IIS 8.0 Reverse Proxy Deployment

Prepared By: Samir Sadikhov APAC_Operations@mediaocean.com
Date Prepared: 12 Feb 2016

Purpose

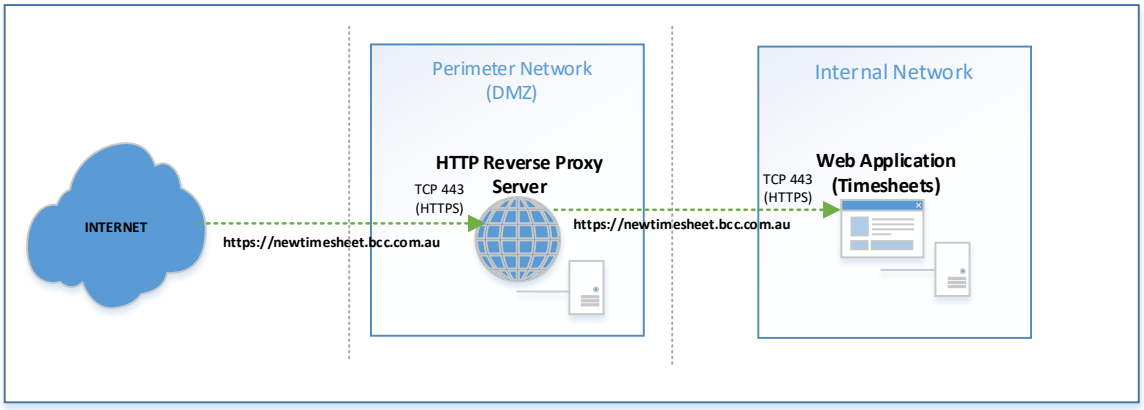
The purpose of this document is to describe the deployment steps of reverse proxy server using IIS role in Windows 2012 Server.

The solution provides implementation of a secure layer to the Mediaocean web applications for those agencies wishing to access Mediaocean web applications from the internet.

General information on reverse proxy server can be found here:

https://en.wikipedia.org/wiki/Reverse_proxy

Architecture Diagram



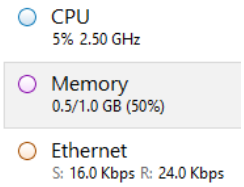
Network requirements

The Reverse proxy server resides in DMZ network. This requires incoming port tcp/443 to be opened from the internet towards the Reverse proxy server in DMZ, and port tcp/443 from Reverse Proxy server in DMZ towards the web service residing on the internal network.

Public DNS entries must be created to access the reverse proxy server over the internet. Hosts file on the reverse proxy server will need to include the server name of the Web server on the internal network

Minimum System requirements

CPU: 1 core
RAM: 1GB
Network: 1 interface on the perimeter network (DMZ)
Disk Space: C: 50GB
OS: Windows 2012 Server Standard
A valid SSL certificate installed on the IIS server that will host the reverse proxy



Assumptions

A valid Web application running on internal network and is accessible via SSL. Valid SSL certificate has been installed on the web service.

Deployment Steps

1. On the perimeter network (DMZ) install Windows 2012 Server Standard environment with all required Windows updates. Please refer to System Requirements for the size of the server.

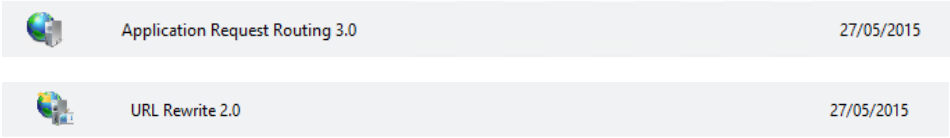
   Note: The server should not need to be on the domain and can be either physical or virtual server.

2. Install Internet Information Services (IIS) from Add Roles and Features Wizard.

3. Using Microsoft Web Platform Installer (WPI), download and install the following two components for IIS:

   a. Application Request Routing

   b. URL Rewrite



Microsoft WPI can be downloaded from:

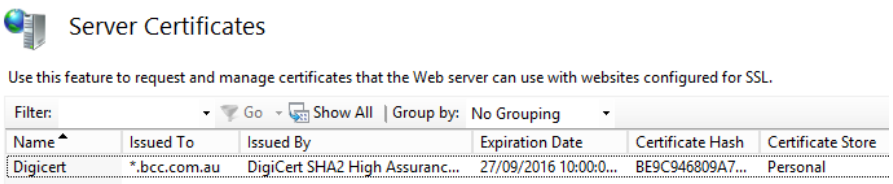
https://www.microsoft.com/web/downloads/platform.aspx,

Alternatively, you can use extracted .msi packages and install them manually.

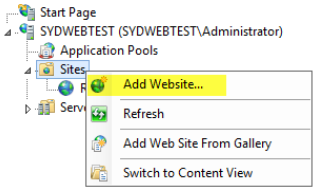
Configuration Steps

1. Open IIS, on the left pane, select the server and using “Server Certificates” install a public SSL certificate. Please refer to your SSL certificate service provider instructions on how to create CSR and generate SSL certificates.

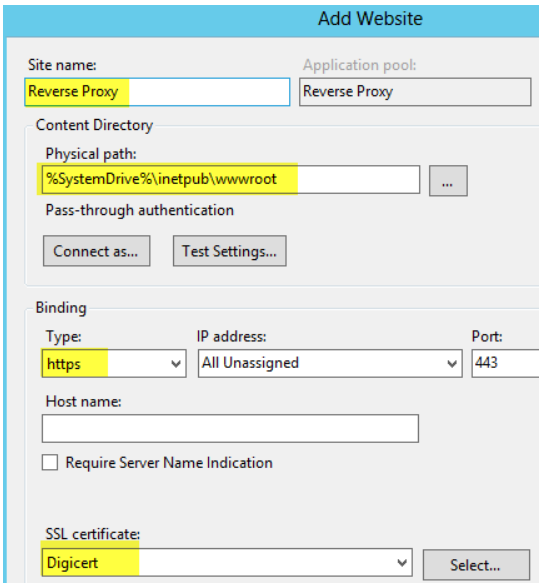
   In our example we are using a wildcard certificate from Digicert as shown below.



2. Right click “Sites” folder on the left pane and Add a new web site

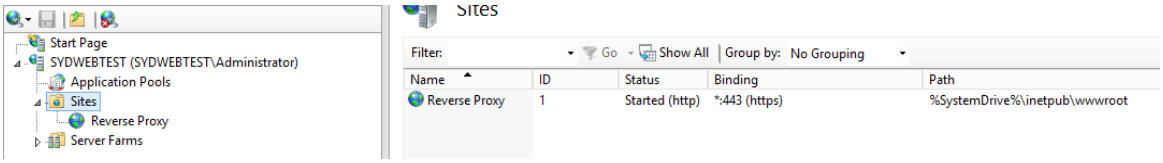


3. Configure the following Web Site parameters (refer to screenshot below):
    a. **Site Name**: This is how the service will be displayed in IIS
    b. **Physical Path**: Default path to the files for the web site (this portion is not critical as we are not hosting any web site, will be using a URL rewrite module to configure the service, so stick with defaults as the field is mandatory)
    c. **Binding Type**: https – we want to run it over a secured http connection.
    d. **SSL certificate**: Select the SSL certificate you have installed in the previous steps.



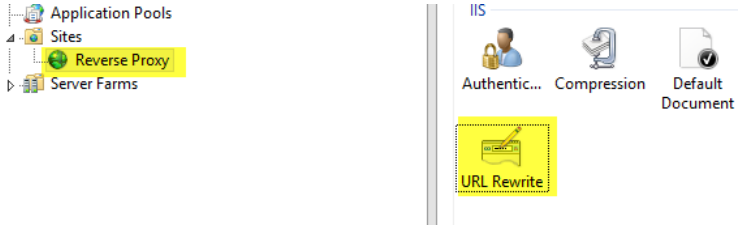
    e. Click Ok

4. Ensure the site is started.



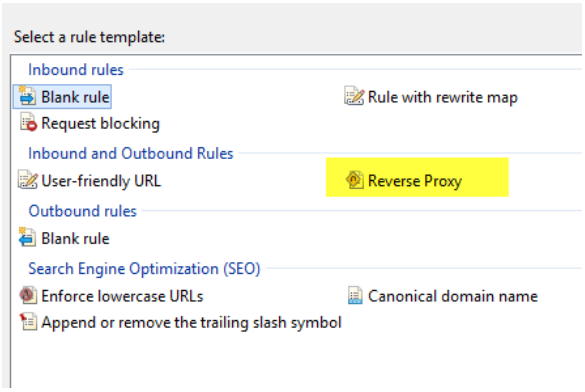
Now that we have configured the site to respond on port 443, we need to configure the redirection to our internal services.

5. Select the site and click on URL Rewrite

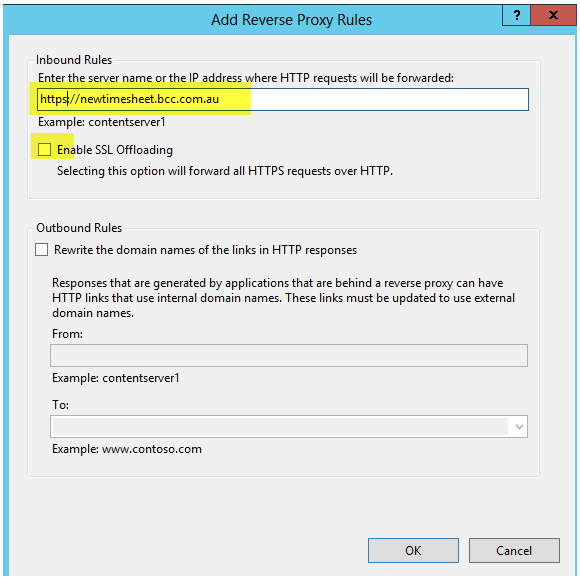


6. On the right pane select Add Rules…

7. Click on Reverse Proxy

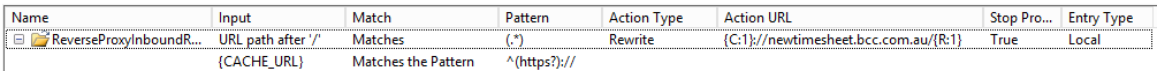


8. In the Reverse Proxy rule window, provide the internal server name and ensure “Enable SSL Offloading” is not ticket. We will be connecting via SSL to the internal server, therefore we do not need to offload.



Click OK to complete Rule configuration.

9. After you added the rule, it should look like this in the URL Rewrite module.



Congratulations! This completes Reverse Proxy setup.

You can use the same Site for configuring reverse proxy for other internal web sites, for which you only need to add and configure a URL Rewrite Rule as outlined in the previous steps. If you use the same internal server hosting multiple web services, a use of host headers or additional IP addresses is essential to distinguish between different web sites, but this is out of scope of reverse proxy deployment.

Post setup instructions

As mentioned in the server requirements, you will need to edit the host file to be able to resolve the internal server names. At the minimum the host file should include the name of the web server on the internal network.

C:\Windows\System32\Drivers\etc

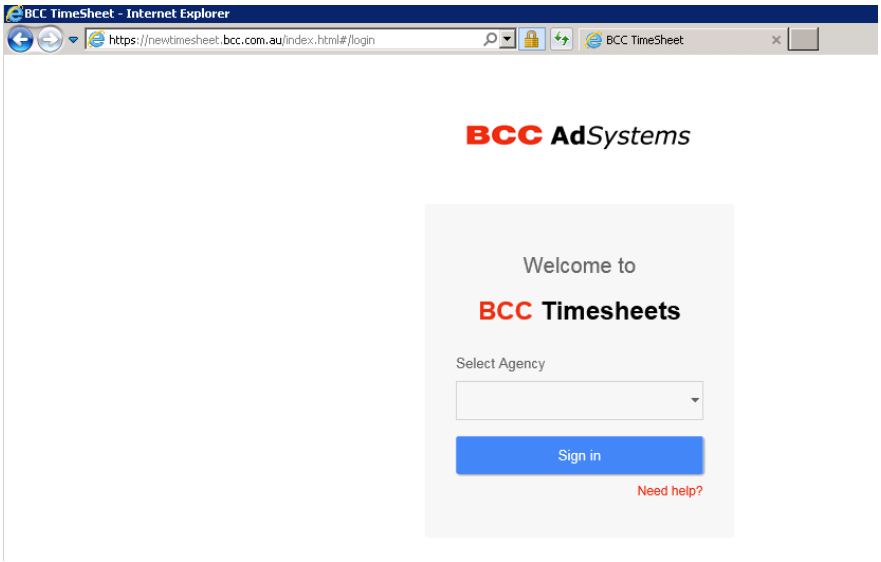
```
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

192.168.1.193           newtimesheet.bcc.com.au
```

Agency may choose to use internal DNS services to resolve names in DMZ network, but for security reasons we advise against using this method of name resolution and use hosts file instead.

Testing

To test the functionality of the reverse proxy server:

1. Please ensure you are outside of the internal network (e.g. 3G/4G network)
2. Open Internet browser and connect to the external URL. Your default page of the web application should be displayed. In our example we are connecting to the timesheet application: https://newtimesheet.bcc.com.au/index.html which brings up the Web interface of the Web Timesheet application located on the internal network.



This proves that we have configured Reverse proxy server correctly.

Troubleshooting Steps

- Ping your internal web server name from Reverse proxy server, the name should be resolved to the correct IP address. Please ensure this IP address is configured on your internal Web server. If you can't, please check your hosts file entries.

- From reverse proxy server, please ensure you can reach the internal web services by opening the URL in the browser. In our case it is:

  https://newtimesheet.bcc.com.au/index.html

  If you can't, please check your firewall rules between DMZ and internal network are configured correctly as per Network Requirements.

- In IIS on the reverse proxy server, ensure the Web site is started.