Load Balancing Microsoft Exchange 2010 with FortiADC

Highly Available, High Performing, and Scalable Deployment with FortiADC E-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 E-series platform. The instructions included within are not designed to be used with the FortiADC D-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 (adaptive, least connections, fastest response time, static weight, server agent, custom, and round robin)
- Content switching – the ability to change load balancing behavior based on the content of a client request
- Smart Events – the ability to specify administrative actions based on observed behavior and conditions
- SSL offloading and acceleration
- Real time graphical performance monitoring and reporting
- Redundant High Availability (HA) configurations
- Tight integration with the VMware Infrastructure to provide higher application performance in a virtualized server environment
- HTTP Compression to reduce bandwidth requirements

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 model 300E
- EQ/OS Version 10.1
- Custom Server hardware running VMware ESX 4
- 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

By default, FortiADC probes server health using ICMP and TCP probes. You can also enable Active Content Verification (which verifies server availability via specific content) as part of TCP probing.

Version 10.1 of EQ/OS also offer an expanded Health Check capability that allows you to define additional server specific health checks: simple health checks that use a load value returned by a user-supplied program running on the server, and VLB health checks that can be used with VMware virtual machine servers. VLB health checks use detailed server health information from VMware that can be used for load balancing policy decisions as well as server health checking. For more information, see the FortiADC Installation and 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 overloads 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 also checking the server’s response time and server agent value (if used). In this way, the least connections policy attempts to optimize the balance of connections to servers in the cluster. Other policies, such as adaptive and fastest response, behave similarly.

In addition, the speed with which all load balancing policies adjust load in response to changes in server characteristics is controlled by the responsiveness setting, which is set to medium by default. Setting responsiveness appropriately when using weighted load balancing policies can help reduce the potential for overloads.

Besides round robin and least connections, FortiADC also offers these load balancing policies:

- **static weight** -- distributes requests among the servers depending on their assigned initial weights. A server with a higher initial weight gets a higher percentage of the incoming requests. Think of this method as a weighted round robin implementation. Static weight load balancing does not support FortiADC’s adaptive load balancing feature – that is, FortiADC does not dynamically adjust server weights based on server performance.

- **adaptive** -- distributes the load according to these performance indicators for each server

  - Server response time is the length of time for the server to begin sending reply packets after FortiADC sends a request.
  - Active connection count is the number of connections currently active on the server.
  - Server agent value is the value returned by the server agent daemon (if any) running on the server.

- **fastest response** -- dispatches the highest percentage of requests to the server with the shortest response time. FortiADC does this carefully: if FortiADC sends too many requests to a server, the result can be an overloaded server with slower response time. The fastest response policy optimizes the cluster-wide response time. The fastest response policy also checks the number of active connections and server agent values (if configured); but both of these have less of an influence than they do under the adaptive load balancing policy. For example, if a server’s active connection count and server agent values are high, FortiADC might not dispatch new requests to that server even if that server’s response time is the fastest in the cluster.

- **custom** – allows you to set the relative importance of load balancing criteria to specifically configure a policy that meets your needs.
Source Network Address Translation (spoof) Setting

The cluster spoof option controls which IP address is used as the source address in packets sent to the servers behind FortiADC; this is more generally known as ‘Source Network Address Translation’ or SNAT:

- **When the spoof option is enabled**, no SNAT is performed on client requests – that is, servers will see the client’s IP address as the source IP in all packets received from FortiADC. *This is the default setting for a new cluster.*

- **Disabling the spoof option** turns on SNAT – FortiADC translates the client IP address to FortiADC’s IP address on the VLAN/subnet. So, the server receiving the request will see FortiADC’s IP address as the source IP address.

In general, Microsoft recommends using SNAT (*disabling* the spoof option) 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 (e.g., for logging):

In a multiple VLAN/subnet configuration, you can either:

   Enable the spoof option 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 (*disable* spoof).

In a single VLAN/subnet configuration, SNAT should be used. The spoof option should be disabled, so that servers see FortiADC’s IP address in the request and send responses back to FortiADC.

Note that Direct Server Return (DSR) configurations are supported by Exchange, but in general SNAT-enabled configurations are recommended by Microsoft to avoid the additional complexity and drawbacks of DSR. For example: to use DSR 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 *Installation and Administration Guide* for more information on FortiADC network configuration.
SSL Offload and Acceleration

SSL offload is performed by FortiADC for Layer 7 HTTPS clusters. The instructions in this document show you how to upload a server certificate to an HTTPS cluster on FortiADC, as well as perform the necessary operations for each offloaded protocol on Exchange 2010.

Data Compression

Data compression is available on the E670LX and E970LX model FortiADCs only. Compression is enabled on a cluster by cluster basis by turning on the compress check box in the cluster’s Networking configuration. Data compression provides throughput in most configurations that is 3 to 5 times the throughput observed when compression is not used.

The FortiADC Administrative Interface

Once FortiADC has an IP address on the network, open the Administrative Interface by opening the following URL in your web browser:

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:

![FortiADC Administrative Interface](image)

The clusters, servers, responders, and match rules you create for Exchange 2010 will be displayed in the left frame, while configuration details are displayed and modified in the right frame:

1. Click an object in the left frame to display the configuration details for that object.
2. Right-click an object in the left frame to display commands for that object.
3. Click FortiADC to display global configuration parameters.
4. Click Help > Context Help at any time to display documentation for the currently displayed configuration details.
Cluster 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>Cluster Type</th>
<th>Cluster Port</th>
<th>Server Port</th>
<th>Affinity (Persistence)</th>
<th>Server Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWA</td>
<td>L7 HTTPS</td>
<td>443</td>
<td>80</td>
<td>Cookie or Source IP</td>
<td>TCP port 80</td>
</tr>
<tr>
<td>Outlook Anywhere</td>
<td>L7 HTTPS</td>
<td>443</td>
<td>80</td>
<td>Cookie or Source IP</td>
<td>TCP port 80</td>
</tr>
<tr>
<td>ActiveSync</td>
<td>L7 HTTPS</td>
<td>443</td>
<td>80</td>
<td>Cookie or Source IP</td>
<td>TCP port 80</td>
</tr>
<tr>
<td>POP3</td>
<td>L4 TCP</td>
<td>995</td>
<td>995</td>
<td>None</td>
<td>TCP port 995</td>
</tr>
<tr>
<td>IMAP4</td>
<td>L4 TCP</td>
<td>993</td>
<td>993</td>
<td>None</td>
<td>TCP port 993</td>
</tr>
<tr>
<td>SMTP</td>
<td>L4 TCP</td>
<td>25</td>
<td>25</td>
<td>None</td>
<td>TCP port 25</td>
</tr>
<tr>
<td>RPC CA (Portmapper)</td>
<td>L4 TCP</td>
<td>135</td>
<td>135</td>
<td>Source IP</td>
<td>TCP port 135</td>
</tr>
<tr>
<td>RPC CA (MAPI)</td>
<td>L4 TCP</td>
<td>59532</td>
<td>59532</td>
<td>Source IP</td>
<td>TCP port 59532</td>
</tr>
<tr>
<td>RPC CA (AddressBook)</td>
<td>L4 TCP</td>
<td>59533</td>
<td>59533</td>
<td>Source IP</td>
<td>TCP port 59533</td>
</tr>
</tbody>
</table>
Creating Servers

This section shows you how to define servers on FortiADC for each of the services running on the servers in your Exchange configuration.

In an Exchange configuration that implements all the Exchange services listed in the table on page 8, 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.

On FortiADC, a 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 – so, we need to define an 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 server definitions:

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Services</th>
<th>FortiADC Servers</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</tr>
</tbody>
</table>
So, in the example above, we would need to define 14 servers on FortiADC for the Exchange services hosted on the 6 CAS array servers and 2 Edge servers. Each server would be defined with the IP address of the CAS or Edge server and the port of the appropriate service.

To define FortiADC servers for Exchange, do the following for each required server:

1. Right-click on the **Servers** label in the left frame object tree of the GUI and select **Add Server** from the drop-down menu.
2. In the **Protocol** drop-down box, select tcp.
3. Enter unique **Server Name**, **IP** address, and **Port** parameters. The IP address and port provided must match the IP address and port used by an Exchange service. The default port used by each service is listed in the table above and in the table on page 8.
4. Click **Commit**.

Once you create a server for each IP address/port offering Exchange services in your configuration, the next step is to organize them into server pools and define the load balancing characteristics of each pool.

**Creating Server Pools**

Server pools are groups of servers that can be assigned as a unit to a FortiADC virtual cluster: 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, or same group of services.

For example, in the simplest Exchange configuration outlined in the previous section, the following server pools might be used to logically organize the FortiADC servers:

<table>
<thead>
<tr>
<th>Server Pool</th>
<th>FortiADC Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPpool</td>
<td>CAS1, CAS2</td>
</tr>
<tr>
<td>Mailpool</td>
<td>CAS3-POP CAS3-IMAP CAS4-POP CAS4-IMAP</td>
</tr>
<tr>
<td>RPCpool</td>
<td>CAS5-PM CAS5-MAPI CAS5-AB CAS6-PM CAS6-MAPI CAS6-AB</td>
</tr>
<tr>
<td>SMTPpool</td>
<td>Edge1 Edge2</td>
</tr>
</tbody>
</table>
While 7 clusters are typically used in an Exchange deployment, we can use 4 server pools in our example since several services run on the same set of servers. How you organize servers into server pools for your configuration depends on the distribution of services across your Exchange servers.

Another factor is load balancing policy. All the servers in a server pool share the same load balancing policy. While round-robin is recommended by Microsoft for all Exchange services, you may find that it does not provide optimal load distribution for your configuration for certain services. In this case, you may want to try another load balancing policy offered by FortiADC, such as least connections or adaptive. If you do, you will also want to organize servers into server pools based not only on the services offered by each but also according to the load balancing policy desired for each service.

To create a server pool and add servers to it, do the following:

1. Right-click on the Server Pools label in the left frame object tree and select Add Server Pool from the drop-down menu.

2. Supply a unique name for the server pool.

3. Click Commit.
   The server pool is created and added to the left frame. The server pool’s configuration tab is opened in the right frame. The server pool is created with default parameters, including the server pool load balancing policy – which by default is set to the Microsoft-recommended round-robin policy. See Load Balancing Policy for more information on other policies.

4. Add the appropriate servers to the server pool. For example, in the example on the previous page, if you just created the HTTPpool server pool, add the CAS1 and CAS2 servers to HTTPpool:
   a. Point your mouse at the CAS1 server, then click and hold the left mouse button.
   b. While still holding the button down, move the mouse pointer over the HTTPpool server pool name in the left frame. [As you do this, an icon appears and travels with the mouse pointer; as you move it over the server pool name, it changes to green indicating that a drop operation is permitted.]
   c. While pointing at HTTPpool, release the mouse button. A popup dialog appears allowing you to set options on the server before adding it to the pool: Initial Weight: This number indicates the relative processing power of the server when compared to the other servers in the server pool. In most cases, the default value is a good starting point.
   Quiesce: This option is enabled by default on a new server and prevents any client requests from being routed to the new server. If the server in the CAS array is up and ready to respond to requests, disable this option; otherwise it can be disabled later.
   d. Click Commit to add the server to the server 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.

**Adding Cluster Certificates**

SSL Offloading will be performed on FortiADC for the Outlook Web App, Outlook Anywhere, and ActiveSync services. This requires the installation of the SSL certificate used for these services on FortiADC.

In Version 10, certificates are uploaded to a central certificate store and then assigned to one or more clusters.

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). In this configuration, all three services have a single cluster 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.

Both cluster certificates and client certificates can be added to the store.

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

1. Click the FortiADC hostname at the top of the left frame object tree and open the Global > Certificates tab in the right frame.
2. Click **Add Certificate** at the right of the screen.
3. Type in a unique certificate **Name**.
4. Use the **Browse** buttons to select these files from the system on which you are running your browser:
   a. The file containing the complete certificate chain.
   b. The file containing the associated private key.
      Both these files must be in PEM or PKCS12 format.
5. Click **Commit** to add the certificate and private key to the certificate store.
Configuring 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 cluster that will provide access for all three services and also offload SSL processing from the servers in the CAS array running these services.

We’ll also show you how to create an additional HTTP cluster and a responder to redirect client requests that mistakenly specify the HTTP protocol instead of HTTPS.

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 Cluster for OWA/OA/AS

1. Right-click Clusters in the left frame and select Add Cluster from the popup menu.
2. In the Protocol drop-down box, select https.
3. Do the following:
   a. Enter a name for the cluster (e.g., “OWA_OA_HTTPS”).
   b. Enter the IP address for the cluster. The Fully Qualified Domain Name that clients use to connect to OWA and OA must resolve to this IP address instead of going through the CAS array directly.
   c. Enter the cluster Port (usually 443).
   d. Click Commit to create the cluster.
4. The cluster appears in the left pane and the Configuration tab for the cluster opens in the right pane.
5. Do the following:
   a. Select the appropriate server pool from the Server Pool drop-down box. In our example configuration, this is the HTTPpool server pool (see Creating Server Pools).
   b. Select the desired persistence method from the Persist Type drop-down box. The default cookie persistence is recommended, but source IP persistence can also be used.
   c. Increase the Client Timeout value to 20 seconds. This is the amount of time that FortiADC waits for the client to send all the headers in a client request. If this timer expires, FortiADC sends a timeout to the client.
   d. Enable the Spoof check box.
   e. Enable the Always check box.
   f. Click Commit.
6. Open the Security tab for the cluster, and do the following:

a. Select the appropriate certificate in the Cluster Certificate drop-down box (see Adding Cluster Certificates).
b. If your configuration requires a client certificate for the cluster, select one from the Client Certificate drop-down box. If client certificates are required, enable the Require Client Certificate check box.
c. Click Commit.

---

**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 servers.

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 HTTPS cluster IP address:

---

**Creating an HTTP Redirect Cluster**

Sometimes a client user will specify `http://` instead of `https://` when attempting to connect to OWA, OA, or AS. This section shows you how to create a FortiADC HTTP cluster and responder that will automatically redirect such requests to the HTTPS cluster created in the previous section. First, we create the cluster, then create the responder, and then associate the responder with the cluster via a new cluster match rule.

1. Right-click Clusters in the left frame and select Add Cluster from the popup menu.
2. In the Protocol drop-down box, select `http`.
3. Do the following:
   a. Enter a name for the cluster (e.g., “OWA_OA_HTTP”).
   b. Enter the IP address for the cluster. This is the same IP address used when you created the HTTPS cluster previously.
4. Click Commit.
**HTTPS Cluster for OWA / OA / AS**

c. Enter the cluster **Port (80)**.
d. Click **Commit** to create the cluster.
e. The cluster appears in the left pane and the **Configuration** tab for the cluster opens in the right pane.

4. Enable the **Spoof** check box in the cluster configuration and click **Commit**.

5. Right-click **Responders** in the left frame object tree and select **Add Responder** from the drop-down menu.

6. In the **Add Responder** dialog that appears, do the following:
   a. Enter a unique **Name** for the responder (e.g., “Exch_https_redirect”).
   b. Ensure that the **Redirect Server** button is selected.
   c. Type the following in the **URL** box:
      
   d. **https://$1**
   e. Type the following in the **Regular Expression** box:
   
   f. **http://(.*)**
   g. Select an appropriate **Status** code from the drop-down box.
   h. Enter a **Status Description** to be included in the redirect message returned to the client.
   i. Click **Commit** to create the responder.

7. In the left frame, right-click on the name of the cluster created above (see Step 3) and select **Add Match Rule** from the popup menu. Enter a name for the match rule (or accept the default) and click **Commit**. The new match rule is added to the left frame and the **Configuration** tab for the match rule opens in the right frame.

8. On the match rule **Configuration** tab, select the name of the responder you created in Step 5 from the **Responder** drop-down box.

9. Click **Commit**.
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. POP3 is load balanced using a Layer 4 TCP cluster, with no persistence. SSL offloading is not performed by FortiADC for POP3.

Creating a POP3 Layer 4 TCP Cluster

1. Right-click FortiADC in the left frame and select Add Cluster from the popup menu.
2. In the Protocol drop-down box, select tcp.
3. Do the following:
   a. Enter a name for the cluster (e.g., “POP3_TCP”).
   b. Enter the IP address for the cluster. The Fully Qualified Domain Name that clients use to connect to POP3 must resolve to this IP address instead of going through the CAS array directly.
   c. Enter the cluster Port (995 – this is the standard port for POP3 over SSL).
   d. Click Commit to create the cluster.
   e. The cluster appears in the left pane and the Configuration tab for the cluster opens in the right pane.
4. Do the following:
   a. Select the appropriate server pool from the Server Pool drop-down box. In our example configuration, this is the Mailpool server pool (see Creating Server Pools).
   b. Enable the Spoof check box.
   c. Click Commit.
**Configuring FortiADC for IMAP4**

To support mailbox access from IMAP4 clients, you need to start the IMAP4 service on the Exchange Client Access Servers. For clients to send email through Exchange, you’ll also need to configure SMTP.

IMAP4 is load balanced using a Layer 4 TCP cluster, and persistence is not needed for IMAP4. SSL offloading is not performed by FortiADC for IMAP4.

Creating an IMAP4 Layer 4 TCP Cluster

1. Right-click FortiADC in the left frame and select Add Cluster from the popup menu.
2. In the Protocol drop-down box, select tcp.
   a. Do the following:
   b. Enter a name for the cluster (e.g., “IMAP4_TCP”).
   c. Enter the IP address for the cluster. The Fully Qualified Domain Name that clients use to connect to IMAP4 must resolve to this IP address instead of going through the CAS array directly.
   d. Enter the cluster Port (993 – this is the standard port for IMAP4 over SSL).
   e. Click Commit to create the cluster.
3. The cluster appears in the left pane and the Configuration tab for the cluster opens in the right pane.
4. Do the following:
   a. Select the appropriate server pool from the Server Pool drop-down box. In our example configuration, this is the Mailpool server pool (see Creating Server Pools).
   b. Enable the Spoof check box.
   c. Click Commit.
Configuring FortiADC for RPC Client Access

Load balancing RPC Client Access services through FortiADC requires three Layer 4 clusters, 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 the RPC CA clusters are configured to use Layer 4 sticky persistence (client or source IP persistence).

Creating the RPC CA Portmapper Layer 4 TCP Cluster

1. Right-click FortiADC in the left frame and select Add Cluster from the popup menu.
2. In the Protocol drop-down box, select tcp.
3. Do the following:
   a. Enter a name for the cluster (e.g., “Portmap_TCP”).
   b. Enter the IP address for the cluster. The Fully Qualified Domain Name that clients use to connect for RPC Client Access must resolve to this IP address instead of going through the CAS array directly.
   c. Enter the cluster Port (135 – this is the standard port for the Portmapper).
   d. Click Commit to create the cluster.
   e. The cluster appears in the left pane and the Configuration tab for the cluster opens in the right pane.
4. Do the following:
   a. Select the appropriate server pool from the Server Pool drop-down box. In our example configuration, this is the RPCpool server pool (see Creating Server Pools).
   b. Set the Sticky Timeout slider to the number of seconds that client/server connections will persist. Microsoft generally recommends one hour (3600 seconds) for load balancer timeouts, though some application may require longer timeouts. Outlook clients assume that all RPC connections are made to the same server, and Outlook opens multiple connections per session, so you want to set this value to the longest anticipated user session, so that the user does not have to close their current connection and reconnect during a session.
   c. Enable the Inter Cluster Sticky option.
   d. Click Commit.
Creating the RPC CA MAPI Layer 4 TCP Cluster

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. Right-click FortiADC in the left frame and select Add Cluster from the popup menu.

3. In the Protocol drop-down box, select tcp.

4. Do the following:
   a. Enter a name for the cluster (e.g., “MAPI_TCP”).
   b. Enter the IP address for the cluster. The Fully Qualified Domain Name that clients use to connect for RPC Client Access must resolve to this IP address instead of going through the CAS array directly.
   c. Enter the cluster Port (59532).
   d. Click Commit to create the cluster.

5. Do the following:
   a. Select the appropriate server pool from the Server Pool drop-down box. In our example configuration, this is the RPCpool server pool (see Creating Server Pools).
   b. Set the Sticky Timeout slider to the number of seconds that client/server connections will persist. Microsoft generally recommends one hour (3600 seconds) for load balancer timeouts, though some application may require longer timeouts. Outlook clients assume that all RPC connections are made to the same server, and Outlook opens multiple connections per session, so you want to set this value to the longest anticipated user session, so that the user does not have to close their current connection and reconnect during a session.
   c. Enable the Inter Cluster Sticky option.
   d. Click Commit.
Creating the RPC CA Address Book Layer 4 TCP Cluster  

**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):

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

2. Right-click FortiADC in the left frame and select Add Cluster from the popup menu.

3. In the Protocol drop-down box, select tcp.

4. Do the following:
   a. Enter a name for the cluster (e.g., “AddrBook_TCP”).
   b. Enter the IP address for the cluster. The Fully Qualified Domain Name that clients use to connect for RPC Client Access must resolve to this IP address instead of going through the CAS array directly.
   c. Enter the cluster Port (59533).
   d. Click Commit to create the cluster.
   e. The cluster appears in the left pane and the Configuration tab for the cluster opens in the right pane.

5. Do the following:
   a. Select the appropriate server pool from the Server Pool drop-down box. In our example configuration, this is the RPCpool server pool (see Creating Server Pools).
   b. Set the Sticky Timeout slider to the number of seconds that client/server connections will persist. Microsoft generally recommends one hour (3600 seconds) for load balancer timeouts, though some application may require longer timeouts. Outlook clients assume that all RPC connections are made to the same server, and Outlook opens multiple connections per session, so you want to set this value to the longest anticipated user session, so that the user does not have to close their current connection and reconnect during a session.
   c. Enable the Inter Cluster Sticky option.
   d. Click Commit.
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 an SMTP Layer 4 TCP Cluster

1. Right-click FortiADC in the left frame and select Add Cluster from the popup menu.
2. In the Protocol drop-down box, select tcp.
3. Do the following:
   a. Enter a name for the cluster (e.g., “SMTP_TCP”).
   b. Enter the IP address for the cluster. The Fully Qualified Domain Name that clients use to connect to SMTP must resolve to this IP address instead of going through the CAS array directly.
   c. Enter the cluster Port (25 – this is the standard SMTP port).
   d. Click Commit to create the cluster.
   e. The cluster appears in the left pane and the Configuration tab for the cluster opens in the right pane.
4. Do the following:
   a. Select the appropriate server pool from the Server Pool drop-down box. In our example configuration, this is the SMTPpool server pool (see Creating Server Pools).
   b. Click Commit.
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 HTTP 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 clusters, 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

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:
3. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA
4. On the Registry Editor menu, click Edit > New > DWORD. A new key appears in the right pane of the editor.
5. Enter SSLOffloaded for the new key Name and press <Enter>.
6. Right-click the new SSLOffloaded key and select Modify from the popup menu.
7. In the Value data field, type 1 (the number one). Click OK to save your changes.
8. Select File > Exit to close the Registry Editor.
9. 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 HTTPS cluster, as shown in this table:

<table>
<thead>
<tr>
<th>Exchange Component</th>
<th>Home Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook Anywhere</td>
<td>Exchweb</td>
</tr>
<tr>
<td>Outlook Web Access</td>
<td>owa</td>
</tr>
<tr>
<td>ActiveSync</td>
<td>Microsoft-Server-ActiveSync</td>
</tr>
</tbody>
</table>

4. Click the name of the home page in the left pane.

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

6. In the **Actions** pane at right, click **Apply**.

7. 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.