Delete because of Duplicate - ISA Server 2006 as Reverse Proxy for SAP Applications

Introduction

Some of our active SDN members have already discussed the reverse proxy implementation on most of the servers other than ISA Server Series. Since we did not have proper help on the configuration of reverse proxy on ISA Server, we had faced some difficulties while implementing the same. This has motivated me to write something on the same and I believe, this information would be really helpful to those who are planning to implement their reverse proxy scenarios on ISA Server series. Here, I will discuss the implementation of reverse proxy on ISA Server 2006.

Important Terms and Definitions

ISA Server

Internet Security and Acceleration (ISA) Server is the integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users with fast and secure remote access to applications and data.

DMZ (DeMilitarized Zone)

A neutral zone that exists between two networks (intranet and internet) that allows connections between the networks.

ISA Server Management

Microsoft ISA Server 2006 can be administered using ISA Server Management. ISA Server Management is a snap-in console in Microsoft Management Console (MMC)

Web Publishing Rule

A rule that is configured to specify how incoming requests to Web Servers will be handled.

Web Listener

The Web Listener specifies the IP addresses and the port on which the ISA Server computer listens for incoming Web requests.

Key Features available in ISA Server 2006

Compared to other servers, ISA server 2006 has the following benefits:

- Better and more advanced protection with additional firewall
- Ease of use and improved management interface
- Web Publishing Load Balancing
- HTTP Compression
- Improved Alerting
- Better Network Integration

Because of these additional benefits, nowadays, most of the customers prefer to implement their reverse proxy scenarios on ISA Server series.

Recommended Landscape

In general, the ISA server 2006 should be located in the DMZ. The SAP servers are located in the Intranet. Below attached figure describes the recommended landscape and a DMZ scenario.

Prerequisite

To use ISA Server, we need

- A personal computer with a 550-megehertz or faster processor. (You need to use a server class machine for production environments).
- Microsoft Windows Server? 2003 operating system with Service Pack 1 (SP1) or Microsoft Windows Server 2003 R2 operating system. (You cannot install ISA on 64-bit versions of Windows Server 2003 operating systems).
- Minimum 256MB RAM should be present. (You should change appropriately for production environments)
- 150 MB of available hard disk space. This is exclusive of hard disk space you want to use for caching.
- One network adapter that is compatible with the computers operating system, for communication with the internal Network. (An additional network adapter for each network connected to the ISA server computer. If you want to implement external scenario also, then you need...
Steps to be followed

You need to perform the below mentioned minimum steps to implement reverse proxy on ISA Server 2006

I) Create Web Publishing Rule

1. Specify Web Publishing Rule Name
2. Select the Rule Action Type
3. Select the Publishing Type
4. Select the Server Connection Security
5. Specify Internal Publishing Details
6. Specify Public Name Details
7. Create Web Listener
   7.1 Specify Web Listener Name
   7.2 Select Client Connection Security
   7.3 Specify Web Listener IP Addresses
   7.4 Select Authentication Settings
   8. Select Authentication Delegation
   9. Specify User Sets

II) Publishing all necessary paths

III) Changing the target port

IV) Activate Link Translation

I) Create Web Publishing Rule

In order to make the SAP applications accessible via the Microsoft ISA Server, you need to define a new Web Server Publishing Rule. For this, in the ISA Server Management, Right click on "Firewall Policy" and choose "New->Web Site Publishing Rule". Wizard for creating Web Publishing Rule will be popped up. Web Publishing Rule determines how the incoming requests to the server will be handled.

1. Specify Web Publishing Rule Name

You can specify the name of the web publishing rule here.

2. Select the Rule Action Type

You need to select the Rule Action Type here. This specifies how you want this rule to respond when the rule conditions are met. We have two rule action types, "Allow" and "Deny".

3. Select the Publishing Type

Here you have to select the publishing type. Select if this rule will publish a single Web Site or external load balancer, a web server farm, or multiple web sites.

4. Select the Server Connection Security

Choose the type of connections ISA Server will establish with the published Web Server or Server farm. We have two types of connection types; one is secured connections and the other non-secured connections. For this test scenario, I preferred the non-secured connection.

5. Specify Internal Publishing Details

You need to specify the internal name of the Web Site you are publishing. This is the name internal users type into their browsers to reach the Web Site. The ISA server should be able to resolve the IP address or the name of the internal server specified.

Specify the internal path and publishing options of the published web site. Based on this, we can publish the entire web site or limit access to a specified folder. For portal, it is /irj* and for BSP applications, it is /sap*. For proper functionality, the check box for "Forward original host header instead of actual" should have been selected.
6. Specify Public Name Details
You need to specify the public domain name or IP address users will type to reach the published web site. The public domain name should be a registered one.

7. Select / Create Web Listener
Web listener specifies the IP address and the port on which the ISA server computer listens for incoming Web Requests. If the Web Listener is already created, then you only have to select the same, otherwise you need to create Web Listener. Web Listeners specify how ISA server listens for and authenticates incoming Web requests from clients.

7.1 Specify Web Listener Name
For creating Web Listeners, you need to specify the Web Listener name.

7.2 Select Client Connection Security
This specifies the type of connections the Web Listener will establish with clients. We have two types of client connection securities, one is secured and the other non-secured. For this test scenario, I preferred the non-secured connection type.

7.3 Specify Web Listener IP Addresses
If all requests are coming from internet, we need to select only the "External". If you want to access the published applications inside your network also, then you need to select the "Internal" also.

7.4 Select the Authentication Type
Select how clients will authenticate to ISA server, and how ISA Server will validate their credentials.

Specify the port that the ISA Server computer will use to listen on the selected IP addresses for incoming web requests. For HTTP connections, the port is 80 and for HTTPS connections, port is 443. Below attached figure is for secure HTTP connections.

Web Listener will be created after this step and you can select the created web listener just like in the below attached picture.

8. Select Authentication Delegation
Authentication Delegation is the method ISA server uses to authenticate the session it opens with the published site. If the published Web Server requests HTTP authentication, ISA server will not pass the authentication request to the user.

9. Specify User Sets
We can limit the requests from users using User Sets. We can apply the rule to requests from all users or we can limit access to specific user sets.

Web publishing rule has been created after this step and you can configure it based on your landscape.

II) Publishing all necessary paths
Based on your requirement, you need to mention all the necessary paths to be published. For exposing portal, normally you need to add /irj/, /logon/, /servlet/, and /webdynpro/. For adding these additional paths, you have to take the properties of the created rule by right clicking and selecting the Properties from the context menu.
III) Changing the target port

By default, the web server publishing rule redirects the incoming requests to the standard port 80 on the specified target. Based on your requirement, you need to change this target port. If it is an SAP Enterprise Portal, you need to change the target port to 5<Instance Number>-00 (HTTP port) and for BSP applications, you need to mention the Web Application Server listening port. For this, in the properties dialog of the Web Publishing Rule, go to the tab "Bridging" and mention the appropriate value there. For HTTPS connection, you need to mention the HTTPS port of the portal server just like mentioned in the picture attached below.

IV) Activate Link Translation

To make sure that no fully-qualified static links may reference internal host names, you need to activate the Link translation functionality. In the Web Publishing Rule's properties dialog, go to the "Link Translation" tab. Here you have to check the option "Apply link translation to this rule" and add a new dictionary entry.

You need to perform these minimum steps to configure reverse proxy on ISA Server 2006 and can publish your SAP Applications over internet!!!

Useful Links

- https://weblogs.sdn.sap.com/pub/wlg/1128
- http://www.isaserver.org/tutorials/
- https://partner.microsoft.com/40029027

Refer My Blog on the same