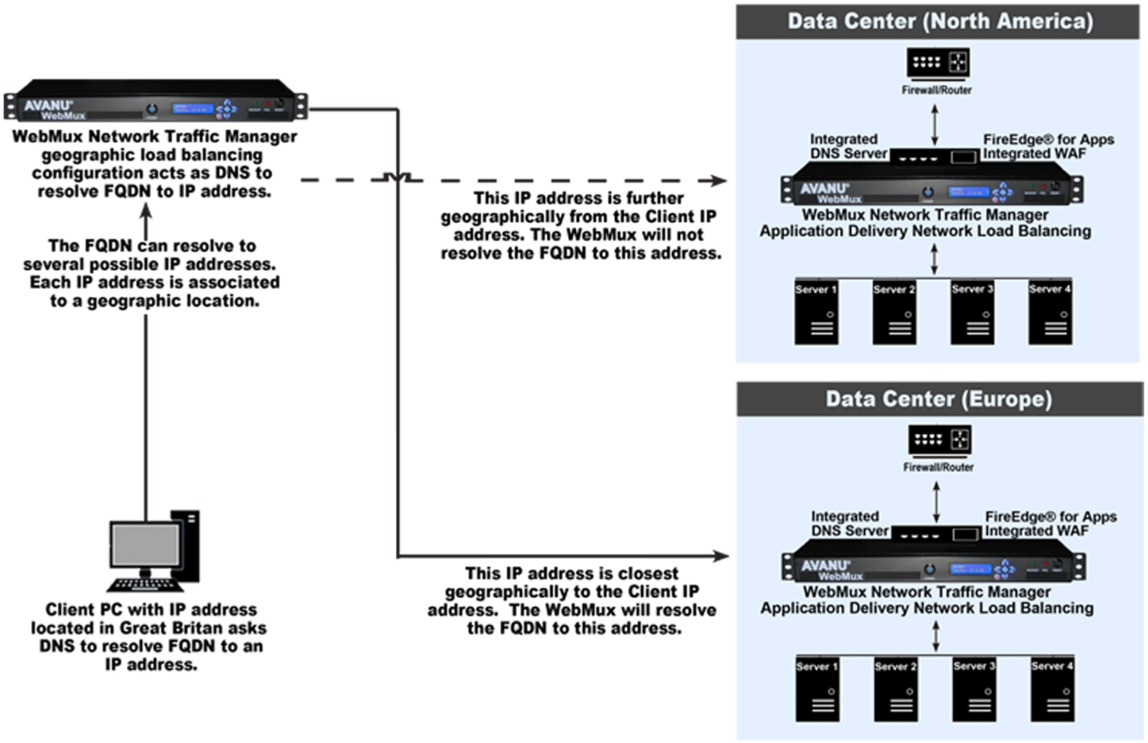
Asks to resolve FQDN to an IP address

This IP address is responding to WebMux' health check marked as "Alive". The WebMux will resolve the FQDN to this IP address.

This IP address is not responding to WebMux' health check marked as "Dead". WebMux will not resolve the FQDN to this IP address.

AVANU WebMux
Data Center 1
Firewall/Router
Integrated DNS Server
FireEdge® for Apps Integrated WAF
AVANU WebMux
WebMux Network Traffic Manager
Application Delivery Network Load Balancing
Server 1
Server 2
Server 3
Server 4
Data Center 2
Firewall/Router
Integrated DNS Server
FireEdge® for Apps Integrated WAF
AVANU WebMux
WebMux Network Traffic Manager
Application Delivery Network Load Balancing
Server 1
Server 2
Server 3
Server 4

Geographic Affinity



Data Center (North America)
Firewall/Router
Integrated DNS Server
FireEdge® for Apps Integrated WAF
WebMux Network Traffic Manager
Application Delivery Network Load Balancing
Server 1
Server 2
Server 3
Server 4
Data Center (Europe)
Firewall/Router
Integrated DNS Server
FireEdge® for Apps Integrated WAF
WebMux Network Traffic Manager
Application Delivery Network Load Balancing
Server 1
Server 2
Server 3
Server 4

WebMux Network Traffic Manager geographic load balancing configuration acts as DNS to resolve FQDN to IP address.

The FQDN can resolve to several possible IP addresses. Each IP address is associated to a geographic location.

Client PC with IP address located in Great Britan asks DNS to resolve FQDN to an IP address.

This IP address is further geographically from the Client IP address. The WebMux will not resolve the FQDN to this address.

This IP address is closest geographically to the Client IP address. The WebMux will resolve the FQDN to this address.

WebMux Network Traffic Manager Highlights

Full-featured integrated load balancing solution

Application Delivery Network (ADN) for local network traffic load balancing

Global Server Load Balancing (GSLB) for added higher-availabilty adding disaster recovery sites and geographic affinity

FireEdge for Apps, a Web Application Firewall (WAF) as an added safety net

Scalable models - software appliances for virtualized platforms and network hardware appliances

WebMux supports many virtualized platforms including VMWare®, Citrix XENServer®, Microsoft® Hyper-V, Oracle Virtual Box®, XEN project, and KVM (Kernal-based Virtual Machine).

WebMux reliable high-performing network hardware appliances for fast plug-and-run deployment ease that are quality built to last.

Operates on-premise, hosted/co-lo data centers, private/public/hybrid Cloud

Proven reliable high performance with extensive load balancing features on all software and hardware appliance models

GUI menu-driven for easy fast setup and manageability (no certified training or timely script writing required)

Self-contained (no royalty or extra hidden costs)

Includes a full year of product technical support; network hardware appliances include two (2) years warranty (parts and labor)

WebMux Network Traffic Manager Summary

Every manufacturer has their way of specifying their network load balancing solutions. It is difficult to make one to one comparison on almost any parameter where details of features may differ, making it more challenging for a buyer.

Proven and tested over time, there are some salient features highlighted by our customers in their selection of WebMux for load balancing their network infrastructure – reliable trouble free operation, ease of setup and operation, performance, and affordability that delivers overall cost-of-ownership value.

In conclusion, WebMux is a solid choice for sophisticated network infrastructures requiring full-featured load balancing flexibility to meet and manage the most stringent network traffic demands.