



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957

Fax: 919.217.5769

PUBLISHING SHAREPOINT PORTAL SERVER VIA ISA SERVER 2000

Products: SharePoint Portal Server 2001, Internet Security & Acceleration Server 2000

Overview

SharePoint Portal Server 2001 offers a compelling knowledge management solution with an integrated web interface. However, this web interface is not initially configured for access outside the local intranet. At the same time, Internet Security & Acceleration (ISA) Server 2000 offers an integrated firewall and web proxy solution, including publishing rules that allow external access to internal servers.

By combining the web interface of SharePoint Portal Server 2001 with ISA Server 2000's powerful web publishing rules, it becomes possible to provide web-based access to a knowledge management system from any supported browser across any Internet connection. This includes the use of Secure Sockets Layer (SSL), which provides encryption for the traffic as it moves between the web browser and the web server.

This technical note describes the steps required to publish SharePoint Portal Server 2001 via an ISA Server 2000 web publishing rule.

More Information

The following assumptions are made in this technical note in describing the configuration required to publish SharePoint Portal Server via ISA Server:

- The server running SharePoint Portal Server will be accessible via the fully qualified domain name of portal.company.com. This server's NetBIOS name may or may not be PORTAL.
- The portal.company.com FQDN is registered in an external DNS and is visible to external clients. The IP address that this FQDN resolves to should be the external IP address of the ISA Server.

These assumptions are illustrated visually in the following diagram.

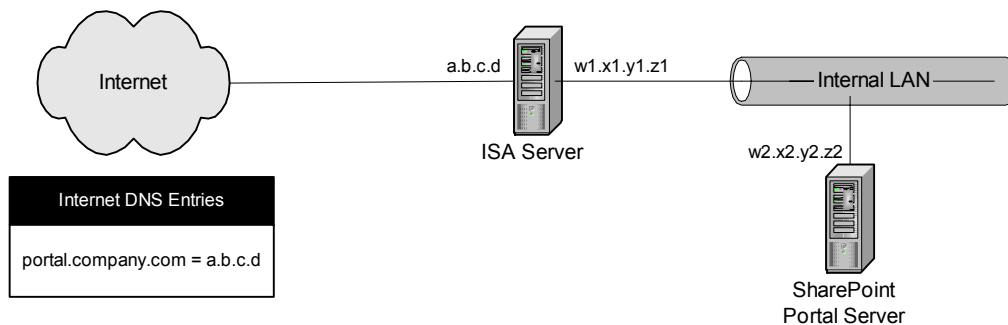


Figure 1. Network diagram for SharePoint Portal Server web publishing

Configuring SharePoint Portal Server

In order for SharePoint Portal Server to be published via ISA Server 2000, SharePoint must be configured to support fully qualified domain names (FQDNs) and Secure Sockets Layer (SSL). By default, SharePoint is not configured to support either FQDNs or SSL.

Two additional technical notes are available that describe the steps required to add support for FQDNs and SSL to SharePoint Portal Server:

- Enabling FQDNs on SharePoint Portal Server
- Enabling SSL on SharePoint Portal Server

Once the steps outlined in these two technical notes have been completed, SharePoint Portal Server should be accessible via a FQDN both with and without SSL. Make note of the FQDN used to access SharePoint (portal.company.com in this example); this FQDN will need to be specified in the ISA Server 2000 web publishing rule.

Configuring Internet Security & Acceleration Server

To configure ISA Server 2000 to publish SharePoint Portal Server, a number of different policy elements will need to be created. These include a destination set for the FQDN used to access SharePoint (see previous paragraph) and a web publishing rule to direct traffic for that destination set to the SharePoint server. In addition, the inbound web listener may need to be configured to support SSL, if that will be included in the final solution. Each of these steps is discussed in more detail in the following sections.

Configuring the Inbound Web Listener

If SSL support is required, the inbound web listener must be configured. Before starting the configuration of the inbound web listener, make sure that the SSL certificate installed on the SharePoint Portal Server has been exported and that the private key was marked as exportable during that process. That certificate will need to be imported and installed onto the ISA Server during this process. In addition, verify that the FQDN on the certificate matches the FQDN that provides access to SharePoint Portal Server (in our example, it should be portal.company.com).

To configure the inbound web listener, follow these steps.

1. In the ISA Management console, right-click the server object and select Properties.
2. Click on the Incoming Web Requests tab.
3. Select the “Configure listeners individually per IP address,” then select the default listing and click the Edit button.
4. In the Add/Edit Listeners dialog box, click the check box labeled “Use a server certificate to authenticate to web clients”.
5. Click the Browse button to select the previously imported SSL certificate whose common name matches the FQDN for which SharePoint Portal Server has been configured. It is important that these FQDNs—on the certificate and on SharePoint Portal Server—match exactly.
6. Select Integrated authentication, then click OK.
7. Back on the server properties dialog box, click the check box labeled “Enable SSL listeners”. Be sure that the SSL port listed is 443.
8. Click OK to return to the ISA Management console.

Upon completing the configuration of the inbound web listener, the web proxy service will need to be restarted. After the web proxy service has restarted, verify that it started successfully by checking the Application log in Event Viewer, then proceed with creating the destination set and web publishing rule.

Creating the Destination Set

The destination set is a critical component of the final solution. The destination set is used to determine how to route a client’s incoming web request based on the URL. This allows ISA Server to route incoming web requests to different internal web servers based on host header or URL path. Using this functionality, it is possible to use a single external hostname to provide access to multiple internal web-based applications based on the URL. For example, <http://www.company.com/workspace> could point to a SharePoint Portal Server workspace, and <http://www.company.com/exchange> could point to Exchange 2000 Outlook Web Access.

To create the destination set, use the following steps.

1. In the ISA Management console, expand the Policy Elements container to show the Destination Sets container. This container holds all defined destination sets.
2. Right-click on the Destination Sets container and select New > Destination Set. The New Destination Set dialog box will appear.
3. Supply a name for the destination set, and optionally, a description.
4. Click the “Add...” button to open the Add/Edit Destination dialog box. Here the actual URL definition is created.

5. In the Destination text box, supply the FQDN for which SharePoint has been configured. As with the SSL certificate used in configuring the inbound web listener, it is important that the FQDN used in the destination set exactly match the FQDN for which SharePoint has been configured, or SharePoint access through ISA Server will not function properly.
6. In the Path text box, type “/workspace*” (without quotes), where “workspace” is the name of the workspace being published. Click OK to close the Add/Edit Destination dialog box and return the New Destination Set dialog box. The hostname and path just entered will be listed in the bottom section.
7. Click OK to save the destination set and return to the ISA Management console. The newly created destination set will be listed in the Destination Sets container.

Now that the destination set has been created, it is time to create the web publishing rule.

Creating the Web Publishing Rule

The web publishing rule is the part that actually routes the traffic. Using the destination set as a building block, the web publishing rule is responsible for making decisions regarding the traffic received by the inbound web listener. There can be multiple web publishing rules in place, and the rules are processed in order from first to last. If a specific URL is not granted by a web publishing rule, then it is denied by the built-in last rule. This follows a well-known security guideline that states that traffic that is not explicitly allowed should be denied.

Before creating the web publishing rule, a DNS entry must first be added to the ISA Server's local HOSTS file. Because the ISA Server uses external DNS for name resolution, attempts to resolve portal.company.com (the FQDN used in this example to publish SharePoint Portal Server) would return the external IP address (shown as a.b.c.d in Figure 1). To prevent this from happening, add an entry for portal.company.com with the internal IP address of the SharePoint Portal Server to the HOSTS file on the ISA Server (shown as w2.x2.y2.z2 in Figure 1). After adding this entry, name resolution attempts from the ISA Server should return the internal IP address.

To create the web publishing rule, use the steps listed below.

1. In the ISA Management console, expand the Publishing node to show the Web Publishing Rules container.
2. Right-click on the Web Publishing Rules container and select New > Rule. The New Web Publishing Rule Wizard opens.
3. Specify a name for this web publishing rule, then click Next.
4. Select the destination set created in the previous section, then click Next.
5. Select how to limit the requests (if at all), then click Next.
6. Select “Redirect the request to this internal Web server”, then specify the FQDN that SharePoint is configured to support (in this example, portal.company.com). As in previous steps, this hostname must match the hostname on the SSL certificate, on the destination set, and on SharePoint Portal Server itself.
7. Be sure that the “Send original host header to the publishing server instead of the actual one (specified above)” is checked. Click Next.

8. Click Finish.
9. To verify SSL bridging, right-click the new web publishing rule and select Properties.
10. Click on the Bridging tab, then be sure that “Redirect SSL requests as SSL (establish a new secure channel to the site)” is selected. To enforce the use of SSL, also be sure that the check box for “Require secure channel (SSL) for published site” is also selected.

It is important to note that the FQDN used to reference the SharePoint Portal Server, `portal.company.com`, should be identical at every step along the way: on the SSL certificate assigned to the inbound web listener on the ISA Server, in the destination set on the ISA Server, in the “Redirect to” box of the web publishing rule on the ISA Server, on the SSL certificate installed on the SharePoint server, and on the SharePoint Portal Server itself. Because SharePoint appears to be so heavily dependent upon the host header, it is critical for success that it remains constant throughout the entire process.

At this point, access to the SharePoint Portal Server workspace should be possible from the outside using the `portal.company.com` hostname and the name of the workspace included in the web publishing rule, e.g., <http://portal.company.com/workspace>.

Troubleshooting

If access to the SharePoint Portal Server workspace is not available from the outside, check some of the following items.

- As mentioned earlier, ensure that the hostname/host header remains constant throughout the entire chain.
- Be sure to have an entry in the HOSTS file on the ISA Server that points the FQDN used to access the SharePoint server to the corresponding internal IP address (noted as `w2.x2.y2.z2` in Figure 1). Note that it may also be necessary to add a similar entry to the HOSTS file on the SharePoint Portal Server itself that references the FQDN to the local IP address.
- Be sure that you can access the SharePoint workspace internally, without going through ISA Server, using the FQDN. If this fails, then the problem most likely resides with SharePoint and not with ISA Server.
- If IIS has is installed on the ISA Server, then the IIS web sites need to be stopped or socket pooling needs to be disabled. Otherwise, IIS will bind to the SSL port (TCP port 443) and prevent ISA from doing so. (In this case, an event will be written to the Application log indicating that ISA could not bind TCP port 443 to the interface because it is already in use.) Stopping the web sites in IIS or disabling socket pooling will correct the problem.

Other Notes

The information regarding the correct configuration of SharePoint Portal Server 2001 in an extranet scenario was heavily derived from material in Microsoft’s white paper titled “Deploying SharePoint Portal Server 2001 Across an Extranet.” This white paper is available from the SharePoint area of Microsoft’s web site.

Also, note that the use of Integrated Authentication on the inbound web listener is only supported for Internet Explorer 5.0 or later. Basic authentication must be used in all other instances.

Related Articles/Resources

None

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.