Load Balancing Microsoft Exchange 2010 with FortiADC

Highly Available, High Performing, and Scalable Deployment with FortiADC D-Series Appliances

Exchange 2010 and Application Delivery
Microsoft® Exchange Server 2010 was released in late 2009 as the successor to Microsoft Exchange Server 2007. It introduced a number of new features as well as changes to existing features. Enhancements were added with Service Pack 1 (SP1) in 2010 and again in 2011 with the release of Service Pack 2 (SP2).

This guide was originally written for SP1 and was revised for SP2 in 2011.

Load Balancing Requirements for Exchange
Microsoft recognizes the need for load balancing client access in all but the smallest Exchange deployments. For Microsoft’s overview of load balancing recommendations in Exchange 2010, please see:


As stated in the above document, client access in Exchange 2010 is concentrated at the Client Access Server (CAS) or middle tier of the Exchange Architecture. Placing a load balancer in front of the CAS array ensures that resources are used efficiently to provide the best user experience for both internal and external client access:

“In earlier versions of Exchange, Outlook® connected directly to the Mailbox server hosting the user’s mailbox, and directory connections were either proxied through the Mailbox server role or referred directly to a particular Active Directory® global catalog server. Now that these connections are handled by the Client Access server role, both external and internal Outlook connections must be load balanced across the array of Client Access servers in a deployment to achieve fault tolerance.

A load-balanced array of Client Access servers is recommended for each Active Directory site and for each version of Exchange.”

Important Note:
This guide is written only for the FortiADC D-series platform. The instructions included within are not designed to be used with the FortiADC E-series platform application delivery controllers.

While software load balancers and reverse proxy solutions can be adequate for smaller deployments, larger deployments will benefit from the features and capacity provided by a hardware load balancer. Among other issues, Microsoft recognizes the following limitations with Windows Network Load Balancing, the most popular software based load balancing solution for Exchange:

“Due to performance issues, we don’t recommend putting more than eight Client Access servers in an array that’s load balanced by WNLB.”
“WNLB doesn’t detect service outages. WNLB only detects server outages by IP address. This means if a particular Web service, such as Outlook Web App, fails, but the server is still functioning, WNLB won’t detect the failure and will still route requests to that Client Access server. Manual intervention is required to remove the Client Access server experiencing the outage from the load balancing pool.”

“WNLB configuration can result in port flooding, which can overwhelm networks.”

“If you have more than eight Client Access servers in a single Active Directory site, your organization will need a more robust load balancing solution. Although there are robust software load balancing solutions available, a hardware load balancing solution provides the most capacity.”

Another reason to deploy a hardware load balancer with Exchange 2010 is that Exchange uses a concept called a Database Availability Group (DAG) to provide high availability at the database level. A DAG is a group of up to 16 Mailbox servers that host a set of databases and provide automatic database-level recovery from failures that affect individual servers or databases. This architecture requires the use of an external load balancer to provide high availability above the database level.
The FortiADC Difference

There are a number of hardware load balancing products available on the market with a wide range of features and capabilities. FortiADC differentiates itself by providing superior value; advanced acceleration features, high performance, and reliability born of over 10 years of industry experience.

FortiADC not only load balances Internet service requests across multiple servers, but also accelerates application performance and provides application aware features that monitor server load and improve server response times – by as much as 25%. In addition to basic load balancing, FortiADC provides:

- Automatic server and application health monitoring
- Intelligent, application aware load balancing policies (least connections, fastest response time, and round robin).
- Content switching – the ability to change load balancing behavior based on the content of a client request
- Content rewriting – the ability to rewrite data or links being sent to the client.
- SSL offloading and acceleration
- Real time graphical performance monitoring and reporting
- Redundant High Availability (HA) configurations
- HTTP Compression to reduce bandwidth requirements
- HTTP Caching to reduce load on servers and speed client responses.
- Virtual Domains to segregate your network into separate domains and multi-tenant environments

For more information on how FortiADC can make your applications work better, faster, and more economically, please visit www.fortinet.com.
Using FortiADC with Exchange 2010

Setting up and configuring Microsoft Exchange 2010 requires significant planning to ensure adequate resources for deployment. Before beginning any deployment of Exchange 2010, thoroughly read and follow Microsoft’s Exchange planning guide:


In particular, it is vital that your hardware and network configuration has the processing capacity (CPU speed and memory), throughput, and bandwidth required for the number of users and client access methods that you need to deploy. Even in a test environment, you must ensure adequate resources, as described in the planning guide, so that your configuration functions efficiently.

For the purposes of this deployment guide, we assume a working Exchange deployment that will be augmented by the addition of FortiADC (or a pair of FortiADCs in a failover configuration). If you are setting up a new deployment of Exchange, we recommend that you first set up your Exchange configuration without FortiADC, verify each of your intended client access methods, and then follow this document to deploy FortiADC into that configuration.

Logically, FortiADC sits in between clients accessing Exchange and the Exchange servers, as shown in the following diagram:
Clients can access Exchange via a number of applications and protocols (generally called Exchange services in the remainder of this guide):

**Outlook Web App (OWA)** – (known as Outlook Web Access in previous Exchange releases). Internal and external clients initiate OWA sessions over HTTP using a web browser, or Outlook Web App Light.

**Outlook Anywhere (OA)** – Outlook clients access Exchange by tunnelling the Outlook MAPI (Messaging Application Programming Interface) protocol over an HTTP connection.

**ActiveSync (AS)** – Mobile clients can synchronize with Exchange services, which push data to the mobile device, over an HTTP connection.

**POP3 and IMAP4** – External and internal third-party mail programs use these protocols (Post Office Protocol v3 and Internet Message Access protocol v4) to retrieve and send email.

**Remote Procedure Call Client Access (RPC CA)** – RPC CA services include the PortMapper, MAPI access to Outlook, and the AddressBook application.

**SMTP** – External mail servers forward mail to Exchange through Edge Servers or Hub Transport Servers using the Simple Mail Transfer Protocol (SMTP).

All of the services above are routed through FortiADC and load balanced to the appropriate Client Access Server (or, in the case of SMTP, to an Edge Server deployed outside of the Exchange domain). Each of these services requires a slightly different FortiADC configuration, as described in the remainder of this document.
Hardware and Software Used in This Guide
To develop this deployment guide, the following hardware and software was used:

- FortiADC VM v4.0.0 build 12
- Custom Server hardware running VMware ESXi 5
- Several VM servers running Microsoft Server 2008
- Microsoft Exchange Server 2010 SP2
- Appropriately configured clients to test client access

Note that the hardware and software required for your configuration will vary from the above depending on your testing and production environment. Microsoft Hyper-V, for example, could be used in place of VMware.

If you do not have locally available clients of all types, Microsoft offers two alternatives that you can use in a testing environment to validate your configuration prior to putting it into production:

- The Exchange Load Generator 2010 can be installed on a local server and can be configured to generate Exchange traffic for the various protocols.
- The Exchange Remote Connectivity Analyzer is an online tool that you configure to test your Internet accessible Exchange configuration.

Click on the links above for more details on configuring and using these tools.

Server Health Checks
FortiADC can probe server health using ICMP and TCP probes. You can also enable HTTP and other application specific healthchecks to ensure that services are running and available.

For more information, see the FortiADC Administration Guide.

Load Balancing Policy
In previous versions of Microsoft Exchange, Microsoft recommended using the least connections load balancing policy, which routes requests to servers that are more lightly loaded in terms of number of open connections. Microsoft has since changed its recommendation, since it is possible that using a load balancing algorithm like least connections can lead to overloading a server when it is first brought online. Microsoft now recommends using a policy that does not depend on weighted criteria, such as round robin – which simply routes requests evenly across all available servers, regardless of performance. The result is that while round robin makes it less likely that any one server will be overloaded when it is brought online, it leads to an imbalance in the distribution of requests across all servers when servers are brought offline and online.

It should be noted that FortiADC’s least connections setting is less prone to overloading a new server, since FortiADC tries to avoid overloading the server by using the concept of warm up time. Whilst in a warm up state the rate of connections to the server will be limited.
Besides round robin and least connections, FortiADC also offers:

fastest response -- dispatches the highest percentage of requests to the server with the shortest response time.

**Source Network Address Translation (SNAT) Setting**

‘Source Network Address Translation’ or SNAT involves changing the source address from the original client IP to an IP owned by the FortiADC in order to ensure correct routing of traffic in complex or single vlan configurations.

▶ For Layer7 Virtual servers, the FortiADC acts as a proxy and will substitute its own interface IP address for the client IP before completing the connection to the back end server.

▶ For Layer4 Virtual servers, the FortiADC can be set to change the source IP address by selecting the Full NAT as the packet forwarding method. In this case, a source pool will need to be created using at least 1 IP address on the same subnet as the ADC interface.

In general, Microsoft recommends using SNAT for all configurations, although it may not be appropriate in circumstances where it is desirable to see the real client IP address at the server.

In a multiple VLAN/subnet configuration, for Layer4 Virtual servers, you can either:

- Use DNAT as the packet forwarding method and set the default gateway on each server to FortiADC’s IP address on the same subnet/VLAN (or, use static routes to send responses to FortiADC’s IP address).

  Or:

- Use SNAT (by choosing Full NAT).

Note that Direct Routing configurations are supported by Exchange, but in general SNAT-enabled configurations are recommended by Microsoft to avoid the additional complexity and drawbacks of Direct Routing. For example: to use Direct Routing with any load balancer requires configuration of a special loopback adapter on each server and is supported only for Layer 4 services.

See the *FortiADC Administration Guide* for more information on FortiADC network configuration.
SSL Offload and Acceleration
SSL offload can be performed by FortiADC for HTTPS or any other protocol using HTTPS or TCPS profiles, respectively. The instructions in this document show you how to upload a server certificate to FortiADC, as well as perform the necessary operations to offload SSL transactions to the FortiADC for all of the relevant protocols used by Exchange 2010.

The FortiADC Administrative Interface
This guide assumes that you have already set up FortiADC on your organization’s network. Full instructions are available in the printed startup guides and CD-ROM delivered with your FortiADC. Documentation is also available from our support site.

http://<FortiADC_IP_addr>

Where <FortiADC_IP_addr> is FortiADC’s management IP address. Log in to FortiADC using a login with administrator privileges. This opens the graphical user interface, as shown in the following figure:

The virtual servers, real server pools, and other objects created for Exchange 2010 will be displayed in the left frame, while configuration details are displayed and modified in the right frame:

Click Help at any time to display documentation for the currently displayed configuration details.
**Virtual Server Configuration Summary**

The following table summarizes the clusters that will be used for Exchange – each cluster is a virtual front-end for one or more Exchange services.

<table>
<thead>
<tr>
<th>Exchange Service</th>
<th>Virtual Server Type</th>
<th>Virtual Server Port</th>
<th>Virtual Server Port</th>
<th>Persistence</th>
<th>Server Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWA/OA/ActiveSync</td>
<td>Layer 7</td>
<td>443</td>
<td>80</td>
<td>Cookie</td>
<td>TCP 80, HTTP</td>
</tr>
<tr>
<td>POP3</td>
<td>Layer 7</td>
<td>995</td>
<td>110</td>
<td>None</td>
<td>TCP 110</td>
</tr>
<tr>
<td>IMAP</td>
<td>Layer 7</td>
<td>993</td>
<td>143</td>
<td>None</td>
<td>TCP 143</td>
</tr>
<tr>
<td>SMTP</td>
<td>Layer 4</td>
<td>25</td>
<td>25</td>
<td>None</td>
<td>TCP 25</td>
</tr>
<tr>
<td>RPC CA (Portmapper)</td>
<td>Layer 4</td>
<td>135</td>
<td>135</td>
<td>Source IP</td>
<td>TCP 135</td>
</tr>
<tr>
<td>RPC CA (MAPI)</td>
<td>Layer 4</td>
<td>59532</td>
<td>59532</td>
<td>Source IP</td>
<td>TCP 59532</td>
</tr>
<tr>
<td>RPC CA (AddressBook)</td>
<td>Layer 4</td>
<td>59533</td>
<td>59533</td>
<td>Source IP</td>
<td>TCP 59533</td>
</tr>
</tbody>
</table>
Creating Health checks

This section shows you how to create the different health checks you will need on FortiADC for each of the services running on the real servers in your Exchange configuration.

To define FortiADC health checks for Exchange, do the following for each required health check:

1. Click on the **Server Load Balancing** label in the left frame object tree of the GUI and expand the Resources section. Click on the health check item to open the relevant page in the right hand pane.

2. Click the add icon to create a health check.

3. Enter a unique Name and select the health check type. Different options will be made available depending on the type of health check selected.

4. Enter the relevant parameters such as port number for a TCP health check, or HTTP request and expected response.

5. Choose the timing parameters. Recommended settings for Exchange are **Interval** 5 seconds, **Timeout** 4 seconds, **Down retry** 2, **Up Retry** 3.

6. Click **Save**.

A health check should be made for each TCP port that will be used by real servers to provide service, as well as one for HTTP if required.

An HTTP health check can be used to ensure that an application is running or that a page is loaded correctly. In this case it is possible to check that the OWA service is running correctly by using an HTTP health check to GET a dynamically generated page.

The HTTP health check for Exchange2010 can be set as **Method Type** ‘GET’, **Port** ‘80’, **Send String** ‘/owa/auth/logon.aspx’, and **Status Code** ‘200’. This will ensure that the OWA application is running and presenting a logon screen to the client rather than just ensuring that the server is listening.
Creating Servers and Pools

This section shows you how to define server pools on FortiADC for each of the services running on the servers in your Exchange configuration and how to add real servers as members to those pools.

In an Exchange configuration that implements all the Exchange services listed in the Virtual server Configuration Summary table, you might have a separate Client Access Server (CAS) for each service; or, some of your servers might host several exchange services on the same IP address using different ports.

Each instance of a service running on a backend server needs to be defined as a real server, and real servers need to be grouped together in Real Server pools so that they can be associated with a virtual server. In this way the service that a virtual server provides to the internet is logically connected to a set of multiple instances of that service running on real servers behind the ADC.

Server pools are groups of servers that can be assigned as a unit to an FortiADC virtual server: the IP address/port that clients access when requesting Exchange services.

In general, a server pool is required for each group of FortiADC servers that offer the same service.

For example, in the simplest Exchange configuration outlined in the previous section, the server pools might be created as shown in the table below. The real servers listed for each pool are explained in further detail in the following section.

<table>
<thead>
<tr>
<th>Server Pool</th>
<th>Real Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP pool</td>
<td>CAS1, CAS2</td>
</tr>
<tr>
<td>POP pool</td>
<td>CAS3-POP, CAS4-POP</td>
</tr>
<tr>
<td>IMAP Pool</td>
<td>CAS3-IMAP, CAS4-IMAP</td>
</tr>
<tr>
<td>PM pool</td>
<td>CAS5-PM, CAS6-PM</td>
</tr>
<tr>
<td>MAPI pool</td>
<td>CAS5-MAPI, CAS6-MAPI</td>
</tr>
<tr>
<td>AB pool</td>
<td>CAS5-AB, CAS6-AB</td>
</tr>
<tr>
<td>SMTP pool</td>
<td>Edge1, Edge2</td>
</tr>
</tbody>
</table>

Real Server pools need to contain one or more real servers as members.

On FortiADC, a real server is a unique IP address, port, and protocol combination. Since all Exchange services are TCP-based services, the protocol specified for an Exchange server on FortiADC will always be TCP. We will need to define a FortiADC server for each unique IP address and port offering an Exchange service.

The following table shows an example configuration with a CAS array of six
servers plus two Edge Servers for SMTP, each of them running the indicated services, and how this configuration translates into FortiADC real server definitions:

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Services</th>
<th>FortiADC Servers</th>
<th>Real Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAS1</td>
<td>OWA / OA / AS</td>
<td>One server definition is needed: all these services run on the IP address of CAS1 and TCP port 80.</td>
<td>CAS1</td>
</tr>
<tr>
<td>CAS2</td>
<td>OWA / OA / AS</td>
<td>One server definition is needed: all these services run on the IP address of CAS2 and TCP port 80.</td>
<td>CAS2</td>
</tr>
<tr>
<td>CAS3</td>
<td>POP3 / IMAP4</td>
<td>Two server definitions are needed: POP3 runs on the IP address of CAS3 and port 995, while IMAP4 runs on port 993.</td>
<td>CAS3-POP, CAS3-IMAP</td>
</tr>
<tr>
<td>CAS4</td>
<td>POP3 / IMAP4</td>
<td>Two server definitions are needed: POP3 runs on the IP address of CAS4 and port 995, while IMAP4 runs on port 993.</td>
<td>CAS4-POP, CAS4-IMAP</td>
</tr>
<tr>
<td>CAS5</td>
<td>Portmapper / MAPI / AB</td>
<td>Three server definitions are needed: the Portmapper runs on the IP address of CAS5 and port 135, MAPI runs on port 59532, and the AddressBook runs on port 59533.</td>
<td>CAS5-PM, CAS5-MAPI, CAS5-AB</td>
</tr>
<tr>
<td>CAS6</td>
<td>Portmapper / MAPI / AB</td>
<td>Three server definitions are needed: the Portmapper runs on the IP address of CAS6 and port 135, MAPI runs on port 59532, and the AddressBook runs on port 59533.</td>
<td>CAS6-PM, CAS6-MAPI, CAS6-AB</td>
</tr>
<tr>
<td>Edge1</td>
<td>SMTP</td>
<td>One server definition is needed: SMTP runs on the IP address of Edge1 and port 25.</td>
<td>Edge1</td>
</tr>
<tr>
<td>Edge2</td>
<td>SMTP</td>
<td>One server definition is needed: SMTP runs on the IP address of Edge2 and port 25.</td>
<td>Edge2</td>
</tr>
</tbody>
</table>

So, in the example above, we would need to define 7 pools containing a total of 14 real servers on FortiADC for the Exchange services hosted on the 6 CAS array servers and 2 Edge servers.

Each pool would be defined to contain the two servers providing the same service.

To define FortiADC real server pools and real servers for Exchange, do the following for each required pool:

1. Click on the **Server Load Balancing** label in the left frame object tree of the GUI and expand the Resources section. Click on the real server item to open a page containing the list of server pools in the right hand pane.

2. Click on the add icon at the top to add a new server pool

3. Enter unique **Name**, and check the health check option box to open the
health check section. For each server pool drag across the ICMP health check as well as the TCP or HTTP health checks that match the service to which this pool will be assigned. E.g. for the SMTP pool the ICMP and TCP port 25 health checks would be used. Please note that only health checks that have been defined as shown in the previous section will be available as options.

4. Scroll down to the members section of the pool configuration page and click on the add icon at the top left of that section to create a real server for this pool. If prompted to save the pool, click ok.

5. Enter an IP address and port for the real server, Warm-Up should be set to 5 seconds and connection limits can be set if necessary. Click ok and the real server will be created as a pool member. Repeat this step for all of the real servers that will be added to this pool.

6. Click SAVE to save the pool.

Perform the above steps to create all the server pools required for your configuration and add servers to them. In our example configuration, create all the server pools shown in the table on the previous page and add the indicated servers to them as members.
Creating Persistence Methods

Exchange 2010 requires persistence for OWA as well as Outlook Anywhere and for all of the RPC ports as show in the table listing the virtual servers.

In order to use persistence, a Persistence object must be created for each type of persistence to be used.

To create a persistence object, do the following for each required form of persistence. In this example we will need two, Source IP, and Cookie Insert.

1. Click on the Server Load Balancing label in the left frame object tree of the GUI and expand the Resources section. Click on the persistence item to open a page containing the list of persistence objects in the right hand pane.

2. Click on the add icon at the top to add a new persistence object.

3. Enter a unique Name and select the type of persistence required. The available options will change depending on the type of persistence chosen. For this example use the default settings for the Source IP persistence object, and the default settings with the keyword set as ‘ADC_cookie’ for the Cookie Insert persistence object.

4. Click SAVE.

Perform the above steps for both persistence methods required.
Adding Certificates

SSL Offloading will be performed on FortiADC for a variety of services used by Exchange2010. This requires the installation of the SSL certificate(s) used for these services on FortiADC.

When using FortiADC for SSL offload, certificates are uploaded to a central certificate store and then assigned, via profiles, to virtual servers.

In the most common configuration described in this guide, SSL Offloading is performed for the servers in the CAS array that are running Outlook Web App (OWA), Outlook Anywhere (OA), and ActiveSync (AS), as well as for the servers running POP3 and IMAP. In this configuration, all three HTTP based services have a single virtual server as their network front end and usually use a single Fully Qualified Domain Name (FQDN) for client access. If different FQDNs are used, then a wildcard certificate must be used that will apply across all the FQDNs.

To add a certificate to the certificate store, do the following:

1. Click on the System label in the left frame object tree of the GUI and expand the Certificates section. Click on the local item to open a page containing the list of certificates held locally in the ADC store, in the right hand pane.
2. Click Import and the Import Certificate dialog will appear. Enter a certificate type and fill out the remaining fields.
3. Click Import to add the certificate to the local store.

Perform the above steps for all certificates required for the Exchange 2010 installation. The number may vary depending on the FQDNs that you use for the services requiring SSL offload.
Creating Profiles

Profiles are assigned to virtual servers and contain information about how they should process the traffic that comes into their assigned IP and port combination. There are a number of read-only, pre-defined profiles on the FortiADC but it is recommended to create your own for each of the virtual servers requiring the same settings.

In this case we will need to create an HTTPS profile for the OWA/OA/AS virtual server, a TCPS profile for the IMAPS and POPS virtual servers (the same profile can be used if the same certificate is to be used for both IMAPS and POPS), an SMTP profile, and a TCP profile for the MAPI and RPC ports.

To add a new profile, do the following:

1. Click on the Server Load Balance label in the left frame object tree of the GUI and expand the Profile section. Click on the profile item to open a page containing the list of profiles currently available in the right hand pane.

2. Click on the add icon to create a new profile.

3. Choose a unique name for the profile and select the type of profile that you want to create. There will be different options available depending on the type of profile selected.

4. For the HTTPS and TCPS profiles, a Local Certificate must be selected. See the section on adding certificates to ensure that you have the correct certificate installed. For the TCP profiles used for SMTP and for MAPI/RPC ports the TCP Session Timeout after FIN should be set to 30 seconds.

5. Click SAVE

Perform the above steps for each of the required profiles. A separate HTTPS or TCPS profile will be required for each certificate used for a service.
Creating a Virtual Server for OWA, Outlook Anywhere, and ActiveSync

In most Exchange configurations, Outlook Web App (OWA), Outlook Anywhere (OA), and ActiveSync (AS) are all configured to run together on the same server or servers in the CAS array.

This means that FortiADC can be easily configured for OWA, OA, and AS using a single HTTPS Virtual Server that will provide access for all three services and also offload SSL processing from the servers in the CAS array running these services.

See the section “Enabling SSL Offloading in Exchange” for how to enable SSL offloading for these services on your Exchange CAS servers.

Creating an HTTPS Virtual Server for OWA/OA/AS:

1. Click on the Server Load Balance label in the left frame object tree of the GUI and expand the Virtual Servers section.
2. Click on the virtual server item to create a new Virtual Server.
3. Choose a unique name for the Virtual Server and choose type L7 Load Balance.
4. In the General Configuration area enter the IP address for the Virtual Server and the port on which it should provide service. For OWA/OA/AS this is usually 443. Select the interface to which this port should be assigned, this will be the interface with an IP on the same subnet as the Virtual Server IP.
5. In the General Resources area, from the Profile list, select the HTTPS profile created for OWA/OA/AS. (See Creating Profiles).
6. From the Persistence list select the Cookie Insert persistence object. (See Creating Persistence Methods).
7. From the Method list, choose Round-Robin.
8. From the Pool list, choose the pool created for OWA/OA/AS. (See Creating Servers and Pools).
9. Click SAVE

Required Name Service Changes:

Clients typically access these services as follows (note that in the descriptions below, <FQDN> means the fully qualified domain name of the Exchange CAS array (e.g., mail.example.com):

Outlook Web App connections originate from client web browsers and use the URL https://<FQDN>/rpc to access Exchange.

Outlook Anywhere (known in previous versions of Exchange as RPC over HTTP) connections originate from Outlook 2010, Outlook 2007, and Outlook 2003 clients, and use the URL https://<FQDN>/ExchWeb to connect to Exchange servers.

Exchange ActiveSync connections can originate from any ActiveSync-enabled...
mobile device and use the URL https://<FQDN>/Microsoft-Server-ActiveSync to access Exchange.

The FQDN used by clients to access the above services must be changed in DNS (the Domain Name Service) and/or Active Directory to point to the FortiADC virtual server IP address.

**Configuring FortiADC for POP3**

To support mailbox access from POP3 clients you need to start the POP3 service on the Exchange Client Access Servers. For clients to send email through Exchange, you’ll also need to configure SMTP.

Because SSL offloading will be performed, the type of virtual server must be set to L7 Load Balance and a TCPS profile must be used. There is no need for persistence with POP3.

Creating a Virtual Server for POP3.

1. Click on the **Server Load Balance label** in the left frame object tree of the GUI and expand the Virtual Servers section.
2. Click on the virtual server item to create a new Virtual Server.
3. Choose a unique name for the Virtual Server and choose type L7 Load Balance.
4. In the **General Configuration** area enter the IP address for the Virtual Server and the port on which it should provide service. For POP3S this is usually 995. Select the interface to which this port should be assigned, this will be the interface with an IP on the same subnet as the Virtual Server IP.
5. In the **General Resources** area, from the **Profile** list, select the TCPS profile created for POP3S. (See Creating Profiles).
6. From the **Method** list, choose Round-Robin.
7. From the **Pool** list, choose the pool created for POP3S. (See Creating Servers and Pools).
8. Click **SAVE**
Configuring FortiADC for IMAP

To support mailbox access from IMAP clients, you need to start the IMAP service on the Exchange Client Access Servers. For clients to send email through Exchange, you’ll also need to configure SMTP.

Because SSL offloading will be performed, the type of virtual server must be set to L7 Load Balance and a TCPS profile must be used. There is no need for persistence with IMAP.

Creating a Virtual Server for IMAPS.

1. Click on the Server Load Balance label in the left frame object tree of the GUI and expand the Virtual Servers section.
2. Click on the virtual server item to create a new Virtual Server.
3. Choose a unique name for the Virtual Server and choose type L7 Load Balance.
4. In the General Configuration area enter the IP address for the Virtual Server and the port on which it should provide service. For IMAPS this is usually 993. Select the interface to which this port should be assigned, this will be the interface with an IP on the same subnet as the Virtual Server IP.
5. In the General Resources area, from the Profile list, select the TCPS profile created for IMAPS. (See Creating Profiles).
6. From the Method list, choose Round-Robin.
7. From the Pool list, choose the pool created for POP3S. (See Creating Servers and Pools).
8. Click SAVE.
Configuring FortiADC for RPC Client Access

Load balancing RPC Client Access services through FortiADC requires three Layer 4 virtual servers, one for the Portmapper, one for MAPI, and one for the Address Book (AB) service. The instructions below assume that you are using a static port configuration for RPC Client Access as recommended by Microsoft.

All three of the RPC CA virtual servers will be configured to use source IP persistence.

Creating a Virtual Server for RPC Portmapper.

1. Click on the Server Load Balance label in the left frame object tree of the GUI and expand the Virtual Servers section.
2. Click on the virtual server item to create a new Virtual Server.
3. Choose a unique name for the Virtual Server and choose type L4 Load Balance.
4. From the Packet Forwarding option list, choose DNAT. (If SNAT is required then the Full NAT option would be used. This requires the creation of a source pool object.)
5. In the General Configuration area enter the IP address for the Virtual Server and the port on which it should provide service. For RPC Portmapper this is usually 135. Select the interface to which this port should be assigned, this will be the interface with an IP on the same subnet as the Virtual Server IP.
6. In the General Resources area, from the Profile list, select the TCP profile created for RPC/MAPI (See Creating Profiles).
7. From the Persistence list chose the Source IP object (See Creating Persistence Methods).
8. From the Method list, choose Round-Robin.
9. From the Pool list, choose the pool created for RPC/MAPI (See Creating Servers and Pools).
10. Click SAVE.

Creating a Virtual Server for RPC MAPI.

1. On all MAPI servers, use the Windows regedit tool to set the static port for the MAPI protocol by setting the following registry key, as in this example, which sets the port to 59532:

   `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeRPC\ParametersSystem]"TCP/IP Port"=dword:0000e88c`

2. Click on the Server Load Balance label in the left frame object tree of the GUI and expand the Virtual Servers section.
3. Click on the virtual server item to create a new Virtual Server.
4. Choose a unique name for the Virtual Server and choose type L4 Load Balance.
5. From the Packet Forwarding option list, choose DNAT. (If SNAT is required then the Full NAT option would be used. This requires the creation of a source pool object.)
6. In the General Configuration area enter the IP address for the Virtual Server and the port on which it should provide service. For RPC MAPI this is usually 135. Select the interface to which this port should be assigned, this will be the interface with an IP on the same subnet as the Virtual Server IP.
7. In the General Resources area, from the Profile list, select the TCP profile created for RPC/MAPI (See Creating Profiles).
8. From the Persistence list chose the Source IP object (See Creating Persistence Methods).
9. From the Method list, choose Round-Robin.
10. From the Pool list, choose the pool created for RPC/MAPI (See Creating Servers and Pools).
11. Click SAVE.
5. From the Packet Forwarding option list, choose DNAT. (If SNAT is required then the Full NAT option would be used. This requires the creation of a source pool object.)

6. In the General Configuration area enter the IP address for the Virtual Server and the port on which it should provide service. For RPC MAPI we have configured Exchange to use 59532. Select the interface to which this port should be assigned, this will be the interface with an IP on the same subnet as the Virtual Server IP.

7. In the General Resources area, from the Profile list, select the TCP profile created for RPC/MAPI (See Creating Profiles).

8. From the Persistence list chose the Source IP object (See Creating Persistence Methods).

9. From the Method list, choose Round-Robin.

10. From the Pool list, choose the pool created for RPC/MAPI (See Creating Servers and Pools).

11. Click SAVE.

Creating a Virtual Server for RPC Address Book.

Note: In Step 1, below, the Address Book static port is set using the method appropriate for Microsoft Exchange 2010. If you have an earlier version of Exchange running on a server, please see the Microsoft Exchange documentation for the version you are running for how to set the Address Book static port.

1. On all Address Book servers, use regedit to set the static port for the Address Book service by navigating to the Registry location shown below and setting the “RpcTcpPort” key as shown in this example (which sets the port to 59533):

   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeAB\Parameters] “RpcTcpPort” = “59533”

2. Click on the Server Load Balance label in the left frame object tree of the GUI and expand the Virtual Servers section.

3. Click on the virtual server item to create a new Virtual Server.

4. Choose a unique name for the Virtual Server and choose type L4 Load Balance.

5. From the Packet Forwarding option list, choose DNAT. (If SNAT is required then the Full NAT option would be used. This requires the creation of a source pool object.)

6. In the General Configuration area enter the IP address for the Virtual Server and the port on which it should provide service. For RPC Address Book we have configured Exchange to use 59533. Select the interface to which this port should be assigned, this will be the interface with an IP on the same subnet as the Virtual Server IP.
7. In the **General Resources** area, from the **Profile** list, select the TCP profile created for RPC/MAPI (See Creating Profiles).

8. From the **Persistence** list chose the Source IP object (See Creating Persistence Methods).

9. From the **Method** list, choose Round-Robin.

10. From the **Pool** list, choose the pool created for RPC/MAPI (See Creating Servers and Pools).

11. Click **SAVE**.

**Configuring FortiADC for SMTP**

SMTP connections in Exchange 2010 may be configured using either Edge Transport Servers or Hub Transport Servers. Just use the appropriate IP addresses for your configuration when adding servers in Step 6, below.

Persistence is not used with the SMTP protocol.

Creating a Virtual Server for SMTP:

1. Click on the **Server Load Balance** label in the left frame object tree of the GUI and expand the Virtual Servers section.

2. Click on the virtual server item to create a new Virtual Server.

3. Choose a unique name for the Virtual Server and choose type **L4 Load Balance**.

4. From the Packet Forwarding option list, choose DNAT. (If SNAT is required then the Full NAT option would be used. This requires the creation of a source pool object.)

5. In the **General Configuration** area enter the IP address for the Virtual Server and the port on which it should provide service. For SMTP this is usually 25. Select the interface to which this port should be assigned, this will be the interface with an IP on the same subnet as the Virtual Server IP.

6. In the **General Resources** area, from the **Profile** list, select the TCP profile created for SMTP (See Creating Profiles).

7. From the **Method** list, choose Round-Robin.

8. From the **Pool** list, choose the pool created for SMTP (See Creating Servers and Pools).

9. Click **SAVE**.
Enabling SSL Offloading in Exchange

SSL offloading means that the client SSL connection is terminated at FortiADC, and FortiADC communicates with the CAS using unencrypted channel. SSL offloading significantly improves CAS performance and simplifies certificate management, since all SSL certificates reside on FortiADC, and FortiADC performs all the CPU-intensive SSL processing.

FortiADC provides SSL offloading for Layer 7 HTTPS virtual servers as well as for other SSL encrypted protocols, so in our deployment we will enable SSL offloading for the following Exchange services:

- Outlook Web App – you must enable SSL offloading in the registry and in IIS on each CAS
- Outlook Anywhere – enable SSL offloading in Outlook Anywhere properties and IIS on each CAS
- Exchange ActiveSync – enable SSL offloading in IIS on each CAS
- POP3- enable POP on each CAS.
- IMAPS- enable IMAP on each CAS.

Enabling Outlook Web App SSL Offloading in the Registry

Enabling SSL offload for Outlook Web App requires that you create a new key in the Windows Registry, as described below.

1. From the desktop, click Start > Run, and enter regedit into the text box. Click OK.
2. Use the left pane tree to navigate to the following registry location:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange_OWA
3. On the Registry Editor menu, click Edit > New > DWORD. A new key appears in the right pane of the editor.
4. Enter SSLOffloaded for the new key Name and press <Enter>.
5. Right-click the new SSLOffloaded key and select Modify from the popup menu.
6. In the Value data field, type 1 (the number one). Click OK to save your changes.
7. Select File > Exit to close the Registry Editor.
8. Go to the section “Enabling SSL Offloading in IIS”.

Configure Outlook Anywhere and SSL Offloading

Use this procedure to turn on Outlook Anywhere and enable SSL offloading at the same time. Do the following for each CAS server:

1. Launch the Exchange Management Console (EMC) from the Start menu.
2. In the console tree at left, navigate to Server Configuration > Client
Access.

3. In the **Client Access** pane (middle pane), click the server on which you want to enable Outlook Anywhere.

4. In the **action** pane, click **Enable Outlook Anywhere**.

5. In the **Enable Outlook Anywhere** wizard, in the box under **External host name**, type the external host name for your organization.

6. Select an available external authentication method. You can select **Basic authentication** or **NTLM authentication**.

7. Enable the check box next to **Allow secure channel (SSL) offloading**.

8. Click **Enable** to apply these settings and enable Outlook Anywhere.

9. Click **Finish** to close the Enable Outlook Anywhere wizard.

10. Go to the section “Enabling SSL Offloading in IIS”.

**Enabling SSL Offload when Outlook Anywhere is Already Configured**

Use this procedure when you have already configured Outlook Anywhere and want to modify it to enable SSL offloading. Do the following for each CAS server:

1. Launch the **Exchange Management Console** (EMC) from the **Start** menu.

2. In the console tree at left, navigate to **Server Configuration > Client Access**.

3. In the **Client Access** pane (middle pane), right-click the name of the server on which you want to enable SSL offloading for Outlook Anywhere, and select **Properties** from the popup menu.

4. In the **Properties** window, open the **Outlook Anywhere** tab.

5. Enable the check box next to **Allow secure channel (SSL) offloading**.

6. Click **OK** to apply these settings and enable Outlook Anywhere on the server.

7. Go to the section “Enabling SSL Offloading in IIS”.

**Enabling SSL Offloading in IIS**

We now need to re-configure the IIS web site on each CAS, so that it will accept HTTP connections instead of requiring HTTPS connections. Do the following on each CAS server in the configuration.

1. From the desktop, click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

2. In the left pane tree, expand **Server_name > Sites > Default Web Site** to display all the default web site home pages.

3. Do the following for each of the components that you are routing through an FortiADC virtual server, as shown in this table:
a. Click the name of the home page in the left pane.

b. In the middle pane, open SSL Settings and disable the Require SSL check box.

c. In the Actions pane at right, click Apply.

4. When you are done, close the IIS Manager.

Summary
FortiADC provides the load balancing, application acceleration, and high availability features demanded by medium to large Microsoft Exchange Server 2010 configurations. This document has presented a step-by-step guide to configuring FortiADC’s features for an Exchange 2010 environment.

About Fortinet’s ADC Solutions
From the leader in Network Security comes a new breed of Application Delivery Controller (ADC), FortiADC, built for your needs today and in the future. FortiADC solutions meet the challenge of delivering mission critical applications reliably, securely and at a value that others can’t match.

We offer a broad selection of hardware and virtual appliances to cover your needs whether you’re a small business looking to expand your website or an enterprise that has to span applications across data centers around the globe.

All FortiADCs offer global server load balancing (GSLB) at no extra cost. If you need to bridge your application across two or more data centers for disaster recovery or to improve response times, the built-in GSLB is easy to setup and manage. For even greater flexibility and more connectivity choices, Fortinet’s FortiDirector GSLB provides a subscription-based GSLB service that can bridge traffic between multiple data centers, single servers or to host-based services. With the ability to route traffic based on server health, network status or even time of day, FortiDirector gives you even greater versatility to manage your applications.

For more information on Fortinet’s portfolio of ADC solutions, please visit www.fortinet.com or contact us directly at the numbers listed below for your region.