



FortiBalancer Exchange 2010 Deployment Guide

for FortiBalancer 8.0 MR2 and higher

Carl Windsor



Revision History

Date	Revision Number	Change Description
2012-03-28	Revision 1	Initial revision.
2012-04-03	Revision 2	Template change

Exchange 2010 Deployment Guide for FortiBalancer Revision 2

28 March 2012

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners.

Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Support will be provided to customers who have purchased a valid support contract. All registered customers with valid support contracts may enter their support tickets via the Fortinet Technical Support web site:

<https://support.fortinet.com>

Contents

Introduction	5
Prerequisites & Assumptions	5
Exchange Server 2010	5
FortiBalancer Appliance	5
Introduction to Exchange Server 2010	6
Exchange Server 2010 Architecture	6
FortiBalancer Application Delivery Controller Benefits	7
Deployment for Exchange Server 2010 Roles	9
FortiBalancer Solution for Exchange Server 2010 Deployments	10
Verification Tools	10
FortiBalancer Configuration Summary	10
Configuring FortiBalancer for Outlook Web App	12
Configuration Steps	12
Create Outlook Web App Service Health Check (Optional)	12
Create Outlook Web App Real Service	14
Create Outlook Web App Service Group	16
Create Outlook Web App Virtual Service	18
Enable Outlook Web App SSL Offloading	20
Enable Outlook Web App Rewrite/Redirect	23
Configuring FortiBalancer for Outlook Anywhere	27
Configuration Steps	27
Create Outlook Anywhere Service Health Check	27
Create Outlook Anywhere Real Service	27
Create Outlook Anywhere Service Group	28
Create Outlook Anywhere Virtual Service	29
Enable Outlook Anywhere SSL Offloading	30
Configuring the FortiBalancer Appliance for ActiveSync	32
Configuration Steps	32
Create ActiveSync Service Health Check	32
Create ActiveSync Real Service	34
Create ActiveSync Service Group	34
Create ActiveSync Virtual Service	35
Enable ActiveSync SSL Offloading	36
Misc – Change TCP Idle Timeout	37
Configuring the FortiBalancer Appliance for RPC Client Access	39

Dynamic Port Configuration Steps	40
<i>Create RPC Client Access Service Health Check</i>	40
<i>Create RPC Client Access Real Service</i>	40
<i>Create RPC Client Access Service Group</i>	41
<i>Create RPC Client Access Virtual Service</i>	42
Configuring the FortiBalancer Appliance for POP3	44
Configuration Steps	44
<i>Create POP3 Service Health Check</i>	44
<i>Create POP3 Real Service</i>	44
<i>Create POP3 Service Group</i>	45
<i>Create POP3 Virtual Service</i>	46
<i>Enable POP3 SSL Offloading</i>	47
Configuring the FortiBalancer Appliance for IMAP4	48
Configuration Steps	48
<i>Create IMAP4 Service Health Check</i>	48
<i>Create IMAP4 Real Service</i>	48
<i>Create IMAP4 Service Group</i>	49
<i>Create Secures IMAP4 Virtual Service</i>	50
<i>Enable IMAP4 SSL Offloading</i>	50
Configuring the FortiBalancer Appliance for SMTP (Edge Transport) 52	
Configuration Steps	52
<i>Create SMTP (Edge Transport) Service Health Check</i>	52
<i>Create SMTP (Edge Transport) Real Service</i>	52
<i>Create SMTP (Edge Transport) Service Group</i>	53
<i>Create SMTP (Edge Transport) Virtual Service</i>	54
<i>Enable SMTP (Edge Transport) SSL Offloading</i>	55
<i>Misc SMTP Outbound Support</i>	55
Configuring the FortiBalancer Appliance for Link Redundancy Using LLB	57
Configuration Steps	57
<i>Add additional port for WAN-2 access</i>	58
<i>Add Duplicate Virtual Service for WAN 2 access</i>	58
<i>Create LLB Links information</i>	59
<i>Create LLB DNS record for inbound traffic</i>	60
Configuring the FortiBalancer Appliance for Exchange 2010 Site Resilience Using GSLB	62
Fault Tolerance Configuration	63
Configuration Steps	63
<i>Define GSLB/SDNS Members</i>	63
<i>Creating GSLB Records</i>	64
<i>GSLB/SDNS Disaster Recovery Site Location</i>	65
<i>Creating DR Group with DNS domain name</i>	66
<i>Setup GSLB/SDNS with BIND 9</i>	67
<i>GSLB/SDNS DR Deployment Verification</i>	68
<i>Log Information</i>	69
Summary	72

Introduction

Prerequisites & Assumptions

Exchange Server 2010

This document is written with the assumption that you are familiar with Microsoft Exchange Server 2010 products. For more information on planning and deploying the Exchange Server 2010 please reference the appropriate documentation at:

<http://technet.microsoft.com/en-us/library/bb124558.aspx>

FortiBalancer Appliance

The FortiBalancer appliance must be running version FBLOS TM 8.2 or later. For more information on deploying the FortiBalancer appliance please refer to the FortiBalancer Web UI Guide which is included in the product CD or access it through the product Web user interface.

We assume that the FortiBalancer appliance is already installed in the network with management IP, interface IP, VLANs and default gateway configured.

Learn about your Exchange Server 2010 deployment in your network and note down VLAN information, IP addresses, and port numbers for various Client Access Servers (CAS) and Edge Transport Servers (ETS) and their roles. You will need them for configuring virtual sites and load balancing policies on the FortiBalancer appliance.

Introduction to Exchange Server 2010

The Exchange Server 2010 is a new architecture that is designed to provide users with the freedom to securely access all of their communications—email, voice mail, instant messaging, and more—from virtually any platform, Web-browser or device regardless of where they are.

Exchange Server 2010 Architecture

The Exchange Server 2010 architecture consists of different server roles:

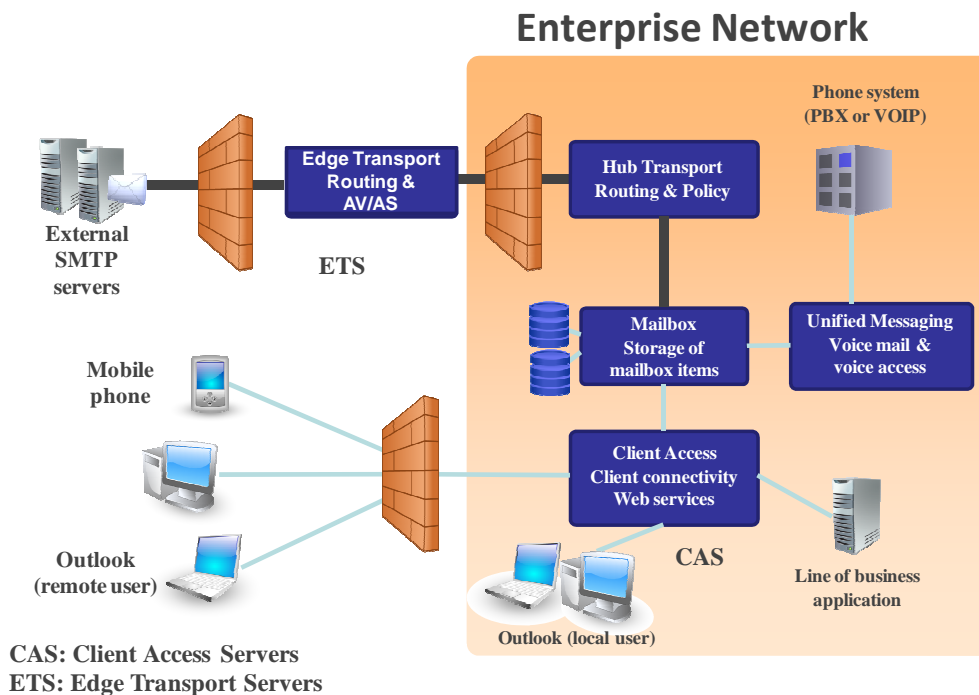


Figure 1:- Exchange Server 2010 Architecture

- **Client Access Server:** This is the server that receives mail requests from remote and internal users from a variety of end user devices
- **Edge Transport Server:** This is the mail routing server that typically sits at the perimeter of the topology and routes mail in to and out of the Exchange Server 2010 environment.
- **Mailbox Server:** This server hosts mailboxes and public folders.
- **Unified Messaging Server:** This is the server that connects a Private Branch eXchange (PBX) system to Exchange 2010.
- **Hub Transport Server:** This is the mail routing server that routes mail within the Exchange organization.

Exchange Server 2010 Load Balancing Requirements

Microsoft recommends a hardware load balancer for the purposes of incorporating high availability, site resiliency, scalability and security to the Exchange Server environment. Also due to various Exchange Server roles and services, session persistence support on the load balancers is an important requirement.

FortiBalancer Application Delivery Controller Benefits

The FortiBalancer delivers all required application delivery functions for optimizing application delivery for Exchange Server 2010 environments, such as Layer 4-7 server load balancing, high availability, SSL acceleration and offloading, DDoS protection, TCP connection multiplexing, caching and compression – all in a single, easy-to-manage appliance.

Availability & Scalability

The FortiBalancer's server load balancing ensures 99.999% uptime for Exchange Server 2010 deployments. Customers can scale their Exchange environment to meet capacity and performance needs with FortiBalancer server load balancers.

Site Resilience

The FortiBalancer's global server load balancing directs traffic away from failed data centers and intelligently distributes services between sites based on proximity, language, capacity, load and response times for maximum performance and availability.

ISP Link Availability

The FortiBalancer's link load balancing with advanced link failover and bandwidth management optimizes the availability, security, cost and performance of Exchange Server 2010 deployments across multiple WAN connections.

SSL Offloading

The FortiBalancer appliance offloads 1024-bit and 2048-bit SSL encryption/decryption from Exchange 2010 Servers to improve performance and reduce the number of Exchange 2010 servers required to support high volume secure mail processing.

TCP Connection Multiplexing

The FortiBalancer appliance multiplexes several client TCP connections into fewer Exchange Server 2010 TCP connections for increase throughput and performance. The FortiBalancer appliance also reuses existing server connections.

Session Persistence

The FortiBalancer appliance performs session persistence for Exchange Server 2010 user traffic and ensures that users are directed to same servers for the duration of their session.

Cache Offload

The FortiBalancer appliance serves frequently requested content from cache for increase performance and scales the capacity of the Exchange 2010 Server environment.

HTTP Compression

The FortiBalancer appliance compresses and delivers Exchange Server 2010 mail attachments and messages over LAN and WAN networks.

Network and Server Protection

The FortiBalancer appliance protect Exchange Server 2010 components (servers and services) from malicious network and server attacks like DDoS attacks, SYN floods, TCP port scans, UDP floods and UDP port scans, etc.

Deployment for Exchange Server 2010 Roles

Exchange Server 2010 has two main roles when front ending end-users in the datacenter, the Client Access Server role and the Edge Transport server role.

The Client Access Server role accepts connections to Exchange 2010 from different clients, such as, but not limited to, Microsoft Outlook.

The five Client Access modes are:

- **Outlook Web App (OWA)** – access your email from any Web browser
- **Outlook Anywhere** – access your email from the Internet using Microsoft Outlook Messaging API (MAPI) over HTTP
- **ActiveSync** – synchronize e-mail between your mobile phone and Exchange 2010
- **Remote Procedure Call (RPC) Client Access** – access your email via Microsoft Outlook MAPI
- **POP3/IMAP4** – access your email from standard email clients

Other Client Access mode services:

- **Exchange Web Services (EWS)** – offers web services API
- **Autodiscovery** – simplify user's profile configuration
- **Offline Address Book (OAB) distribution** – OAB access via web-based distribution for Outlook clients

The Edge Transport server role performs anti-spam and antivirus filtering, and applies messaging and security policies to messages in transport in and out of datacenter.

- **Simple Mail Transfer Protocol (SMTP)** – Routes mail in to and out of the Exchange Server 2010 environment

This guide gives you step-by-step procedures for configuring the FortiBalancer appliance to optimize each mode.

FortiBalancer Solution for Exchange Server 2010 Deployments

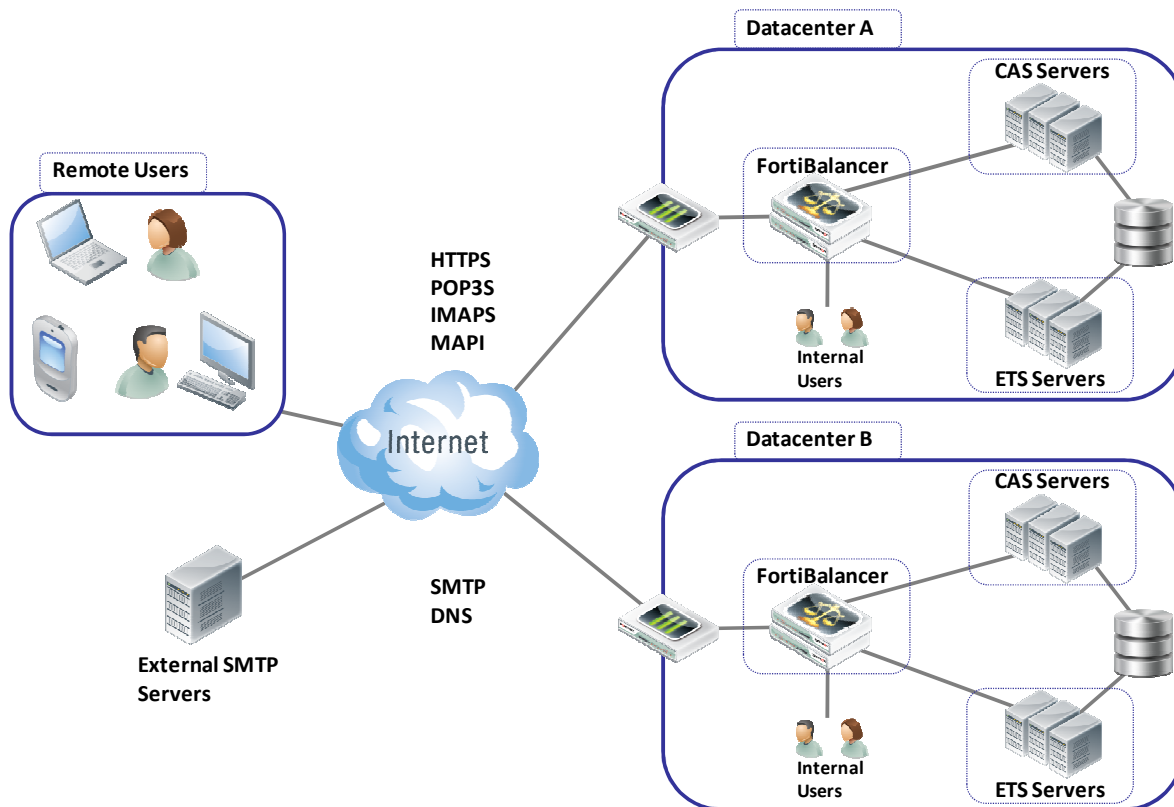


Figure 2:- Load Balancing Solution for Exchange 2010

Verification Tools

To validate Exchange 2010 and the FortiBalancer deployment, Microsoft provides tools to generate simulated Exchange workload. Following tools are recommended:

[Exchange Server Load Generator 2010](#)

The Load Generator (LoadGen) tool is designed to produce a simulated client workload against a test Exchange deployment. LoadGen is capable of simulating Microsoft Office Outlook 2003 (online and cached), Outlook 2007 (online and cached), and POP3, IMAP4, SMTP, ActiveSync, and Outlook Web App client activity.

From Outlook Local Users:

[Exchange Remote Connectivity Analyzer](#)

Microsoft provides online *Exchange Remote Connectivity Analyzer* for Exchange customers to validate internet access.

FortiBalancer Configuration Summary

Following table shows the FortiBalancer configuration information used for Virtual Service and Real Service.

Application/ Service	Virtual Service		Real Service		Affinity	Health Check
	Protocol	Port	Protocol	Port		
OWA	HTTPS	443	HTTP	80	Cookie	HTTP
Outlook Anywhere	TCP	443	TCP	80	None	HTTP
ActiveSync	HTTPS	443	HTTP	80	None	HTTP
POP3	POP3S	995	POP3	110	None	TCP
IMAP	IMAP4S	993	TCP	143	None	TCP
SMTP	TCP	25	TCP	25	None	TCP
RPC Client Access	TCP	135, Port range	TCP	any	Client IP	PING+ Additional

Configuring FortiBalancer for Outlook Web App

Outlook Web App allows authorized users to securely access their Exchange mailboxes through a web browser. By using FortiBalancer load balancers/traffic managers in front of Outlook Web App servers, you gain the following high-availability and improved user experience benefits:

- The FortiBalancer appliance can load balance and monitor application availability ensuring high-availability across multiple Outlook Web App servers.
 - The FortiBalancer appliance provides SSL offloading, content caching/compression features which improve client performance and reduces server load.
- The FortiBalancer appliance can transparently redirect HTTP to HTTPS for client requests.
- The FortiBalancer appliance can transparently rewrite and redirect from HTTP to HTTPS for server response.
- The FortiBalancer appliance can alleviate security concerns, such as DDoS/Spike.

OWA setup also can serve Exchange Control Panel (ECP) service.

Configuration Steps

Create Outlook Web App Service Health Check (Optional)

Make certain you are in **Config** mode and have selected the feature **Real Services** from the sidebar **[a]**. The configuration window will display two tabs **[b]**, **Real Services** and **Health Check Setting**.

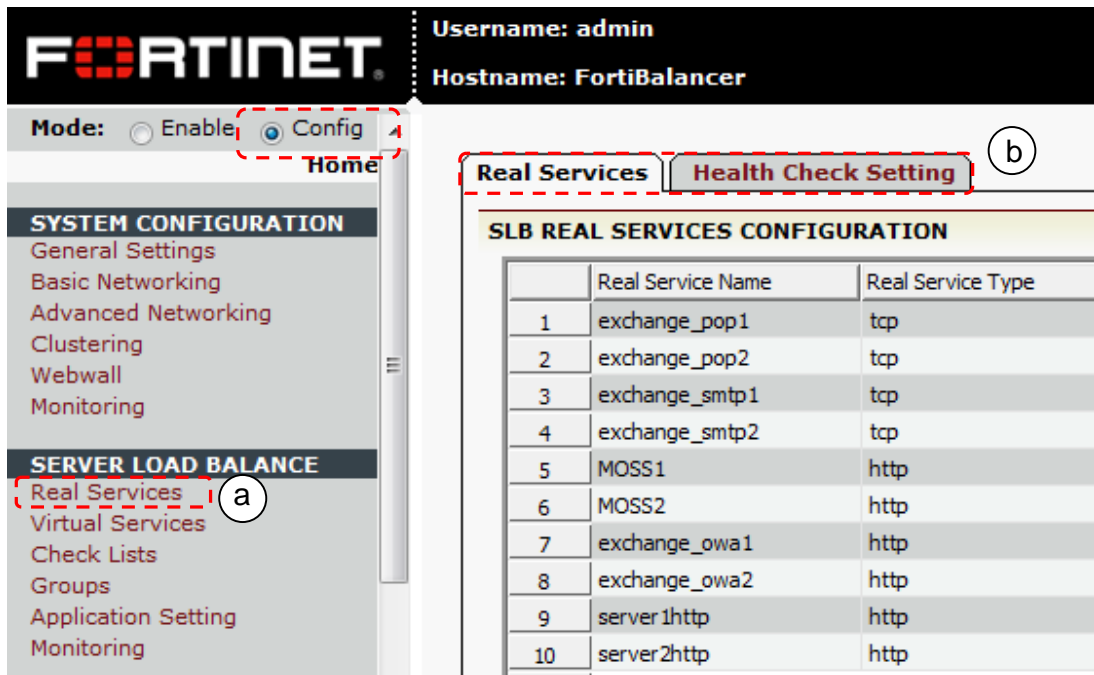


Figure 3 Add Real Service

Optional: For better OWA application service Health Check, simple HTTP content health check can be better than TCP/ICMP health check for service availability:

1. Click on the "Health Check Setting" tab [b], a new window will display.
2. Select "3 HEAD / HTTP/1.0\r\n\r\n" [see figure below].
3. Input the fields relating to the Response String.
4. In our example we need to input "GET /owa/cas.cfm HTTP/1.0\r\n\r\nHOST: owa.domain.com".
5. Select "3 200 OK".
6. Input the fields relating to the Response String. In our example we need to input "SERVER IS UP!".
7. Finish the Health Check Setting by clicking "SAVE CHANGES".

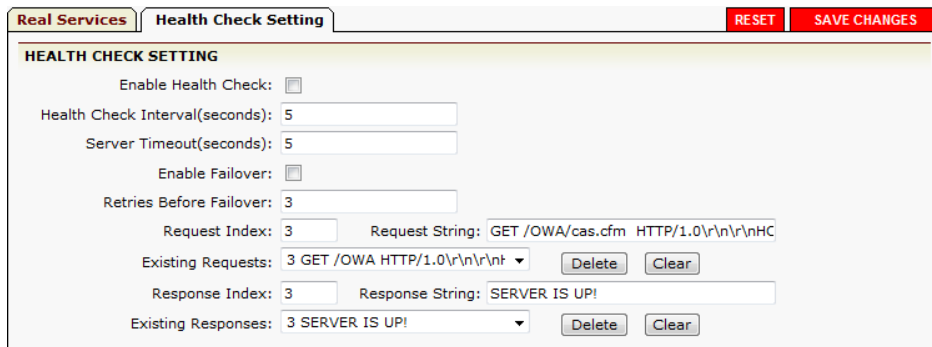


Figure 4:- Customize OWA Health Check Setting

Equivalent CLI Configuration:

```
health request 3 "GET /OWA/cas.cfm HTTP/1.0\r\n\r\n"  
health response 3 "SERVER IS UP!"
```

Note: The “cas.cfm” is (optional faked) Web page to help monitor CAS OWA application availability. You can use any Web page and check its returned content for the application status.

Create Outlook Web App Real Service

Real Services are the 3 CAS servers. Add each CAS server with its name, IP/port and protocol information as a Real Service using the following steps:

1. Select the action link “**Add Real Service Entry**”. The configuration window will present a new screen for SLB REAL SERVICES CONFIGURATION.



	Real Service Name	Real Service Type	Real Service IP	Real Service Port	Real Service Status
1	eas-ssl-link	tcp	10.2.40.114	443	✓
2	eoas-ssl-link	tcp	10.2.40.113	443	✓

Figure 5:- SLB REAL SERVICES CONFIGURATION Screen

2. “**Add Real Service Entry**” screen is for you to configure real servers. In our example, we enter “**owa-cas-1**” as the Real Service Name. Select HTTP as Real Service type and enter IP addresses **10.10.10.11** and **port 80**.
3. Select the **HTTP** health check type for the real service and configure the related parameters for health check. Notice the parameter fields may vary with different health check types. Make certain you have set the “**Health Up Limit**” and “**Health Down Limit**” to **1**. This indicates how many times for application test fail/success to declare the Real Service is “Down” or “Up”.
4. Make certain you select the “**3 GET /owa/ HTTP/1.1\r\n\r\n**” and “**3 400 Bad Request**”.
5. Finish the creation of the real service and its health check configuration by clicking “**Save**” on the desired action link.

Real Services | **Health Check Setting**

ADD REAL SERVICE ENTRY Cancel | Save & Add Another | Save

REAL SERVICE SETUP [Enable this Service:]

Real Service Name: owa-cas-1

Real Service Type: http

Real Service IP: 10.10.10.11

Real Service Port: 80

Connection Limit: 1000

HEALTH CHECK SETUP

Health Check Type: http

Health Up Limit: 1 Health Down Limit: 1

Request Index: 3 GET /OWA HTTP/1.0\r\n\r\n

Response Index: 3 400 Bad Request

Figure 6:- Create Real Service for OWA

Follow the same steps: add “**owa-cas-2**” and “**owa-cas-3**” CAS servers as OWA real services.

Technical Notes:

Enable this Service: Check Box

To enabled or disabled the Real Service. If disabled, FortiBalancer will not dispatch new traffic to the Real Service.

Connection Limit: 1000

Set max connection to the real service. This setting helps with application stability without overloading the server or application. Increase the number if server is capable of handling greater loads.

Equivalent CLI Configuration:

```
slb real http "owa-cas-1" 10.10.10.11 80 1000 http 1 1
slb real http "owa-cas-2" 10.10.10.12 80 1000 http 1 1
slb real http "owa-cas-3" 10.10.10.13 80 1000 http 1 1

health server "owa-cas-1" 3 3
health server "owa-cas-2" 3 3
health server "owa-cas-3" 3 3
```

Create Outlook Web App Service Group

Outlook Web App Server Affinity

OWA client need affinity to the same Client Access Server, “insert cookie” (automatically added by the FortiBalancer) will be used as the persistent method and “RR” as the first choice method for requests without the “insert cookie” (first log-in requests).

Make certain you are in Config mode and select “**Groups**” from the sidebar [a]. The configuration window will display two tabs [b] **Groups** and **Groups Setting**.

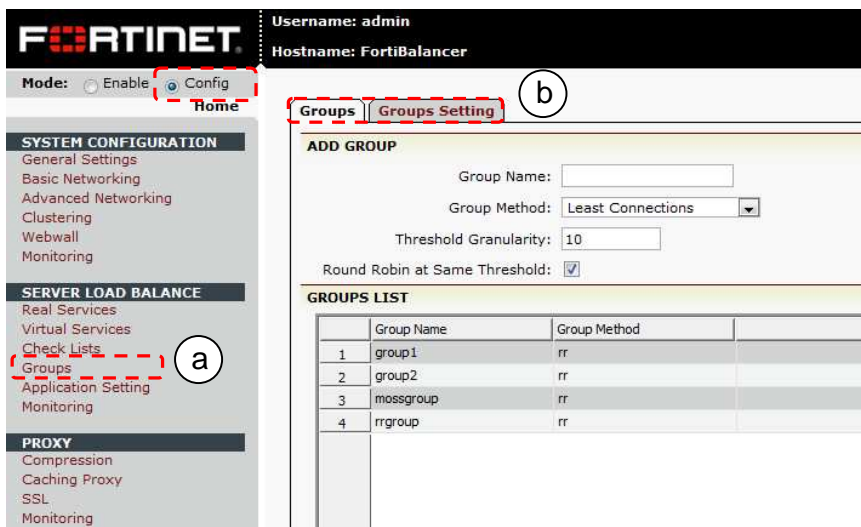


Figure 7:- Creating OWA SLB Group

1. Input the group name **owa_ic** [a]. Select “insert cookie” group method by selecting from the pull down menu [b]. Depending on which method is selected, certain parameter fields will change, appear, or disappear. Insert a random cookie name. In our example we insert “**nfmoahbgjx**” [c]. Select “**Round Robin**” group method by selecting from the pull down menu [d] and make certain to insert “1” in path flag [e]. After making configurations on those parameter fields, click on the action link “**Add**” [f]. The newly created “owa_ic” will be displayed in the sort ready table below [g]. Choose “owa_ic”

in the table and double click on it or click on the action link “**Edit**” [h]. A new configuration page will be displayed.

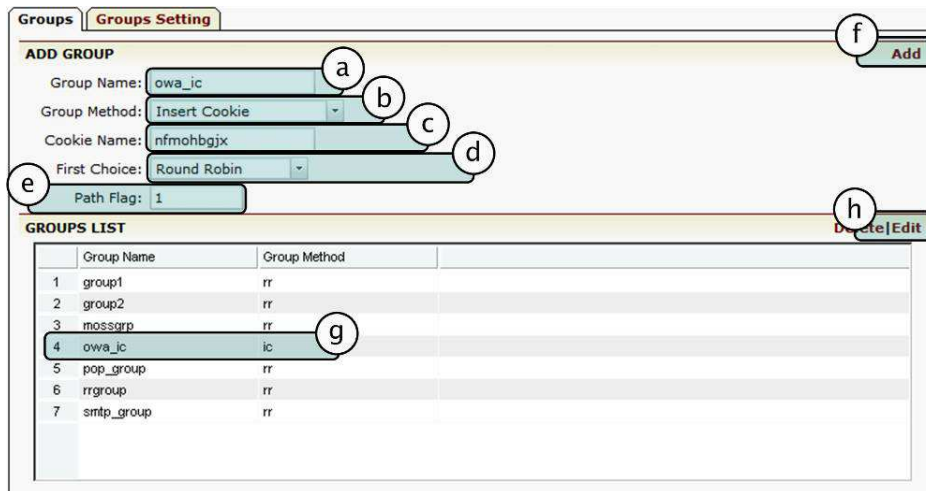


Figure 8:- Add Group for OWA

2. You can modify the group method and relevant configurations in the area [a]. Depending on which method is selected, certain parameter fields will change, appear, or disappear.
3. Under “GROUP MEMBERS” section, assign the configured real services **owa-cas-1**, **owa-cas-2**, and **owa-cas-3** to the newly created groups by using the pull down menu “**Eligible Reals**” [b]. Then, click on the “**Add**” action link [d] and the assigned real services “exchange_owa1” and “exchange_owa2” will appear in the display window [e].
4. Also at this page, there is a display window showing the current running statistics of the particular group [f].

Groups **Groups Setting** Cancel | Save

GROUP INFORMATION

Group Name: owa-ic Group Method: Insert Cookie
 Cookie Name: owa-cookie
 Path Flag: 1
 First Choice: Round Robin
 Keep group member configuration only:

** Note: Change group parameter may not success because of the compatibility among real service type, group method, policy and virtual service.
 For example:
 Group member and group method is not compatible: A group with TCP member can not change method from Round Robin to Insert Cookie.
 Group method and virtual service type is not compatible: A Hash Header method group can not associate with a FTP virtual service by any policy.
 Group method and policy is not compatible: A group with insert cookie method can not associate with virtual service by policies except default and insert cookie.*

GROUP SETTINGS Set | Clear

Number of Active Real Servers: 0 (1-65535)
 Persistence Timeout: Minutes (0-50000)

GROUP MEMBERS Add | Delete | Save

Eligible Reals: owa-cas-1
 Weight: 1
 Priority: 0

	Real Service Name	Weight	Priority	Active	Re
1	owa-cas-1	1	0	YES	
2	owa-cas-2	1	0	YES	
3	owa-cas-3	1	0	YES	
4	owa-cas-4	1	0	YES	

Figure 9:- Add OWA Group Members

Equivalent CLI Configuration

```
slb group method "owa-ic" ic "FortiBalancer-owa" 1 lc 10
slb group member "owa-ic" "owa-cas-1" 1 0
slb group member "owa-ic" "owa-cas-2" 1 0
slb group member "owa-ic" "owa-cas-3" 1 0
```

Create Outlook Web App Virtual Service

The next step is to create OWA Virtual Service for external OWA client to access. On the FortiBalancer appliance, a Virtual Service is defined by a Virtual IP/Port and the protocol. External client OWA requests will be terminated on it and the FortiBalancer appliance will load balance the requests to different OWA Real Services.

Make certain you are in the Config mode and have selected the feature link Virtual

Services from the sidebar [a]. The configuration ADD VIRTUAL SERVICE window will display four tabs [b]. The Virtual Services page is displayed by default.

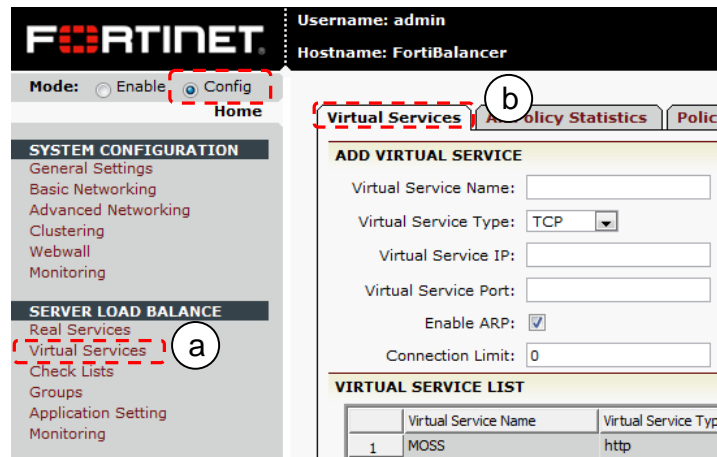


Figure 10:- Creating a Virtual Service

1. Enter “exchange_owa_virtual” [a] for the Virtual Service Name. Use the check box to enable the virtual service [b]. Select the virtual service type **http** from the selector [c]. Set the virtual service IP and port **80** [d]. Use the check box to enable ARP [e]. Set the maximum number of open connections per virtual service [f]. Depending on which type of virtual service is specified, certain parameter fields will appear, change or disappear. Click on the desired action link [g] to add a virtual service. Once a virtual service has been added, it will be displayed within the table. Select a virtual service in the table [h] and double click on it or click on the action link “Edit” [i]. A new configuration window will present a new series of tabs for completing virtual services configuration.

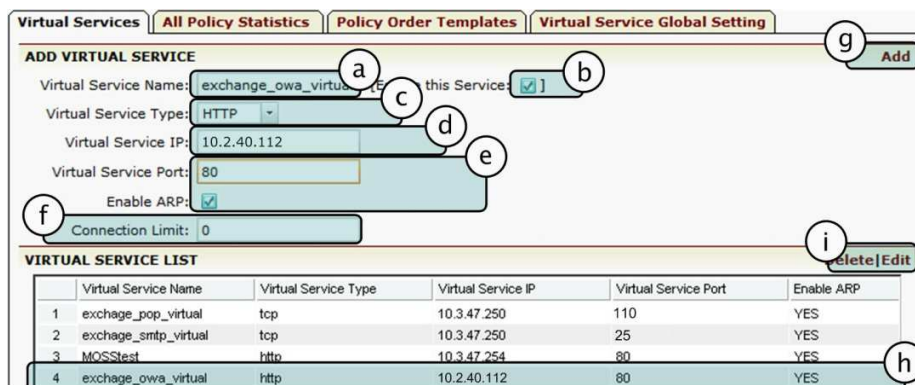


Figure 11:- Add Virtual Service for OWA (HTTPS)

2. Select the pre-created **owa_ic** [e] and set it to be the **icookie** policy [f], insert the policy name “**owa_ic_policy**” [g] and give **100** as the Policy

Precedence. Click the “Add” button to save this Virtual Service-SLB Group association [h]. The owa_ic will be shown in the ASSOCIATE GROUPS list [i].

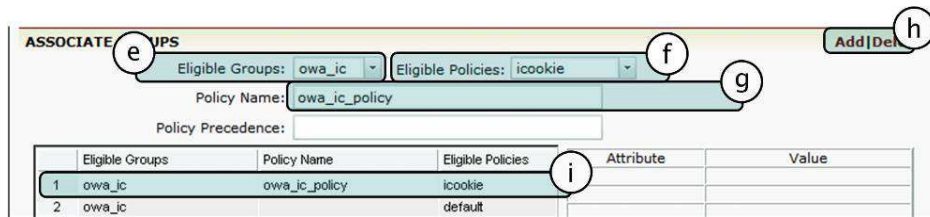


Figure 12:- Route Request to OWA SLB Group

3. Select the pre-created **owa_ic** [j] and set it to be the **default** policy [k]. Click the **add** button to save this Virtual Service-SLB Group association [l]. The owa_ic will be shown in the ASSOCIATE GROUPS list [m].

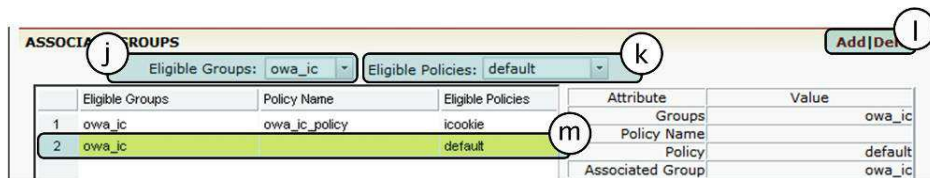


Figure 13:- Add Default Group

Equivalent CLI Configuration

```
slb virtual http "exchange_owa_virtual" 10.2.40.112 80 arp0
slb policy icookie "owa_ic_policy" "exchange_owa_virtual" "
owa-ic" 100
slb policy default exchange_owa_virtual owa-ic
```

Enable Outlook Web App SSL Offloading

The FortiBalancer appliance supports SSL acceleration for secured client access, offloads Exchange CAS SSL processing overhead (CPU/Memory) and provide centralized certificate management. Furthermore, the FortiBalancer appliance can be enabled to perform normal traffic management functions, such as cookie affinity, content routing, caching/compression and connection pooling acceleration functions, which cannot be supported with encrypted traffic.

To enable SSL for SLB Virtual Service:

- 1) Associate the SSL Virtual Host to the SLB Virtual Service
- 2) If the SSL Virtual Host is not fully configured:
 - a. Generate CSR (and Private Key)
 - b. Import Cert/Key (see example below)
- 3) Start the SSL Virtual Host

Following are the detailed configuration steps:

1. Selected the feature link **SSL** from the sidebar. Click **Virtual Hosts** tab, click **Add** button to enter the SSL Virtual Host window.
2. Add the SSL Virtual Host, enter “**exchange-ssl**” as the SSL Virtual Host Name and select “**owa-ssl**” from SLB Virtual Service. Then click **Save**.

Figure 14:- Bind SSL Virtual Host to a SLB Virtual Service

Note: Multiple SLB Virtual Services can be assigned to the same SSL Virtual Host. Up to 64 SLB Virtual Services can share the same SSL Virtual Host.

If SSL Virtual Host “**exchange-ssl**” is already with proper private key and certificate, jump to step 6 to start the SSL Virtual Host. Otherwise, import certificate and private key for the SSL Virtual Host “**exchange-ssl**”.

3. Select “**exchange-ssl**” to **Edit**.

	Virtual Host Name	SLB Virtual Service
1	exchange-ssl	owa-ssl

Figure 15:- Select & Edit New SSL Virtual Host

4. To import Exchange Server Certificate and Key, select “Import Cert/Key” and type in the local disk file for Local File or Manual Input.

Select SSL Virtual Host: exchange-ssl [Back to top menu]

Virtual Host CSR/Cert/Key **Virtual Host Settings**

CSR/Key **Import Cert/Key** Backup/Restore Cert/Key Import Client Cert/Key

SSL KEY [Using: Local File TFTP Manual Input] **Import**

Local File Path: G:\Download\exchange.rtf

Key Passphrase:

SSL CERTIFICATE [Using: Local File TFTP Manual Input] **Import**

Local File Path: G:\Download\exchange.rtf

Key Passphrase:

Note: You should input key passphrase when the format of a certificate is pfx, otherwise, keep it empty.

INTERMEDIATE CA CERTIFICATE [Using: Local File TFTP Manual Input] **Import**

Local File Path:

TRUSTED CA CERTIFICATE [Using: Local File TFTP Manual Input] **Import**

Note: This is used for Verifying Client Certificates

Local File Path:

CRL CA CERTIFICATE [Using: Local File TFTP Manual Input] **Import**

Local File Path:

Figure 16:- Import SSL Certificate & Private Key

- To enable SSL service, select “Virtual Host Settings”. Select the “Enable SSL” check box. The SSL will start.

Select SSL Virtual Host: exchange-ssl [Back to top menu]

Virtual Host CSR/Cert/Key **Virtual Host Settings**

Basic Settings **Advanced Settings**

SSL BASIC SETTINGS

Note: You need to generate a CSR or import a certificate and key before enabling SSL.

Enable SSL:

VIEW CERTIFICATE [Mode: Simple Complete]

Certificate 1:
 Issuer: C=US, ST=CA, L=Sunnyvale, O=Fortinet Inc., OU=FortiBalancerDemo, CN=www.fortinet.com, emailAddress=
 Validity

Figure 17:- Start the SSL Virtual Host with the selected Virtual Service

- Optional: For better security: Click Virtual Host Setting and Advanced Settings, advanced SSL features. Disable weak cipher “EXP-RC4-MD%” and “EXP-DES-CBC-SHA” so that no client can use those weak ciphers.

Select SSL Virtual Host: exchange-ssl [Back to top menu]

Virtual Host CSR/Cert/Key | Virtual Host Settings

Basic Settings | **Advanced Settings**

SSL ADVANCED SETTINGS

SSL Versions: SSLv3: TLSv1: TLSv1.1: TLSv1.2:

Enable Session Reuse:

Enable SSL Renegotiation:

CLIENT AUTHENTICATION

Enable Client Authentication:

Auth Cert Subject: (Optional)

Note:
1) You need to import the trusted CA certificate to enable client authentication.

CIPHER STRENGTH REDIRECTION

Minimum Acceptable Cipher Strength: No Minimum Cipher Strength Required 40 bits 56 bits 128 bits 168 bits 256 bits

Redirect URL:

CIPHER SUITES

Disabled Cipher Suites: EXP-RC4-MD5
EXP-DES-CBC-SHA

Enabled Cipher Suites: RC4-MD5
RC4-SHA
DES-CBC3-SHA
AES128-SHA
AES256-SHA
DES-CBC-SHA

>> << Move Up Move Down

Figure 18:- Figure 217 Advanced Setting for SSL

Equivalent CLI Configuration

```
ssl host virtual "exchange-ssl" "owa-ssl"
ssl settings ciphersuite "exchange-ssl" "RC4-MD5:RC4-SHA:DES-
CBC3-SHA:AES128-SHA:AES256-SHA:DES-CBC-SHA:!SSLv2:"
ssl settings protocol "exchange-ssl"
"SSLv3:TLSv1:TLSv1.1:TLSv1.2"
ssl start "exchange-ssl"
```

Enable Outlook Web App Rewrite/Redirect

Caching/Compression are default “on” for Virtual Service with type HTTP and HTTPS. OWA Virtual Service is with type HTTPS so that caching/compression are default “on”. You can select the check box to enable or disable cache and compression for a Virtual Service.

HTTP redirect to HTTPS

Client may type **http://...** (unsecured) rather than **https://...** to access secured OWA service. To make this more user friendly, the FortiBalancer appliance can be configured to auto redirect http request to https.

To configure the HTTP redirection:

1. Add a new Virtual Service “**owa**” for HTTP and virtual service port “**80**”.

Figure 19:- Create a HTTP Virtual Service for Redirect

2. Select the Virtual Service “**owa**” for Edit. Check the box for “Redirect All HTTP Requests to HTTPS”.

Figure 20:- Enable HTTP to HTTPS Redirect

Equivalent CLI Configuration

```
slb virtual http "owa" 10.2.40.112 80 arp 0
http redirect https "owa"
```

Request Rewrite

For OWA access, client may omit **/owa** directory which is needed by CAS to access **/owa** directory. The FortiBalancer appliance can be configured auto insert **/owa** if missing from client OWA request.

To configure:

1. Select Virtual Service “**owa-ssl**” for editing. Click URL Rewrite tab. Enter ‘**AddOWA**’ for Policy Name. “**100**” for Priority. “**owa.exchange.a.com**” as the host name (the external host name issued by client). Enter **^/\$** for Path Regex. “**^**” means start of the URI. “**\$**” means end of URI. In between only one “**/**”. Enter **/owa** for “Path Replacement”.

Select Virtual Service: owa-ssl [Back to top menu]

Virtual Service Settings | Virtual Service Statistics | URL Rewrite | URL Filter | HTTP Forwarding

HTTP REDIRECT Add|Delete

Policy Name: Priority: Response Code: 301

Original Protocol: https Host: Path Regex:

New Protocol: http Host: Path Replacement:

Policy Name	Priority	Host	Path Regex	New Protocol	Host	Path Replacement	Respon:

HTTP REWRITE REQUEST URL Add|Delete

Policy Name: AddOWA Priority: 100

Original Protocol: https Host: owa.exchange.a.com Path Regex: ^/\$

New Protocol: https Host: owa.exchange.a.com Path Replacement: /owa

Policy Name	Priority	Host	Path Regex	Host	Path Replacement
1	AddOWA	100	owa.exchange.a.... ^/\$	owa.exchange.a....	/owa

Figure 21:- Rewrite "/" to "/owa"

Equivalent CLI Configuration

```
http rewrite request url "owa-ssl" "AddOWA" 100
"owa.exchange.a.com" "^/$" "owa.exchange.a.com" "/owa
```

Enable Compression (cache optional)

On the FortiBalancer appliance, HTTP compression and/or caching are available for HTTP or HTTPS type of Virtual Services. Compression can reduce object size so less data is transmitted. Smaller/less data reduces transmission time for slow link makes OWA go faster. Also, better fit into monthly data quota and may reduce charge if data is metered.

To enable compression for the unit; select **Compression** under **PROXY** from the left pane. Make sure the "Enable Compression" check box is checked.

Setting | Type | Statistics

HTTP COMPRESSION SETTING Enable VS Compression|Disable VS Compression

Enable Compression:

HTTP/HTTPS Virtual Service(s): owa

COMPRESSION IS ENABLED FOR THE FOLLOWING HTTP/HTTPS VIRTUAL SERVICES:

Virtual service
1 owa
2 combined
3 eas-ssl
4 eoa-ssl
5 owa-ssl
6 owa-ssl-wan2

Figure 22:- Enable Compression

To enable compression (and others) for “owa-ssl” Virtual Service, from SERVER LOAD BALANCE; select **Virtual Services** on the left pane. Select “owa-ssl” from the VIRTUAL SERVICE LIST. Under “owa-ssl” VIRTUAL SERVICE SETTING, Compression, Cache and many other parameters are configurable. After entered or selected, do not forget to click “Save” to make the change(s) take effect.

Select Virtual Service: owa-ssl [Back to top menu]

Virtual Service Settings | Virtual Service Statistics | URL Rewrite | URL Filter | HTTP Forwarding

VIRTUAL SERVICE INFORMATION Cancel | Save

Virtual Service Name: owa-ssl Virtual Service Type: HTTPS

Virtual Service IP: 10.2.40.112

Virtual Service Port: 443

Enable ARP:

Connection Limit: 0

* Note: Change virtual service parameter will delete all original configuration of this virtual service: policy, URL rewrite, URL filter etc.

VIRTUAL SERVICE SETTING

TCP Timeout:

Enable OWA Support:

Additional HTTP Request Headers:

HTTP Client IP Headers:

Remove Port From Location Header:

Rewrite Redirections From Backend to Use HTTPS:

Enable data compression for this service:

Enable X-Forwarded-For for this service:

RegEx case mode: insensitive sensitive use global mode

Mode: Use System Mode Operate as Transparent Proxy Operate as Reverse Proxy

Enable this Service:

Enable Cache:

ASSOCIATE GROUPS Add | Delete

Virtual Service Or Vlink: owa-ssl

Figure 23:- Enable/Disable Compression per Virtual Service

Configuring FortiBalancer for Outlook Anywhere

Exchange Outlook Anywhere for Exchange 2010 allows you to use Outlook 2007 and Outlook 2003 clients to connect to your Exchange Server environment over the Internet, using HTTPS to encapsulate RPC traffic.

Note: Encapsulate RPC traffic is incompatible with normal HTTP traffic.

By using the FortiBalancer appliance in front of Outlook Anywhere server farm, you gain High Availability and improved user experience benefits:

- Load balance and monitor application availability to ensure high-availability across multiple Outlook Anywhere servers.
- SSL offload for improved client performance, reduced server load and simplify SSL Certificate management.
- Alleviate security concerns, such as DDoS/Spike.

Configuration Steps

Create Outlook Anywhere Service Health Check

Built-in HTTP health check can be used to check the following RPC link that needed for EOA RPC and without any credential input, the server shall return 401 (or 403).

<http://domain.com/rpc/rpcproxy.dll>

To customize Health Check, select Real Services, Health Check Setting. Edit Request Index "8" and Response Index "8". Enter "GET /rpc/rpcproxy.dll HTTP/1.0/r/n/Host: domain.com/r/n/r/n" for Request String. And "401" for the Response String.

The screenshot shows the 'Health Check Setting' configuration page in the FortiBalancer interface. The page has a title bar with 'Real Services' and 'Health Check Setting' tabs, and 'RESET' and 'SAVE CHANGES' buttons. The main content area is titled 'HEALTH CHECK SETTING' and contains the following fields:

- Enable Health Check:
- Health Check Interval(seconds): 5
- Server Timeout(seconds): 5
- Enable Failover:
- Retries Before Failover: 3
- Request Index: 8
- Request String: GET /rpc/rpcproxy.dll HTTP/1.0/r/n/Hos
- Existing Requests: 8 GET /rpc/rpcproxy.dll HTTP/: [Delete] [Clear]
- Response Index: 8
- Response String: 401
- Existing Responses: 8 401: [Delete] [Clear]

Figure 24:- Outlook Anywhere Health Check

Create Outlook Anywhere Real Service

Same as add OWA Real Services into the unit. Add 3 Real Services “**eoacas-1**”, “**eoacas-2**” and “**eoacas-3**” to the unit.

Note: The real service type is TCP, however, the Health Check Type is HTTP and Index 8 is used for both Request and Response.

Figure 25:- Create Real Service for Outlook Anywhere

Equivalent CLI Configuration

```
slb real tcp "eoacas-1" 10.10.10.11 443 1000 http 3 3
slb real tcp "eoacas-2" 10.10.10.12 443 1000 http 3 3
slb real tcp "eoacas-3" 10.10.10.13 443 1000 http 3 3

health server "eoacas-1" 8 8
health server "eoacas-2" 8 8
health server "eoacas-3" 8 8
```

Create Outlook Anywhere Service Group

Outlook Anywhere Server Affinity

Outlook Anywhere client does not support cookie. . The “chi” (Constant Hash IP) method can be used for server affinity. “chi” will also provides server persistency in the event of FortiBalancer failover.

However; “chi” may not effective for load balancing when inbound connections come through a small number of NAT devices. In that case, RPCHTTP LBS component in Windows may be used to handle RPCHTTP connection affinity – see Microsoft TechNet for further information.

Selected the feature link **Groups** from the sidebar. ADD GROUP window will be displayed.

1. Enter **“group-OutlookAnywhere”** as OutlookAnywhere SLB Group Name. Select **“LC”** for Group Method. Click **“Add”**. **“group-OutlookAnywhere”** should be displayed within the GROUPS LIST.
2. GROUPS LIST table contains all SLB Groups in the unit. Select **“group-OutlookAnywhere”** and click **“Edit”** (or double click) to enter individual Group configuration window.

Figure 26:- Create SLB Group for Outlook Anywhere

3. Under GROUP MEMBERS window, select Eligible Reals **“eoa-cas-1”**, **“eoa-cas-2”** and **“eoa-cas-3”**, and click **Add** button to add to the group one by one.

	Real Service Name	Weight	Priority	Active	Reason
1	eoa-cas-1	1	0	YES	
2	eoa-cas-2	1	0	YES	
3	eoa-cas-3	1	0	YES	

Figure 27:-Add Real Service to SLB Group

Equivalent CLI Configuration –

```
slb group method "group-OutlookAnywhere" lc
slb group member "group-OutlookAnywhere" "eoa-cas-1" 1 0
slb group member "group-OutlookAnywhere" "eoa-cas-2" 1 0
slb group member "group-OutlookAnywhere" "eoa-cas-3" 1 0
```

Create Outlook Anywhere Virtual Service

1. Click **Virtual Services** link from the left function list. Enter **“eoa-ssl”** for Virtual Service Name. Select **“TCPS”** as the Virtual Service Type. Enter IP **“10.2.40.114”** and Port **“443”**.

Figure 28:- Create Virtual Service for Outlook Anywhere

- From Virtual Service List, select **eo-a-ssl** for **Edit**. Under ASSOCIATE GROUP, select “**g-OutlookAnywhere**” for Eligible Vlink Or Group and “**default**” for the Eligible policy. Then click **Add** button.

Figure 29:- Associate with g-OutlookAnywhere Group with default policy

Equivalent CLI Configuration –

```
slb virtual tcps "eoa-ssl" 10.2.40.114 443 arp 0
slb policy default "eoa-ssl" "group-OutlookAnywhere"
```

Enable Outlook Anywhere SSL Offloading

Note: To configure SSL offloading for Outlook Anywhere please refer to the following link from Microsoft TechNet.

<http://technet.microsoft.com/en-us/library/aa998346.aspx>

To enable SSL for SLB Virtual Service “**eo-a-ssl**”, SSL Virtual Host need be added. Go to SSL-> Virtual Hosts -> Add. Enter “**exchange-ssl**” SSL Virtual Host and select “**eo-a-ssl**” SLB Virtual Service. Click **Save**.

Global Settings	SSL Errors	Virtual Hosts	Real Hosts
SSL VIRTUAL HOST Cancel Save & Add Another Save			
Virtual Host Name: <input type="text" value="exchange-ssl"/>			
SLB Virtual Service: <input type="text" value="eoa-ssl"/>			
<div style="border: 1px solid gray; padding: 5px; font-size: small;"> If you can't select SLB Virtual Service, please go to Server Load Balancing->Virtual Services page to add https/tcps virtual service first. </div>			

Figure 30:- Add SSL Virtual Host for Outlook Anywhere Virtual Service

As “**exchange-ssl**” SSL Virtual Host already had its Key/Certificate imported and is Enabled (running), no other setup is needed. Clients will be able to access **eoa-ssl** Virtual Service now.

Equivalent CLI Configuration –

```
ssl host virtual "exchange-ssl" "eoa-ssl"
```

Configuring the FortiBalancer Appliance for ActiveSync

Exchange ActiveSync is a Microsoft Exchange synchronization protocol that is optimized to work together with high-latency and low-bandwidth networks. The protocol, based on HTTP and XML, enables mobile phone users access to corporate information on the Microsoft Exchange environment. Exchange ActiveSync enables mobile phone users to access their e-mail, calendar, contacts and tasks, and to continue to be able to access this information while they are working offline.

By deploying the FortiBalancer appliance in front of ActiveSync-enabled servers you gain better security for TCP SYNC and DDoS attacks, and the advantages of intelligent load balancing, SSL/TLS offloading, and ease of certificate management.

As with Outlook Anywhere, many of the the FortiBalancer appliance configuration procedures for ActiveSync are nearly identical to the procedures for Outlook Web App. Since ActiveSync main clients are Mobile Phone Applications, cookies may not support. Also, since ActiveSync application information transaction is single connection based, multiple connections affinity to the same server may not be required. Normal Round Robin or Least Connection Load Balancing should be efficient enough to support Active Sync. Furthermore, since ActiveSync event may take extended time for new events to happen, connection timeouts need to be extended.

Configuration Steps

Create ActiveSync Service Health Check

ActiveSync service application health check can be done by sending HTTP request to virtual directory and checking the response content. For more accurate application health check, the following request string "HEAD /Microsoft-Server-ActiveSync/ HTTP/1.1\r\nHost: mail.domain.com\r\n" can be sent. Also, depending on your CAS server setup, the response string "401 Authorization Required" can be checked.

Real Services Health Check Setting RESET SAVE CHANGES

HEALTH CHECK SETTING

Enable Health Check:

Health Check Interval(seconds): 5

Server Timeout(seconds): 5

Enable Failover:

Retries Before Failover: 3

Request Index: 6 Request String: HEAD /Microsoft-Server-ActiveSync

Existing Requests: 0 HEAD / HTTP/1.0\r\n\r\n Delete Clear

Response Index: 0 Response String: 401 Authorization Required

Existing Responses: 0 200 OK Delete Clear

Health Earlywarning: 0 (0-60000 milliseconds) Clear

Figure 31:- Configure Health Check

Create ActiveSync Real Service

This is the same as adding OWA Real Services. Add Real Services “**eas-cas-1**” to the unit. Select HTTP as the Health Check Type. Select Index 6 as Request Index and Response Index. Index 6 will check “/Microsoft-Sever-ActiveSync” virtual directory. The same as “**eas-cas-2**” and “**eas-cas-3**”.

The screenshot shows the 'ADD REAL SERVICE ENTRY' window with the following configuration:

- REAL SERVICE SETUP**
 - Real Service Name: eas-cas-1
 - Real Service Type: http
 - Real Service IP: 10.10.10.1
 - Real Service Port: 80
 - Connection Limit: 1000
- HEALTH CHECK SETUP**
 - Health Check Type: http
 - Health Up Limit: 3
 - Health Down Limit: 3
 - Request Index: 6 HEAD /Microsoft-Sever-ActiveSync HTTP/1.0\r\n\r\n
 - Response Index: 401 Authorization Required

Figure 32:- Creating ActiveSync Real Services

Equivalent CLI Configuration –

```
slb real http "eas-cas-1" 10.10.10.11 80 1000 http 3 3
slb real http "eas-cas-2" 10.10.10.12 80 1000 http 3 3
slb real http "eas-cas-3" 10.10.10.13 80 1000 http 3 3

health server "eas-cas-1" 5 6
health server "eas-cas-2" 6 6
health server "eas-cas-3" 6 6
```

Create ActiveSync Service Group

Selected the feature link **Groups** from the sidebar. ADD GROUP window will be displayed.

1. Enter “**group-eas**” as ActiveSync SLB Group Name. Select “**Least Connections**” for Group Method. Click “**Add**”. “**group-eas**” should be displayed within the GROUPS LIST.

Groups | Groups Setting

ADD GROUP Add

Group Name:

Group Method:

Threshold Granularity:

Round Robin at Same Threshold:

GROUPS LIST Delete | Edit

Figure 33:- Add Group for Exchange ActiveSync

- GROUPS LIST table contains all SLB Groups in the unit. Select “**group-eas**” and click “Edit” (or double click) to enter individual Group configuration window. Under GROUP MEMBERS window select Eligible Reals “**eas-cas-1**”, “**eas-cas-2**” and “**eas-cas-3**” and click **Add** button to add to the group one by one.

GROUP MEMBERS Add | Delete | Save

Eligible Reals:

Weight:

Priority:

	Real Service Name	Weight	Priority	Active	Reason
1	eo-a-cas-1	1	0	YES	
2	eo-a-cas-2	1	0	YES	
3	eo-a-cas-3	1	0	YES	

Figure 34:- Add Member to ActiveSync Group

Equivalent CLI Configuration –

```
slb group method "group-eas" ic "FortiBalancer-eas" 0 lc 10
slb group member "group-eas" "eas-cas-1" 1 0
slb group member "group-eas" "eas-cas-2" 1 0
slb group member "group-eas" "eas-cas-3" 1 0
```

Create ActiveSync Virtual Service

Selected the feature link **Virtual Services** from the sidebar. **ADD VIRTUAL SERVICE** window will be displayed.

- Enter “**eas-ssl**” for Virtual Service Name. Select **HTTPS** for Virtual Service Type. Enter Virtual Service IP “**10.2.40.113**” and Port “**443**”. Click Add. “**eas-ssl**” shall be displayed within the **VIRTUAL SERVICE LIST** table.
- VIRTUAL SERVICE LIST** table contains Virtual Services in the unit. Select “**eas-ssl**” and click “Edit” (or double click) to enter individual Virtual Service configuration window.

Virtual Services | All Policy Statistics | Policy Order Templates | Virtual Service Global Setting

ADD VIRTUAL SERVICE Add

Virtual Service Name: [Enable this Service:]

Virtual Service Type:

Virtual Service IP:

Virtual Service Port:

Enable ARP:

Connection Limit:

VIRTUAL SERVICE LIST Delete | Edit

	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP
1	rpc	tcp	10.2.40.112	0	YES
2	smtp	tcp	10.2.40.112	25	YES
3	smtp-wan-2	tcp	192.168.1.112	25	YES
4	owa	http	10.2.40.112	80	YES
5	combined	https	10.2.40.115	443	YES
6	eas-ssl	https	10.2.40.113	443	YES
7	eoas-ssl	https	10.2.40.114	443	YES
8

Figure 35:- Add ActiveSync Virtual Service

3. ASSOCIATE GROUPS: For Virtual Service eas-ssl, select **group-eas** from Eligible Groups and select **icookie** from Eligible Policies. Enter “**eas-policy-1**” for Policy Name and **100** for Policy Precedence. Click **Add**. Do the similar for “**default**” Eligible Policy.

ASSOCIATE GROUPS Add | Delete

Virtual Service Or VLink:

Eligible Groups: Eligible Policies:

	Eligible VLink Or Groups	Policy Name	Eligible Policies	Attribute	Value
1	group-eas		default		

Figure 36:- Associate group-eas to Virtual Service

Equivalent CLI Configuration –

```
slb virtual https "eas-ssl" 10.2.40.113 443 arp 0
slb policy default "eas-ssl" "group-eas"
```

Enable ActiveSync SSL Offloading

To enable SSL for SLB Virtual Service “**eas-ssl**”, SSL Virtual Host needs to be added. Go to SSL-> Virtual Hosts -> Add. Enter “**exchange-ssl**” SSL Virtual Host and select “**eas-ssl**” SLB Virtual Service. Click **Save**.

Global Settings | SSL Errors | Virtual Hosts | Real Hosts

SSL VIRTUAL HOST Cancel | Save & Add Another | Save

Virtual Host Name:

SLB Virtual Service:

If you can't select SLB Virtual Service, please go to Server Load Balancing->Virtual Services page to add https/tcps virtual services

Figure 37:- Enable SSL Offloading for ActiveSync

Equivalent CLI Configuration –

```
ssl host virtual "exchange-ssl" "eas-ssl"
```

As “**exchange-ssl**” SSL Virtual Host already had its Key/Certificate imported and is Enabled (running), no other setup is needed. Client shall be able to access **eas-ssl** Virtual Service now.

Note: For more information on configure SSL offloading for Exchange 2010 please refer to the following link from Microsoft TechNet.

<http://technet.microsoft.com/en-us/library/bb124558.aspx>

Misc – Change TCP Idle Timeout

ActiveSync uses Direct Push technology which issues a long-lived HTTPS request to Exchange for any mailbox change for the next x-minutes. For optimal Direct Push performance, Microsoft recommended increases the TCP time-out to 30 minutes. The FortiBalancer appliance default TCP idle timeout is 300 seconds (5 minutes, for whole unit). Each Virtual Service can have its own TCP timeout.

For more information on ActiveSync and Direct Push, see the Microsoft documentation.

<http://technet.microsoft.com/en-us/library/aa998357.aspx>

<http://technet.microsoft.com/en-us/library/aa997252.aspx>

To configure TCP timeout for individual Virtual Service, click **Virtual Services** from the left function list, and double click “**eas-ssl**” from the VIRTUAL SERVICE LIST for edit. Enter “**1800**” (30 minutes) for TCP Timeout.

VIRTUAL SERVICE SETTING

TCP Timeout:

Enable OWA Support:

Additional HTTP Request Headers:

HTTP Client IP Headers:

Remove Port From Location Header:

Rewrite Redirections From Backend to Use HTTPS:

Enable data compression for this service:

Enable X-Forwarded-For for this service:

Mode: Use System Mode Operate as Transparent Proxy Operate as Reverse Proxy

Enable this Service:

Enable Cache:

Figure 38:- Change TCP timeout to 30 minutes

Equivalent CLI Configuration –

```
slb timeout "eas-ssl" 1800
```

Configuring the FortiBalancer Appliance for RPC Client Access

RPC Client Access service was introduced with Exchange Server 2010 to support Microsoft Outlook client use MAPI RPC to access the mailbox through the CAS server, instead of directly to the mailbox servers. This change applies business logic to clients more consistently and provides a better client experience when CAS failover occurs.

The FortiBalancer appliance can load balance incoming MAPI connections to multiple Client Access servers. With L4 port range SLB, multiple port range or static ports can be specified for client access. In addition, health checks can be added for better RPC Client Access service availability. Unlike most of the other Client Access server roles, the RPC Client Access service does not allow FortiBalancer SSL offloading.

NOTE:

By default Windows Server 2008 and 2008 R2 are configured with a dynamic RPC range of 49152- 65535 for outbound connections. Earlier versions of Windows Server by default used port 1025-65535 (for more details reference Microsoft KB article: [The default dynamic port range for TCP/IP has changed in Windows Vista and in Windows Server 2008](#)). When Exchange 2010 Client Access server role is installed on Windows Server 2008 or 2008 R2, the dynamic RPC port range is changed to 6005-59530 and the highest usable port number is set to 60554.

However, dynamic port could cause issues with firewalls. To avoid these issues Static Port for RPC services is recommended by Exchange Server 2010. If you want to utilize Static Port, be sure you have correctly configured the RPC services of Exchange Server (for detail, please reference this link <http://social.technet.microsoft.com/wiki/contents/articles/configure-static-rpc-ports-on-an-exchange-2010-client-access-server.aspx>)

Besides port 135, we also need to know predefined Static Port for Client Access Service, Address Book Service and Public Folders. Then the TCP virtual service can be created for each port and these virtual services can be bind with the corresponding CAS real servers.

The following describes both the more complicated dynamic port configuration and the simpler setup for static ports for the RPC Client Access.

Dynamic Port Configuration Steps

Create RPC Client Access Service Health Check

The RPC service will be configured as raw TCP service so that the basic TCP health check will be used. Also, as RPC service is with multiple ports, Additional Health Check with main port (135) will be added to check after RPC Client Access Real Service is defined.

Create RPC Client Access Real Service

Create a Real Service for each Exchange RPC server. Enter “**rpc-cas-1**” as Real Service Name. Enter the IP address and “0” for Real Service Port. The port 0 means the FortiBalancer will initiate the connection with the same port that client is destined to. Select “**icmp**” as Health Check Type. Also, for RPC Real Service “**rpc-cas-2**” and “**rpc-cas-3**”.

The screenshot shows the 'Real Services' configuration page with the 'Health Check Setting' tab selected. The 'ADD REAL SERVICE ENTRY' section includes a 'REAL SERVICE SETUP' area with the following fields: Real Service Name (rpc-cas-1), Real Service Type (tcp), Real Service IP (10.10.10.11), Real Service Port (0), and Connection Limit (1000). Below this is the 'HEALTH CHECK SETUP' area with Health Check Type (icmp) and Health Up/Down Limits (both 3). Buttons for 'Cancel', 'Save & Add Another', and 'Save' are visible at the top right.

Figure 39:- Add RPC Client Access Real Service

Add additional health for RPC Client Access service. Select the Real Service and click “Additional Health Check” tab. Enter the IP address and the port 135 for TCP health check. This means ... ICPM + TCP worked and FortiBalancer will decide the RPC service is OK.

The screenshot shows the 'Edit Real Service' configuration page with the 'Additional Health Check' tab selected. The 'ADDITIONAL HEALTH CHECK RELATION' section has radio buttons for 'or' and 'and', with 'and' selected. The 'ADD ADDITIONAL HEALTH CHECK' section includes fields for Real Service Name (rpc-cas-1), Real Service Type (tcp), Health Check IP (10.10.10.11), Health Check Port (135), Type (tcp), and Health Up/Down Limits (both 3). Buttons for 'Cancel' and 'Add' are visible at the top right. Below is the 'ADDITIONAL HEALTH CHECK LIST' section with a table header and a 'Delete' button.

Real Service Name	Health Check IP	Health Check Port	Health Check Type	Real Service Stat
-------------------	-----------------	-------------------	-------------------	-------------------

Figure 40:- Add Additional Health Check for RPC Real

Equivalent CLI Configuration –


```

slb real tcp "rpc-cas-1" 10.10.10.11 0 1000 icmp 3 3
slb real health "rpc-cas-1" 10.10.10.11 135 tcp 3 3
slb real tcp "rpc-cas-2" 10.10.10.11 0 1000 icmp 3 3
slb real health "rpc-cas-2" 10.10.10.12 135 tcp 3 3
slb real tcp "rpc-cas-3" 10.10.10.11 0 1000 icmp 3 3
slb real health "rpc-cas-3" 10.10.10.13 135 tcp 3 3

```

Create RPC Client Access Service Group

RPC Client Access Server Affinity

For RPC Client Access Server Affinity the recommended persistence method is by Client IP. We will use CHI (Constant Hash IP) method which also provides server affinity the event of a FortiBalancer failover.

Select “Groups” from left pane. ADD GROUP, enter a Group Name “group-rpc” and select Group Method with “Consistent Hash IP”. Click “Add” to enter “group-rpc”.

Figure 41:- Add SLB Group for RPC Client Access

Add Real Service **rpc-cas-1**, **rpc-cas-2** and **rpc-cas-3** to the SLB Group “**group-rpc**”.

	Real Service Name	Weight	Priority	Active	Reason
1	rpc-cas-1	1	0	YES	
2	rpc-cas-2	1	0	YES	
3	rpc-cas-3	1	0	YES	

Figure 42:- Add Real Service to RPC SLB Group

Equivalent CLI Configuration –

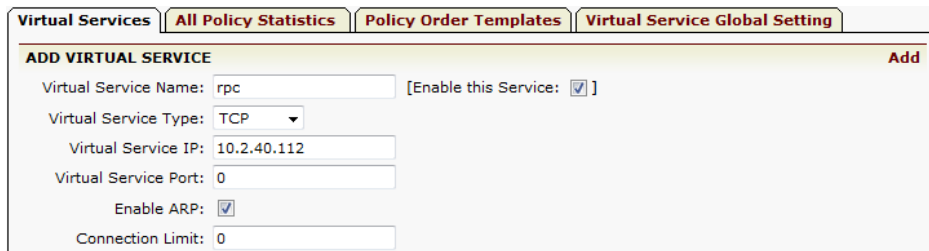
```

slb group method "group-rpc" chi 32
slb group member "group-rpc" "rpc-cas-1" 1 0
slb group member "group-rpc" "rpc-cas-2" 1 0
slb group member "group-rpc" "rpc-cas-3" 1 0

```

Create RPC Client Access Virtual Service

Select “Virtual Services” from left function list. ADD VIRTUALSERVICE, enter a Virtual Service Name “**rpc**”, the Virtual Service IP “**10.10.40.112**”. Enter “**0**” for Virtual Service Port. Port “0” means all ports. Then click “**Add**” to create the “rpc” Virtual Service.



Virtual Services | All Policy Statistics | Policy Order Templates | Virtual Service Global Setting

ADD VIRTUAL SERVICE Add

Virtual Service Name: [Enable this Service:]

Virtual Service Type:

Virtual Service IP:

Virtual Service Port:

Enable ARP:

Connection Limit:

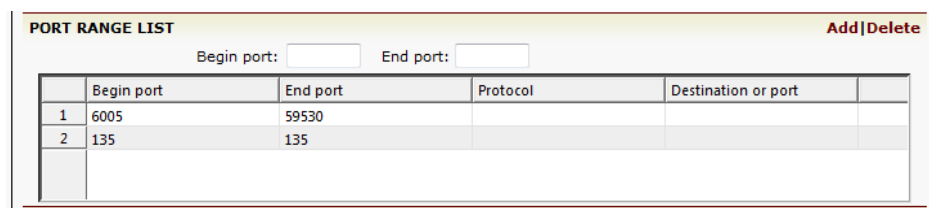
Figure 43:- RPC Client Access Virtual Service

Technical Note for RPC Ports:

An IP port is an opening through which information can pass from the originating computer to the destination computer. By default, the dynamic port range for outgoing connections on Windows Server 2008 R2 is 49152 to 65535. **Exchange 2010 Client Access changes this range to 6005 through 59530.** The range was expanded to provide sufficient scaling for large deployments. This is a large range of ports to balance through your firewall between the client and the Client Access servers or Client Access array.

<http://technet.microsoft.com/en-us/library/ee332317.aspx>

To only enable needed ports for RPC Client Access. Select the “rpc” Virtual Service for Editing. From PORT RANGE LIST, add port range **135** (range 135-135) and **6005 to 59530**. Client access with unspecified ports will not be severed.



PORT RANGE LIST Add | Delete

Begin port: End port:

	Begin port	End port	Protocol	Destination or port
1	6005	59530		
2	135	135		

Figure 44:- Specify Port Range for RPC Client Access Virtual Service (Dynamic Ports)

Configuring static ports for the RPC Client Access service

Note:

For static ports for the RPC client access, Microsoft recommends you set this to a unique value between 59531 and 60554 and use the same value on all CAS in any one AD site. For example, uses 59532 for the RPC Client Access service and 59533 for the Address Book service. In this case , it is needed to add port

range 59532 (range 59532 -59532) and port range 59533(range 59533-59533) into the PORT RANGE LIST. As a result, the port range list will be changed to Figure 57 .:

PORT RANGE LIST					Add Delete
Begin port:		End port:			
	Begin port	End port	Protocol	Destination or port	
1	135	135			
2	59532	59532			
3	59533	59533			

Figure 45:- Specify Port Range for RPC Client Access Virtual Service (Static Ports)

To direct the RPC traffic for RPC Virtual Service to RPC SLB group, select the “rpc” and under ASSOCIATE GROUPS, select “group-rpc” and “default” for Eligible Policies.

ASSOCIATE GROUPS					Add Delete
Eligible Vlink Or Groups:		group-rpc	Eligible Policies: default		
	Eligible Groups	Policy	Eligible Poli	Attribute	Value
1	group-rpc	group-rpc	default		

Figure 46:- SLB Group for RPC Client Access Virtual Service

Equivalent CLI Configuration – (Dynamic Ports)

```
slb virtual tcp "rpc" 10.2.40.112 0 arp 0
slb virtual portrange "rpc" 6005 59530
slb virtual portrange "rpc" 135 135
slb policy default "rpc" "group-rpc"
```

Equivalent CLI Configuration – (Static Ports)

```
slb virtual tcp "rpc" 10.2.40.112 0 arp 0
slb virtual portrange "rpc" 59532 59532
slb virtual portrange "rpc" 59533 59533
slb virtual portrange "rpc" 135 135
slb policy default "rpc" "group-rpc"
```

Configuring the FortiBalancer Appliance for POP3

POP3 enables a variety of clients to connect to the Exchange Server environment. These include Outlook, Outlook Express, and third-party clients such as Eudora or Mozilla Thunderbird.

The FortiBalancer appliance shall perform the following functions:

- Load Balancing based on Least Connection
- POP3 application health check with basic TCP health check
- SSL offloading to reduce CAS server load

Configuration Steps

Create POP3 Service Health Check

For a simple check, we will utilize existing TCP protocol health check for POP3 service.

Create POP3 Real Service

Create Real Service for each CAS real server. Enter “**pop3-cas-1**”, “**pop3-cas-2**”, and “**pop3-cas-3**” as Real Service Name. Select **TCP** for Real Service Type. Enter IP address and port **110**.

Note: Port 995 can be used for the real service if the CAS server is also running SSL.

Real Services | Health Check Setting

ADD REAL SERVICE ENTRY Cancel | Save & Add Another | Save

REAL SERVICE SETUP [Enable this Service:]

Real Service Name: pop3-cas-1

Real Service Type: tcp

Real Service IP: 10.10.10.11

Real Service Port: 110

Connection Limit: 1000

HEALTH CHECK SETUP

Health Check Type: tcp

Health Up Limit: 3 | Health Down Limit: 3

Figure 47:- POP3 Real Service

Equivalent CLI Configuration

```

slb real tcp "pop3-cas-1" 10.10.10.11 110 1000 tcp 3 3
slb real tcp "pop3-cas-2" 10.10.10.12 110 1000 tcp 3 3
slb real tcp "pop3-cas-3" 10.10.10.13 110 1000 tcp 3 3

```

Create POP3 Service Group

POP3 application does not require server affinity. "Least Connection" will be used for load balancing. To configure the POP3 SLB Group, selected the feature link **Groups** from the sidebar. ADD GROUP window will be displayed.

1. Enter "**group-pop3**" as Group Name. Select "**Least Connections**" for Group Method. Click "**Add**". "**group-pop3**" should be displayed within the GROUPS LIST.
2. GROUPS LIST table contains all SLB Groups in the unit. Select "**group-pop3**" and click "Edit" (or double click) to enter individual Group configuration window.

The screenshot shows the 'Groups Setting' interface. Under 'ADD GROUP', the 'Group Name' field contains 'group-pop3', the 'Group Method' dropdown is set to 'Least Connections', and the 'Threshold Granularity' field is '10'. The 'Round Robin at Same Threshold' checkbox is checked. Below this is a 'GROUPS LIST' table with columns for Group Name and Group Method. It lists two groups: 'group-OutlookAnywhere' (method: chi) and 'group-eas' (method: ic).

Figure 48:- Create SLB Group for POP3 Real Service

3. Add Real Service **pop3-cas-1**, **pop3-cas-2** and **pop3-cas-3** to the SLB Group "**group-pop3**".

The screenshot shows the 'GROUP MEMBERS' configuration window. The 'Eligible Reals' dropdown is set to 'pop3-cas-1'. The 'Weight' field is '1' and the 'Priority' field is '0'. Below is a table with columns: Real Service Name, Weight, Priority, Active, and Reason. It lists three real services: 'pop3-cas-1', 'pop3-cas-2', and 'pop3-cas-3', all with a weight of 1, priority of 0, and active status.

Figure 49:- Add Real Service to POP3 SLB Group

Equivalent CLI Configuration

```

slb group method "group-rpc" lc 10 yes
slb group member "group-pop3" "pop3-cas-1" 1 0

```

```
slb group member "group-pop3" "pop3-cas-2" 1 0
```

Equivalent CLI Configuration

```
slb group member "group-pop3" "pop3-cas-3" 1 0
```

Create POP3 Virtual Service

Selected the feature link **Virtual Services** from the sidebar. ADD VIRTUAL SERVICE window will be displayed.

1. Enter **pop3-ssl** for Virtual Service Name. Select **TCPS** for Virtual Service Type. Enter Virtual Service IP **10.2.40.112** and Port **995**. Click Add. **pop3-ssl** shall be displayed within the VIRTUAL SERVICE LIST table.
2. VIRTUAL SERVICE LIST table contains Virtual Services in the unit. Select **pop3-ssl** and click **Edit** (or double click) to enter individual Virtual Service configuration window.

The screenshot shows the 'Virtual Services' configuration page. The 'ADD VIRTUAL SERVICE' form is filled with the following values: Virtual Service Name: pop3-ssl, Virtual Service Type: TCPS, Virtual Service IP: 10.2.40.112, Virtual Service Port: 995, Enable ARP: checked, and Connection Limit: 0. Below the form is a table titled 'VIRTUAL SERVICE LIST' with the following data:

	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP
1	pop3-ssl	tcps	10.2.40.112	995	YES
2	imand-ssl	tcps	10.2.40.112	995	YES

Figure 50:- Create POP3S Virtual Service

3. Select **group-pop3** for Eligible Vlink Or Groups and **default** for Eligible Policies.

The screenshot shows the 'ASSOCIATE GROUPS' configuration window. The 'Eligible Vlink Or Groups' dropdown is set to 'group-pop3' and the 'Eligible Policies' dropdown is set to 'default'. Below these are two tables:

	Eligible Groups	Policy Name	Eligible Policies
1	group-pop3		default

Attribute	Value
Groups	group-pop3
Policy Name	

Figure 51:- Associate SLB Group to POP3 Virtual Service

Equivalent CLI Configuration

```
slb virtual tcps "pop3-ssl" 10.2.40.112 995 arp 0
slb policy default "pop3-ssl" "group-pop3"
```

Enable POP3 SSL Offloading

To enable SSL for SLB Virtual Service “**pop3-ssl**”, SSL Virtual Host need be added. Go to SSL-> Virtual Hosts -> Add. Enter “**exchange-ssl**” SSL Virtual Host and select “**pop3-ssl**” SLB Virtual Service. Click **Save**.

Global Settings | SSL Errors | Virtual Hosts | Real Hosts

SSL VIRTUAL HOST Cancel | Save & Add Another | Save

Virtual Host Name:

SLB Virtual Service:

If you can't select SLB Virtual Service, please go to Server Load Balancing->Virtual Services page to add https/tcps virtual service first.

Figure 52:- Add SSL Virtual Host for POP3 Secured Access

Equivalent CLI Configuration

```
ssl host virtual "exchange-ssl" "pop3-ssl"
```

As “**exchange-ssl**” SSL Virtual Host already has its Key/Certificate imported and is Enabled (running) no other setup is needed. Client shall be able to access **pop3-ssl** Virtual Service for now.

Configuring the FortiBalancer Appliance for IMAP4

Configuring the FortiBalancer Appliance for IMAP4

IMAP4 enable a variety of clients to connect to the Exchange Server environment. These include Outlook, Outlook Express, and third-party clients such as Eudora or Mozilla Thunderbird.

The FortiBalancer appliance shall perform the following functions:

- Load Balancing based on Least Connection
- IMAP application health check with basic TCP health check
- SSL offloading (optional)

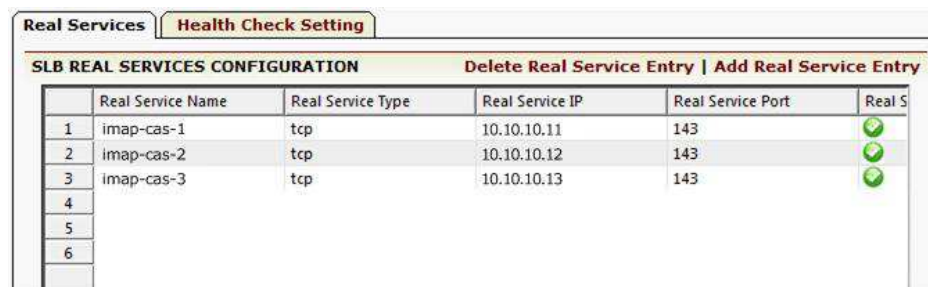
Configuration Steps

Create IMAP4 Service Health Check

Default basic TCP protocol health check will be used for this example. Based on Client Access Server setup, Additional Health Check and/or Script Application Health Check can be added for more reliable application availability check.

Create IMAP4 Real Service

Follow the same instruction that were used to add OWA Real Services to add IMAP Real Services on CAS. We give different Real Service name as “imap-cas-1”, “imap-cas-2” and “imap-cas-3”. The protocol is TCP and the port address is 143.



The screenshot shows the 'SLB REAL SERVICES CONFIGURATION' interface. It has two tabs: 'Real Services' and 'Health Check Setting'. The 'Real Services' tab is active. At the top right of the table area, there are links for 'Delete Real Service Entry' and 'Add Real Service Entry'. The table has six columns: 'Real Service Name', 'Real Service Type', 'Real Service IP', 'Real Service Port', and 'Real S'. There are three rows of data, each with a green checkmark in the 'Real S' column. The rows are: 1. imap-cas-1, tcp, 10.10.10.11, 143; 2. imap-cas-2, tcp, 10.10.10.12, 143; 3. imap-cas-3, tcp, 10.10.10.13, 143. Below the table are empty rows numbered 4, 5, and 6.

	Real Service Name	Real Service Type	Real Service IP	Real Service Port	Real S
1	imap-cas-1	tcp	10.10.10.11	143	✓
2	imap-cas-2	tcp	10.10.10.12	143	✓
3	imap-cas-3	tcp	10.10.10.13	143	✓
4					
5					
6					

Figure 53:- Create Real Service for IMAP4

Equivalent CLI Configuration

```
slb real tcp "imap-cas-1" 10.10.10.11 143 1000 tcp 3 3
slb real tcp "imap-cas-2" 10.10.10.12 143 1000 tcp 3 3
slb real tcp "imap-cas-3" 10.10.10.13 143 1000 tcp 3 3
```

Create IMAP4 Service Group

IMAP application does not require server affinity, "Least Connection" can be used for load balancing. To configure the IMAP SLB Group, selected the feature link **Groups** from the sidebar. ADD GROUP window will be displayed.

1. Enter "**group-imap**" as Group Name. Select "**Least Connections**" for Group Method. Click "**Add**". "**group-imap**" should be displayed within the GROUPS LIST.
2. GROUPS LIST table contains all SLB Groups in the unit. Select "**group-eas**" and click "Edit" (or double click) to enter individual Group configuration window.

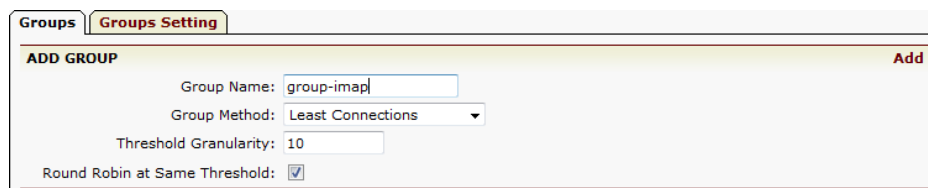
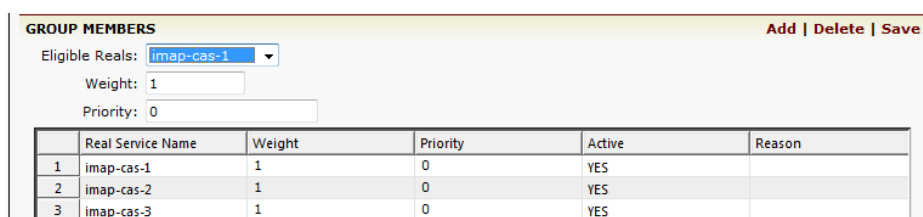


Figure 54:- Create SLB Group for IMAP4

3. GROUPS MEMBERS, add Real Service **imap-cas-1**, **imap-cas-2** and **imap-cas-3** to the SLB Group "**group-imap**".



	Real Service Name	Weight	Priority	Active	Reason
1	imap-cas-1	1	0	YES	
2	imap-cas-2	1	0	YES	
3	imap-cas-3	1	0	YES	

Figure 55:- Add Real Service to IMAP SLB Group

Equivalent CLI Configuration

```
slb group method "group-imap" lc 10 yes
slb group member "group-imap" "imap-cas-1" 1 0
```

```
slb group member "group-imap" "imap-cas-2" 1 0
```

```
slb group member "group-imap" "imap-cas-3" 1 0
```

Create Secures IMAP4 Virtual Service

Select the feature link **Virtual Services** from the sidebar. ADD VIRTUAL SERVICE window will be displayed.

1. Enter **imap4-ssl** for Virtual Service Name. Select **TCP** for Virtual Service Type. Enter Virtual Service IP **10.2.40.12** and Port **993**. Click Add. **imap4-ssl** shall be displayed within the VIRTUAL SERVICE LIST table.
2. VIRTUAL SERVICE LIST table contains Virtual Services in the unit. Select **imap4-ssl** and click **Edit** (or double click) to enter individual Virtual Service configuration window.

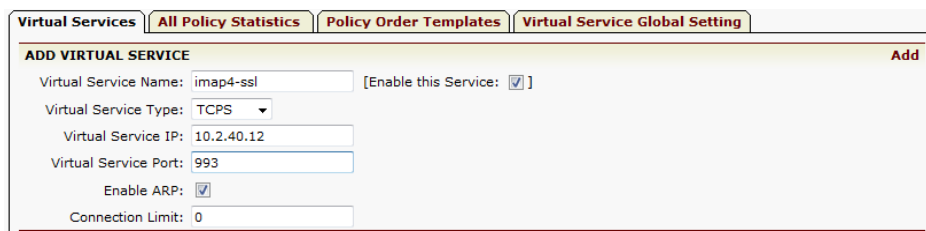


Figure 56:- Virtual Service for IMAP4

3. Select **group-imap** for Eligible Vlink or Groups and **default** for Eligible Policies.

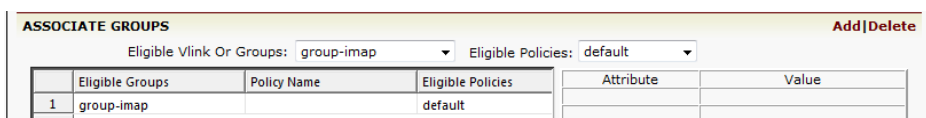


Figure 57:- Associate SLB Group to IMAP Virtual Service

Equivalent CLI Configuration

```
slb virtual tcp "imap4-ssl" 10.2.40.12 993 arp 0  
slb policy default "imap4" "group-imap"
```

Enable IMAP4 SSL Offloading

To enable SSL for SLB Virtual Service **imap4-ssl**, SSL Virtual Host needs to be

added. Go to SSL-> Virtual Hosts -> Add. Enter “**exchange-ssl**” SSL Virtual Host and select “**imap4-ssl**” SLB Virtual Service. Click **Save**.

Global Settings | SSL Errors | Virtual Hosts | Real Hosts

SSL VIRTUAL HOST Cancel | Save & Add Another | Save

Virtual Host Name:

SLB Virtual Service:

If you can't select SLB Virtual Service, please go to Server Load Balancing->Virtual Services page to add https/tcps virtual service first.

Figure 58:- SSL Virtual Host for IMAP4 Secured Access

Equivalent CLI Configuration

```
ssl host virtual "exchange-ssl" "pop3-ssl"
```

As “**exchange-ssl**” SSL Virtual Host already has its Key/Certificate imported and is Enabled (running) no other setup is needed. Client shall now be able to access **imap4-ssl** Virtual Service.

Configuring the FortiBalancer Appliance for SMTP (Edge Transport)

In Microsoft Exchange Server 2010, the Edge Transport server role is deployed at organization's perimeter network. Designed to minimize the attack surface, the Edge Transport server handles all Internet-facing mail flow, which provides SMTP relay and smart host services for the Exchange environment. Additional layers of message protection and security are provided by a series of agents that run on the Edge Transport server and act on messages as they are processed by the message transport components. These agents support the features that provide protection against viruses and spam and apply transport rules to control message flow.

The FortiBalancer appliance can spread the load among Edge Transport Servers and detect failure for SMTP high availability.

Also, the FortiBalancer appliance can provide TLS (SRATRTTLS) offload to reduce CPU and memory usage on CAS.

Configuration Steps

Access WebUI, make certain in "Config" mode. Left side is selectable feature links.

Create SMTP (Edge Transport) Service Health Check

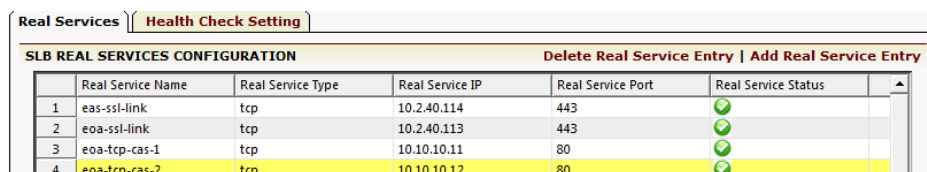
Default basic TCP protocol health check will be used for the example. Based on Edge Transport Server setup, Additional Health Check and/or Script Application Health Check can be added for more reliable application availability check.

Create SMTP (Edge Transport) Real Service

Note: SMTP Server Affinity is not required.

Select the feature link **Real Services** from the sidebar.

1. The default page is **Real Services/Health Check Setting**. To create Real Service for SMTP, click "**Add Real Service Entry**" to enter ADD REAL SERVICE ENTRY window. (Figure 7.1)



Real Services		Health Check Setting				
SLB REAL SERVICES CONFIGURATION					Delete Real Service Entry	Add Real Service Entry
	Real Service Name	Real Service Type	Real Service IP	Real Service Port	Real Service Status	
1	eas-ssl-link	tcp	10.2.40.114	443	✓	
2	eoas-ssl-link	tcp	10.2.40.113	443	✓	
3	eoas-tcp-cas-1	tcp	10.10.10.11	80	✓	
4	eoas-tcp-cas-2	tcp	10.10.10.12	80	✓	

Figure 59:- Real Services/Health Check Setting

- Under ADD REAL SERVICE ENTRY window, enter “**mail-smtp1**” for Real Service Name. Select “**tcp**” as Real Service Type. Enter Real Service IP and Port (25 for SMTP). Click “**Save**”.

Figure 60:- Create Real Service for SMTP

- Do the similar for “**mail-smtp2**”.

Equivalent CLI Configuration

```
slb real tcp "mail-smtp1" 10.10.20.11 25 9999 tcp 1 3
slb real tcp "mail-smtp2" 10.10.20.12 25 9999 tcp 1 3
```

Create SMTP (Edge Transport) Service Group

Selected the feature link **Groups** from the sidebar. ADD GROUP window will be displayed.

- Enter “**group-smtp-et**” for Edge Proxy Group Name. Select “**Consistent Hash IP**” for Group Method. Click “Add”. “**group-smtp-et**” should be displayed within the GROUPS LIST.
- GROUPS LIST table contains all SLB Groups in the unit. Select “**group-smtp-et**” and click “Edit” (or double click) to enter individual Group configuration window.

Figure 61:- Create Service Group for SMTP

- GROUP MEMBERS: select “**mail-smtp1**” and “**mail-smtp2**” from Eligible Reals to **Add** to group and click “**Save**”.

Real Service Name	Weight	Priority	Active	Reason
1 mail-smtp1	1	0	YES	
2 mail-smtp2	1	0	YES	

Figure 62:- Add Group Member to SMTP Group

Equivalent CLI Configuration

```
slb group method "group-smtp" chi 32
slb group member "group-smtp" "mail-smtp1"
slb group member "group-smtp" "mail-smtp2"
```

Create SMTP (Edge Transport) Virtual Service

Selected the feature link **Virtual Services** from the sidebar. **ADD VIRTUAL SERVICE** window will be displayed.

- Enter “**smtp**” for Virtual Service Name. Select **TCP** for Virtual Service Type. Enter Virtual Service IP “**10.2.40.112**” and Port “**25**” (SMTP). Click Add. “**smtp**” shall be displayed within the VIRTUAL SERVICE LIST table.
- VIRTUAL SERVICE LIST table contains Virtual Services in the unit. Select “**smtp**” and click “Edit” (or double click) to enter individual Virtual Service configuration window.

Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP
1 rpc	tcp	10.2.40.112	0	YES
2 smtp	tcp	10.2.40.112	25	YES

Figure 63:- Add Virtual Service for SMTP

- VIRTUAL SERVICE SETTING: Select “Operate as Transparent Proxy”. For Transparent Proxy, client IP will be used to make TCP connection to Edge

Transport servers so that Edge Transport servers may use client IP for its policy use (such as for white/black list).

4. ASSOCIATE GROUPS: Select **group-smtp-et** from Eligible Groups and select **default** from Eligible Policies. Click Add button to enter. The **group-smtp-et** will be displayed within the ASSOCIATE GROUPS list.

Select Virtual Service: smtp [Back to top menu]

Virtual Service Settings | Virtual Service Statistics | URL Rewrite | URL Filter | HTTP Forwarding

VIRTUAL SERVICE INFORMATION Cancel | Save

Virtual Service Name: smtp Virtual Service Type: TCP

Virtual Service IP: 10.2.40.112

Virtual Service Port: 25

Enable ARP:

Connection Limit: 0

* Note: Change virtual service parameter will delete all original configuration of this virtual service: policy, URL rewrite, URL filter etc.

VIRTUAL SERVICE SETTING

TCP Timeout:

Mode: Use System Mode Operate as Transparent Proxy Operate as Reverse Proxy Operate as Triangle Proxy

Enable this Service:

ASSOCIATE GROUPS Add | Delete

Eligible Vlink Or Groups: group-smtp-et Eligible Policies: default

	Eligible Groups	Policy Name	Eligible Policies	Attribute	Value
1	group-smtp-et		default		

Figure 64:- Virtual Service Setting for SMTP

Equivalent CLI Configuration

```
slb virtual tcp "smtp" 10.2.40.112 25 arp 0
slb policy default "smtp" "group-smtp-et"
system mode transparent "smtp"
```

Enable SMTP (Edge Transport) SSL Offloading

The FortiBalancer appliance can be configured to provide SMTP TLS (STARTTLS) access. For the SMTP TLS Virtual Service, the Virtual Service Type will be TCPS and can be port 25 or an unused port (please inform your client).

Misc SMTP Outbound Support

To enable internal SMTP servers to transport emails to other internet SMTP email servers, NATing will need to be setup on the FortiBalancer.

Select **Advanced Networking** feature tab, click **Add NAT Port**

NAT **Port Forwarding**

ADD NAT PORT Cancel | Save & Add Another | Save

Virtual IP:

Network IP:

Netmask:

Timeout: (Seconds)

Gateway:

Figure 65:- Add NAT Port

Equivalent CLI Configuration

```
nat port 10.2.40.112 10.10.20.8 255.255.255.248 60 10.2.1.1
```


Configuring the FortiBalancer Appliance for Link Redundancy Using LLB

To increase the bandwidth and improve application access availability in case the ISP/WAN link goes down a second ISP/WAN link is recommended.

FortiBalancer Link Load Balancing (LLB) is an integrated feature which manages multiple ISP/WAN links through link health check for automatically failover, policy based routing and link load balancing.

To utilize multiple ISP/WAN links, multiple Virtual Services (redundant) need be added to facility client access through different link (ISP IP) for Exchange 2010, and each IP can be added to the DNS as different DNS A Record for the same domain name.

<u>Record FQDN</u>		<u>Record Type</u>	<u>Record Value</u>
owa.domain.com	A		10.2.40.112
owa.domain.com	A		192.168.1.112

For SMTP, SMTP redundancy is built-in with DNS multiple MX records. Multiple MX records for a domain can be added to a DNS server. Each MX record can be assigned with preference.

<u>Record FQDN</u>		<u>Record Type</u>	<u>Record Value</u>	<u>MX Pref.</u>
domain.com		MX	mail1.domain.com.	10
domain.com		MX	mail2.domai.com.	20
mail1.domain.com	A		10.2.40.112	
mail2.domain.com	A		192.168.1.112	

For outbound email, the FortiBalancer appliance policy based routing can be used to speed up mail delivery for specific target and failover when needed.

Following is a configuration steps for how to setup multiple link (multi-home) access for Exchange 2010 mail service.

Configuration Steps

Add additional port for WAN-2 access

Config -> Basic Networking -> Port

To make port 2 usable for the second WAN link, select “port2” and enter static IP “192.168.1.21” and Static Mask 255.255.255.0.

The screenshot shows the configuration page for a Port. The 'INTERFACE SETTINGS' section is visible, with the following values: Port ID: port2, Name: port2, Port Speed: auto (selected), MTU: 1500, Static IP Address: 192.168.1.21, and Static Netmask: 255.255.255.0. There are also buttons for 'RESET' and 'SAVE CHANGES'.

Figure 66:- Add additional interface for WAN 2

Add Duplicate Virtual Service for WAN 2 access

This setup is the same as previous examples to create SLB Virtual Services. In this example, we add Virtual Service. smtp-wan-2, imap4-ssl-wan2, pop3-ssl-wan2 and owa-ssl-wan2.

The screenshot shows the 'VIRTUAL SERVICE LIST' table. The table has columns for Virtual Service Name, Virtual Service Type, Virtual Service IP, Virtual Service Port, and Enable A. The last four entries are highlighted in red:

	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable A
7	smtp-ssl	tcps	10.2.40.112	465	YES
8	eas-ssl	https	10.2.40.113	443	YES
9	eoas-ssl	https	10.2.40.114	443	YES
10	combined	https	10.2.40.115	443	YES
11	oa-tcps	tcps	10.2.40.116	443	YES
12	smtp-wan-2	tcp	192.168.1.112	25	YES
13	imap4-ssl-wan2	tcps	192.168.1.112	993	YES
14	pop3-ssl-wan2	tcps	192.168.1.112	995	YES
15	owa-ssl-wan2	https	192.168.1.115	443	YES

Figure 67:- List of redundant SLB Virtual Service

The new SLB Virtual Services added for “wan-2” shall use the same SLB group as the other Virtual Service for WAN 1.

Virtual Service Name	Related Groups	Related Real Services
owa-ssl	group-owa-ic	owa-cas-1
		owa-cas-2
		owa-cas-3

Figure 68:- owa-ssl (WAN-1)

Virtual Service Name	Related Groups	Related Real Services
owa-ssl-wan2	group-owa-ic	owa-cas-1
		owa-cas-2
		owa-cas-3

Figure 69:- owa-ssl-wan2 (WAN-2)

Create LLB Links information

Link Load Balance -> OutBound Settings -> Add

Enter a unique name “wan-1” for the Link Name. Enter IP address “10.2.1.1” as the gateway IP address (external router IP address) of this LLB link. Enter “10.2.1.11” as the Health check destination IP. LLB health check will continuous sending ICMP requests to the assigned Health Check destination IP address via the link “wan-1”. Enter “10” for the Interval. This is the time interval of LLB health check. Enter “1” for the Weight of the Link (optional). Assign “10.2.40.111” as the Health Check source IP. This is the IP address assigned as the source IP of the LLB health check IP. Click “Save”.

InBound Settings	OutBound Settings	Statistics	Report
<p>ADD LINK ROUTE Cancel Save & Add Another Save</p> <p>Link Name: wan-1</p> <p>GateWay IP: 10.2.1.1</p> <p>Health Check IP: 10.2.1.11</p> <p>Interval: 10 (Seconds)</p> <p>Weight: 1</p> <p>Health Check Source IP: 10.2.40.111</p>			

Figure 70:- Create LLB Link

For WAN link 2, enter a unique name “wan-2” for the Link Name. IP address “192.168.1.11”. Enter “12.12.12.12” as the Health check destination IP (just for example). Enter “10” for the Interval (default). Enter “1” for the Weight (default). And click “Save”.

InBound Settings | OutBound Settings | **Statistics** | Report

LLB LINK GLOBAL SETTINGS

Method: Round Robin

Enable Link Health Check:

LLB LINK ROUTE Edit | Delete | Add

	Link Name	GateWay IP	Health Check IP	Interval	Weight	Enable	Health Che
1	wan-1	10.2.1.1	10.2.1.11	10	1	<input checked="" type="checkbox"/>	10.2.1.111
2	wan-2	192.168.1.11	12.12.12.12	10	1	<input checked="" type="checkbox"/>	192.168.1.2

Figure 71:- LLB Link Information

Equivalent CLI Configuration

```
llb link route "wan-1" 10.2.1.1 10.2.1.11 2 1
llb link route "wan-2" 192.168.1.11 12.12.12.12 10 1
```

Create LLB DNS record for inbound traffic

Link Load Balance -> Inbound Settings -> Add

ADD DNS ENTRY window will appear. Enter **owa.domain.com** for the Host Name and IP address **10.2.40.115** (this is the IP of the A record) and Port **443**. This is the same as SLB Virtual Service "owa-ssl" IP and Port and will be accessed through "wan-1" link. Enter **1** for the Weight (default). Click **Save**.

InBound Settings | OutBound Settings | **Statistics** | Report

ADD DNS ENTRY Cancel | Save & Add Another | Save

Host Name: owa.domain.com

IP: 10.2.40.115

Port: 443

Weight: 1

Figure 72:- Create domain name and Service IP

Based on the IP and Port entered, LLB will try to match local SLB Virtual/Real Service configured in LLB system. If a match is found, LLB will utilize SLB health check status for the Virtual/Real Service as corresponding IP status (UP/DOWN). If no match, the IP configured is assumed "UP" (like normal DNS). LLB DNS only resolves the "UP" IP to the client DNS queries.

The name "owa.domain.com" is the domain name that user entered in their browser to access Outlook Web App.

For link “wan-2”, enter “**owa.domain.com**” for the host name and IP address “**192.168.1.115**” and Port “**443**”. Enter “**1**” for the Weight. Click “**Save**”.

DNS LOAD BALANCE				
Method: Round Robin				
DNS ENTRIES				
	Host Name	IP	Port	Weight
1	owa.domain.com	192.168.1.115	443	1
2	owa.domain.com	10.2.40.115	443	1

Figure 73:- Domain name and Service IP list

Equivalent CLI Configuration

```
llb dns host "owa.domain.com" 192.168.1.115 1 443  
llb dns host "owa.domain.com" 10.2.40.112 1 443  
llb dns ttl "owa.domain.com" 60
```

Configuring the FortiBalancer Appliance for Exchange 2010 Site Resilience Using GSLB

Exchange 2010 may be deployed with a backup site in separate geographic locations, with mailbox data synchronized between the two sites and with the ability for one of the sites to take on the entire load if the other fails. Exchange 2010 uses database availability groups (DAGs) to keep multiple copies of your mailboxes on different servers synchronized.

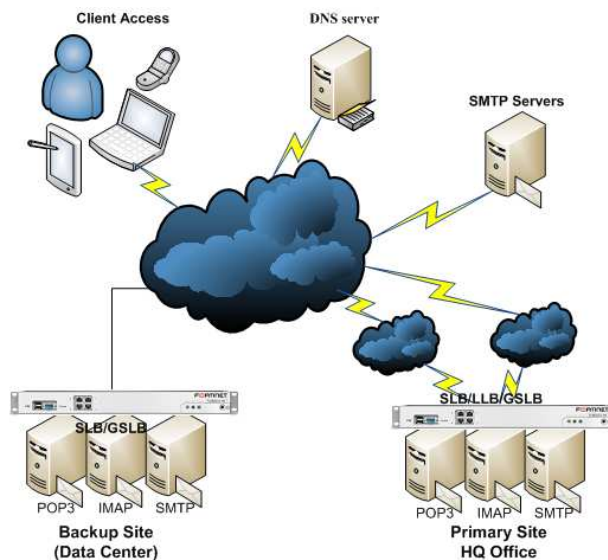


Figure 74:- Global Load Balancing for Exchange 2010

Fault Tolerance Configuration

In case your mail server fails you are still able to receive incoming e-mail messages. Most small to medium sized companies will pay their ISPs a monthly fee for storage space on the ISP's mail servers. For that to happen, a new MX Record will be added to their DNS information, pointing to the ISP's mail server with a higher priority. For example:

Record FQDN	Record Type	Record Value	MX Pref.
mail.domain.net	MX	mail1.domain.com	10
mail.domain.net	MX	mail2.domain.com.	20

Normally clients from Internet accesses "mail.domain.com" for mailbox access and the request is sent to the Primary site. In the event the Primary site down, the mail access switches automatically to the Backup Site.

Note: FortiBalancer GSLB/SDNS supports BIND9. Named and zone file can be imported to FortiBalancer for DNS use. The zone file can include MX record for client access.

For non-SMTP clients or other Exchange Services, client may type "owa.domain.com" for its mailbox access and regular DNS query for "owa.domain.com" A record. Normal DNS can resolve "owa.domain.com" to HQ-link1-ip1 or round-robin with HQ-Link2-IP2 so that traffic will stay on the Primary Site. If one link is down, approximately 50% of access will need to be restarted as normal DNS does not care if the Link or Primary Site is down. In the case Primary Site is down, to switch to the Backup Site, client need type a different name, such as "owa2.domain.com" to access the backup site to continue to access email service.

With *FortiBalancer* GSLB/SmartDNS, in case HQ-link1 (or HQ-link2) goes down, the SmartDNS can resolve "owa.domail.com" to the health IP and Exchange traffic will stay on the Primary Site. Also, once the Primary Site both links are down (or Exchange is down/disabled under maintenance), SmartDNS at both sites or on the Data Center (backup site) can resolve "owa.domain.com" to the Data Center IP so that mail access can through Backup Site. This shall give higher email serviceability and a more user friendly (single "owa.domail.com").

Configuration Steps

Define GSLB/SDNS Members

GSLB/SDNS Members are typical FortiBalancers which exchange status with other SDNS members in a GSLB/SDNS networks. To create SDNS Member from WebUI:

Global Load Balance -> General Settings -> Add Member Entry

Type "HQ-FortiBalancer1" for the Name, select "all" for the Type. Enter "10.2.40.111"

for the IP address and “5888” as the Port. Click **Save & Add Another** to add “DC-FortiBalancer1” member.

Figure 75:- Create SDNS Member

Note: SDNS Member Type can be:

- **Proxy** - serve with SLB function and report VIP/RIP health and load to SDNS members
- **DNS** - serve with DNS server
- **All** - Proxy + DNS

From SDNS MEMBER SETTING, check the Local Member radius button to assign the member as the Local Member.

SDNS MEMBER SETTINGS							
Delete Member Entry Add Member Entry							
	Name	Type	IP Address	Port	Max Connections	Status	Local Member
1	HQ-APV1	all	10.2.40.111	5888	1000	UP	<input checked="" type="radio"/>
2	DC-APV1	all	192.168.40.111	5888	1000	DOWN	<input type="radio"/>

Figure 76:- SDNS Member List

Creating GSLB Records

To add domain name A Records for SDNS to manage.

Global Load Balance -> Records

Enter “**pop3.domain.com**” for the Domain Name and type in the IP/port information. Or select the Virtual Service or Real Service from the available list. Click **Save**.

ADD A RECORDS Save

Domain Name:

IP: Port: Weight:

Name ▲	Service Flag	IP	Port	Weight
pop3-cas-1	Real	10.10.10.11	110	1
pop3-cas-2	Real	10.10.10.12	110	1
pop3-cas-3	Real	10.10.10.13	110	1
pop3-ssl	Virtual	10.2.40.112	995	1
pop3-ssl-wan2	Virtual	192.168.1.112	995	1

Figure 77:- Create A Record

General Settings **Records** **Topology** **Methods** **Bandwidth** **DPS** **IANA** **Statistics** **Report**

A Cname Others IPv6 SNMP IP Delete

A RECORDS

Domain Name:

	Host Name ▲	IP	Port	Weight	Service	Health Check
1	imap.domain.com	10.2.40.112	993	1	Virtual: imap4-ssl	
2	imap.domain.com	192.168.1.112	993	1	Virtual: imap4-ssl-wan2	
3	owa.domain.com	10.2.40.115	443	1	Virtual: combined	
4	owa.domain.com	192.168.1.115	443	1	Virtual: owa-ssl-wan2	
5	pop3.domain.com	192.168.1.112	995	1	Virtual: pop3-ssl-wan2	
6	pop3.domain.com	10.2.40.112	995	1	Virtual: pop3-ssl	

Figure 78:- List of A-Record

GSLB/SDNS Disaster Recovery Site Location

Site Location for Disaster Recovery is collection of members. A GSLB/SDNS network can contain multiple sites. To create a Site Location:

Global Load Balance -> **Topology** -> **Site** (Default) -> **Add Site Entry**

Enter **“Primary-HQ”** as the given Site and **“100”** for Weight. Click **Save & Add Another** to Add **“Backup-DC”**.

General Settings **Records** **Topology** **Methods** **Bandwidth** **DPS** **IANA** **Statistics** **Report**

Site Region Proximity Over Flow Chain DR Group Cancel | Save & Add Another | Save

ADD SITE ENTRY

Site:

Weight:

Figure 79:- Create a SDNS Site

To add member to the selected site:

Select the “Primary-HQ” site by click the View. Click **Edit Members of the Site** and SDNS SITE’S (Member) LIST windows will display.

General Settings							Records		Topology		Methods		Bandwidth		DPS		IANA		Statistics		Report		
Site	Region	Proximity	Over Flow Chain	DR Group																			
SDNS SITE SETTINGS																						Delete Site Entry Add Site Entry	
Site	Weight	Members	View																				
1	Backup-DC	100	1	<input type="radio"/>																			
2	Primary-HQ	100	1	<input checked="" type="radio"/>																			
MEMBERS OF THE SELECTED VIEW																						Delete Member Edit Members of the Site	
Name	IP Address	Status																					
1	HQ-APV1	10.2.40.111	(L)																				

Figure 80:- Edit Members of the Site

Under SDNS SITE’S (Member) LIST windows, check the “Is Site Member” box for member belonging to the “Primary-HQ” site. Click **Save**.

General Settings							Records		Topology		Methods		Bandwidth		DPS		IANA		Statistics		Report		RESET	SAVE
Site	Region	Proximity	Over Flow Chain	DR Group																				
SDNS SITE’S LIST																								
Name	IP Address	Status	Is Site Member																					
HQ-APV1	10.2.40.111	(L)	<input checked="" type="checkbox"/>																					
DC-APV1	192.168.40.111	all	<input type="checkbox"/>																					

Figure 81:- Site Members List

Creating DR Group with DNS domain name

Global Load Balance -> Topology -> DR Group

Type “**mail-pop3**” for Group Name (any unique name) and “**pop3.domain.com**” for the Domain Name. The Domain name is the name that client used to access the service. Click **Add DR Group**. Enter all domain names that will be supported by the DR site.

General Settings							Records		Topology		Methods		Bandwidth		DPS		IANA		Statistics		Report		
Site	Region	Proximity	Over Flow Chain	DR Group																			
SDNS DRGROUP SETTINGS																						Delete DrGroup Add DrGroup	
Group Name:		mail-xxxx																					
Domain Name:		xxxx.domain.com																					
Group Name	Domain Name	Primary Status	Standby Status	Switch On	View Sites																		
1	mail-pop3	pop3.domain.com	Active	Inactive	<input type="checkbox"/>	<input checked="" type="radio"/>																	
2	mail-imap	imap.domain.com	Active	Inactive	<input type="checkbox"/>	<input type="radio"/>																	
3	mail-owa	owa.domain.com	Active	Inactive	<input type="checkbox"/>	<input type="radio"/>																	

Figure 82:- Add DR Group

FortiBalancer GSLB/SDNS Disaster Recover supports two Site Groups - “Primary” and “Standby”. To assign sites to Primary Site Group:

1. For Service Group Name mail-pop3, check the “View Sites” radius. All available “Site” should show to serve the Group.
2. Select the “**Primary**” from Select Group/SiteView. Check To Current Group box for Primary-HQ Site. Click **Save Group Site Setting**.
3. Select the “**Backup**” from Select Group/SiteView. Check To Current Group box for Backup-DC Site. Click **Save Group Site Setting**.
4. Repeat step 1, 2 and 3 for Service group mail-imap and mail-owa.

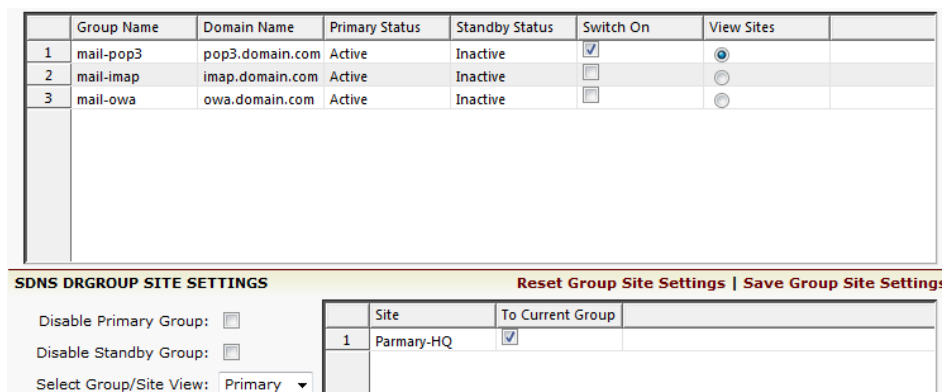


Figure 83:- Assign DR Sites to the Service Group

You need do the similar setup for SDNS member on the backup site.

Setup GSLB/SDNS with BIND 9

The FortiBalancer GSLB/SDNS includes standard BIND9 (named) functionalities. You may import the standard “named.conf” and individual zone files onto FortiBalancer to support full DNS functions. Other than DNS A records, all other DNS records are supported by BIND9. For example, to make GSLB/SDNS support MX record resolution, the MX records for a domain need be added to the normal domain zone file and import the zone file.

To import, select Global Load Balance -> Records -> Others. You can hit “Browse” to select local files for input to the FortiBalancer.

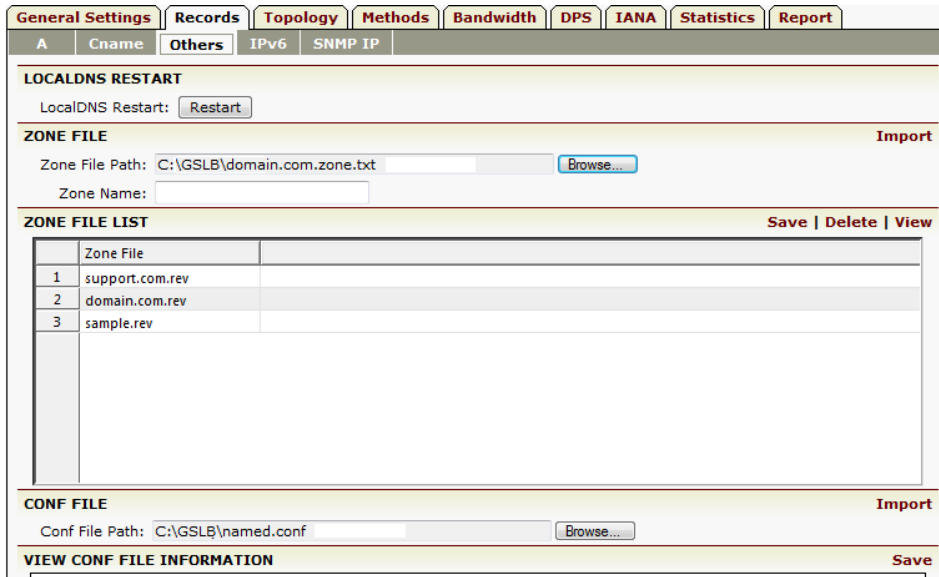


Figure 84:- Importing Zone File

Once the BIND 9 Configure file and/or selected zone files are imported, click Restart to restart LocalDNS service to enable the changes.

GSLB/SDNS DR Deployment Verification

To validate the FortiBalancer GSLB/SDNS can correctly resolve DNS queries for DNS A and MS records, Windows command tool “nslookup” can be used. On the Windows command tool, type “nslookup” to enter nslookup utility. Type “server 10.2.40.111” to set the FortiBalancer as the DNS server and “set q=a” (for Query DNS A Record).

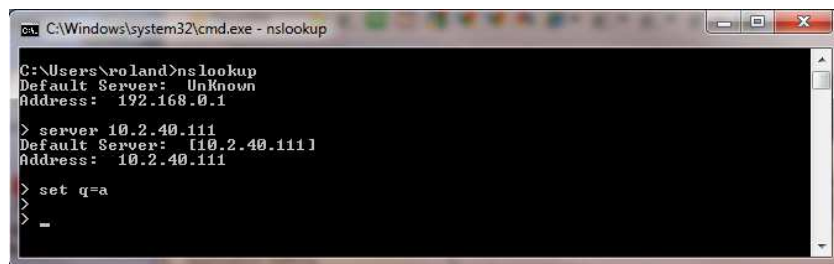


Figure 85:- Query NSLookup for A Records

Type the domain names that are managed by *FortiBalancer* GSLB/SDNS – See the following.

For the Primary-HQ site, it is dual home for “owa.domain.com” so that two addresses (10.2.40.111 and 192.168.1.115) are returned in round-robin term. The second IP can be disabled as the Link is down or the Virtual Service is disabled (consider down).

```

C:\Windows\system32\cmd.exe - nslookup
> ova.domain.com
Server: [10.2.40.111]
Address: 10.2.40.111

Name: ova.domain.com
Addresses: 10.2.40.112
           192.168.1.115

> ova.domain.com
Server: [10.2.40.111]
Address: 10.2.40.111

Name: ova.domain.com
Addresses: 192.168.1.115
           10.2.40.112

> pop3.domain.com
Server: [10.2.40.111]
Address: 10.2.40.111

Name: pop3.domain.com
Addresses: 192.168.1.112
           10.2.40.112

> pop3.domain.com
Server: [10.2.40.111]
Address: 10.2.40.111

Name: pop3.domain.com
Addresses: 10.2.40.112
           192.168.1.112

```

Figure 86:- NSLookup Returned A Records

To test the MX record support, enter “nslookup” utility, set the FortiBalancer as the default DNS server. Type “set q=mx” to set the default DNS query type to MX record and type the domain name. The FortiBalancer GSLB/SDNS BIND9 shall able to resolve it. See the following:

```

C:\Windows\system32\cmd.exe - nslookup
C:\Users\poland>nslookup
Default Server: UnKnown
Address: 192.168.0.1

> server 10.2.40.111
Default Server: [10.2.40.111]
Address: 10.2.40.111

> set q=mx
> domain.com
Server: [10.2.40.111]
Address: 10.2.40.111

domain.com      MX preference = 20, mail exchanger = mail2.domain.com
domain.com      MX preference = 10, mail exchanger = mail1.domain.com
domain.com      nameserver = ns1.domain.com
domain.com      nameserver = ns2.domain.com
mail1.domain.com internet address = 10.2.40.111
mail2.domain.com internet address = 10.7.15.70
ns1.domain.com  internet address = 10.2.40.111
ns2.domain.com  internet address = 10.7.15.70
>
>
>

```

Figure 87:- Query NSLookup for MX Records

Log Information

On the FortiBalancer appliance each DNS query can be logged with INFO level as the following:

```

INFO Apr 19 22:16:23 The DNS request information: LocalDNS-
10.1.14.13, Request Domain Name-pop3.domain.com, Request Type-
A, Request-success, UpTime-2011/4/19,22:16
INFO Apr 19 22:16:25 The DNS request information: LocalDNS-
10.1.14.13, Request Domain Name-pop3.domain.com, Request Type-
A, Request-success, UpTime-2011/4/19,22:16

```

Primary Site Configuration Summary

```
#link load balancing DNS configuration
llb dns host "owa.domain.com" 192.168.1.115 1 443
llb dns host "owa.domain.com" 10.2.40.112 200 443
llb dns host "pop3.domain.com" 192.168.1.112 1 995
llb dns host "pop3.domain.com" 10.2.40.112 200 995
llb dns host "imap.domain.com" 192.168.1.112 1 993
llb dns host "imap.domain.com" 10.2.40.112 200 993
llb dns ttl "owa.domain.com" 60
llb dns ttl "pop3.domain.com" 60
llb dns ttl "imap.domain.com" 60

#smart DNS configuration
sdns on Check
sdns member attribute "HQ-FortiBalancer1" 10.2.40.111 5888 all
sdns member attribute "DC-FortiBalancer1" 192.168.40.111 5888
all
sdns member local "HQ-FortiBalancer1" 1000
sdns interval heartbeat 2
sdns site location "Backup-DC" 100
sdns site location "Primary-HQ" 100
sdns site member "Primary-HQ" "HQ-FortiBalancer1"
sdns group dr "mail-pop3" "pop3.domain.com"
sdns group preempt "mail-pop3" 1
sdns group primary "mail-pop3" "Primary-HQ"
sdns group standby "mail-pop3" "Backup-DC"
sdns group dr "mail-imap" "imap.domain.com"
sdns group preempt "mail-imap" 1
sdns group primary "mail-imap" "Primary-HQ"
sdns group standby "mail-imap" "Backup-DC"
sdns group dr "mail-owa" "owa.domain.com"
sdns group preempt "mail-owa" 1
sdns group primary "mail-owa" "Primary-HQ"
sdns group standby "mail-owa" "Backup-DC"
sdns group dr "exchange2010" "eas.domain.com"
sdns group preempt "exchange2010" 1
sdns interval report 30
sdns dps interval send 120
sdns dps interval query 1200
sdns dps history 9000
sdns dps expire 1
sdns dps method rtt
sdns dps off
sdns dps master off
#NoCheck IP Address
sdns snmp interval 300
sdns snmp version "v2c"
sdns statistics on all

sdns statistics on localdns
```

```
sdns persistent timeout 3600
sdns recursion off
```

Backup Site Configuration Summary

```
#link load balancing DNS configuration
llb dns host "pop3.domain.com" 10.7.15.72 1 995
llb dns host "imap.domain.com" 10.7.15.72 1 993
llb dns host "owa.domain.com" 10.7.15.72 1 443
llb dns ttl "pop3.domain.com" 60
llb dns ttl "imap.domain.com" 60
llb dns ttl "owa.domain.com" 60

#smart DNS configuration
sdns on Check
sdns member attribute "HQ-FortiBalancer1" 10.2.40.111 5888 all
sdns member attribute "DC-FortiBalancer1" 10.7.15.70 5888 all
sdns member local "DC-FortiBalancer1" 1000
sdns interval heartbeat 2
sdns site location "Backup-DC" 100
sdns site member "Backup-DC" "DC-FortiBalancer1"
sdns site location "Primary-HQ" 100
sdns group dr "mail-pop3" "pop3.domain.com"
sdns group preempt "mail-pop3" 1
sdns group primary "mail-pop3" "Primary-HQ"
sdns group standby "mail-pop3" "Backup-DC"
sdns group dr "mail-imap" "imap.domain.com"
sdns group preempt "mail-imap" 1
sdns group primary "mail-imap" "Primary-HQ"
sdns group standby "mail-imap" "Backup-DC"
sdns group dr "mail-owa" "owa.domain.com"
sdns group preempt "mail-owa" 1
sdns group primary "mail-owa" "Primary-HQ"
sdns group standby "mail-owa" "Backup-DC"
sdns interval report 30
sdns dps interval send 120
sdns dps interval query 1200
sdns dps history 9000
sdns dps expire 1
sdns dps method rtt
sdns dps off
sdns dps master off
#NoCheck IP Address
sdns snmp interval 300
sdns snmp version "v2c"
sdns statistics on all
sdns statistics on localdns
sdns persistent timeout 3600

sdns recursion off
```

Summary

FortiBalancer Application Delivery Controllers deliver all required application delivery functions for optimizing Exchange Server 2010 environments, such as Layer 4-7 server load balancing, link load balancing, high availability/DR, SSL acceleration and offloading, Session Persistence, TCP connection multiplexing, caching and compression – all in a single, easy-to-manage appliance.

FortiBalancer Application Delivery Controllers enhance the availability, performance and security characteristics of Microsoft Exchange 2010 solution.