

# SOPHOS



sophos **nac**

ADVANCED

Configuring Microsoft ISA  
Server 2004



Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in retrieval system, or transmitted, in any form or by any means electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names are trademarks or registered trademarks of their respective owners.

Document version 3.2  
Published January 2011

## Table of Contents

Configuring Microsoft ISA Server 2004 as a Proxy .....	4
Overview.....	4
Considerations.....	4
Configuring Microsoft ISA Server 2004 .....	4
Configuring a Web Listener .....	4
Configuring a Secure Web Server Publishing Rule.....	5
Configuring ISA Server to Proxy Requests from Sophos.....	7

## Configuring Microsoft ISA Server 2004 as a Proxy

### Overview

This document provides detailed information about the process necessary to configure the Microsoft® ISA Server 2004 to act as a proxy for the Sophos Compliance Application Server. The ISA Server acts as a proxy for inbound connections to the Compliance Application Server for both management and Sophos Compliance Agent access, and as outbound proxy for the Compliance Application Server when it is retrieving Microsoft OS patch definition updates from the Sophos update server.

**Note:** When you make any changes to the ISA Server, you need to save the changes by clicking the Apply button that appears on the top of the Management Console page. In some cases, you may need to restart the ISA Server service.

### Considerations

The configuration process of the Microsoft ISA Server to act as a proxy for the Compliance Application Server depends on the following prerequisites:

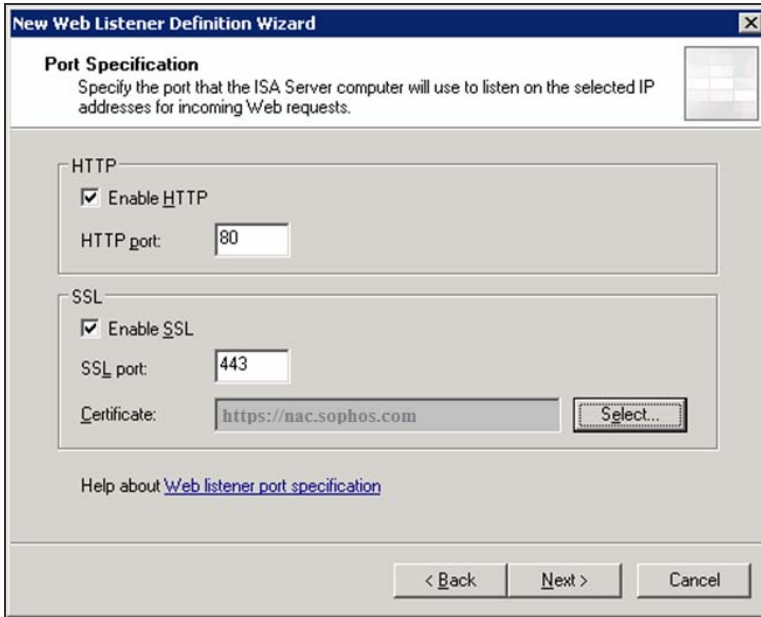
- Microsoft ISA Server 2004 Standard Edition or Enterprise Edition has been installed with the default configuration and no configuration changes have been made.
- The Microsoft ISA Server has been configured with both an internal and external network interface and each interface has been connected to the network.
- The Compliance Application Server is on the internal side of the ISA Server.
- A valid SSL Certificate signed by a trusted authority is installed on the server that will host ISA through the Certificates snap-in. More information on this topic is in the Microsoft Knowledge Base Article 324167.

## Configuring Microsoft ISA Server 2004

### Configuring a Web Listener

By default, ISA Server 2004 does not listen for incoming requests, so you must configure a Web listener to publish the Sophos Web site.

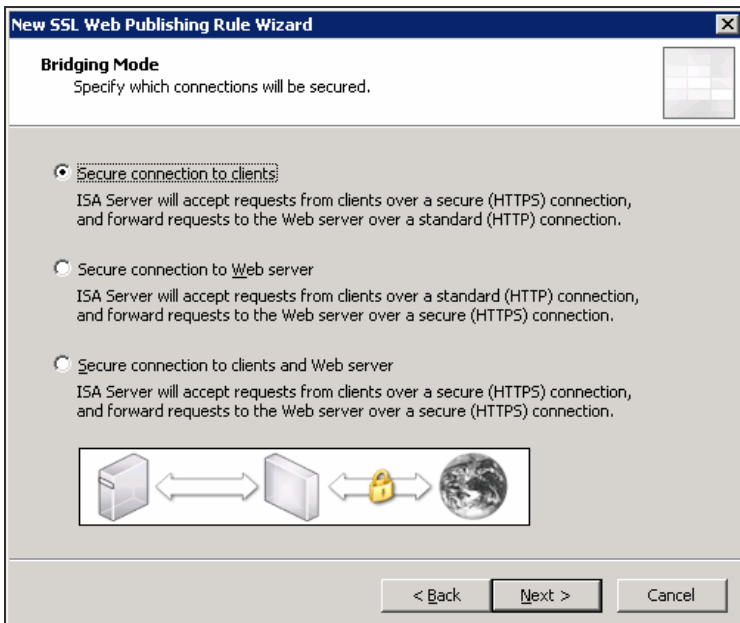
1. In the ISA Server console, select **Firewall Policy** for the computer node, the name of your ISA Server that is going to accept the incoming connection, and then select **Network Objects** on the **Toolbox** tab.
2. Right-click the **Web Listeners** folder, and then select **New Web Listener** to open the New Web Listener Definition Wizard.
3. Type a Web listener name, and then click **Next**.
4. On the **IP Addresses** panel, select **External** network from the **Listen for request from these networks** list box, and then click **Next**.
5. Select the **Enable HTTP** and **Enable SSL** check boxes.
6. Click **Select** to select a certificate.
7. Select the certificate, click **OK**, and then click **Next**.



8. Click **Finish** to complete adding the Web listener.
9. Click **Apply** above the **Firewall Policy** tab to save the changes.

## Configuring a Secure Web Server Publishing Rule

1. In the ISA Server console, right-click **Firewall Policy** for the computer node and from the **New** menu, select **Secure Web Server Publishing Rule**.
2. Type an SSL Web publishing rule name, and then click **Next**.
3. In the Publishing Mode window, select **SSL Bridging**, and then click **Next**.
4. Click the **Allow** option button in the Select Rule Action window, and then click **Next**.
5. Click the “**Secure connection to clients**” option button on the Bridging Mode window, and then click **Next**.



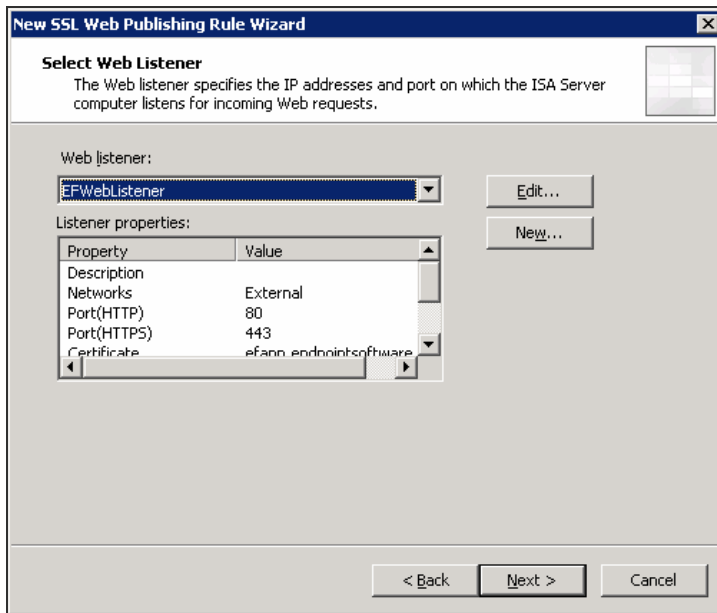
6. Type the public name of the Compliance Application Server in the **Computer name** field, and then click **Next**.  
**Note:** This computer name must match the fully qualified domain name on the SSL Certificate selected in step 7 of the Configuring a Web Listener procedure.

The screenshot shows the 'New SSL Web Publishing Rule Wizard' dialog box, specifically the 'Define Website to Publish' step. The title bar reads 'New SSL Web Publishing Rule Wizard'. The main heading is 'Define Website to Publish' with a sub-instruction: 'Specify the computer (Web server) on which the website is located. You can publish the entire website or limit access to a specified folder.' Below this, there is a text box for 'Computer name or IP address:' containing 'https://nac.sophos.com' and a 'Browse...' button. A checkbox is present with the label 'Forward the original host header instead of the actual one (specified above)'. Below that, a text box for 'Path:' is empty, with a sub-instruction: 'Enter the name of the file or folder you want to publish. To include all files and subfolders within a folder use /\*. Example: folder/\*.'. A summary line states: 'Based on your selection, the following Web site will be published:'. Below this, a text box for 'Site:' contains 'https://nac.sophos.com'. A sub-instruction reads: 'Set the port to which requests should be redirected on the Bridging tab of the rule properties page.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

7. Select **This domain name** from the **Accept requests for** list box, type the fully qualified domain name in the **Public name** field, and then click **Next**.

The screenshot shows the 'New SSL Web Publishing Rule Wizard' dialog box, specifically the 'Public Name Details' step. The title bar reads 'New SSL Web Publishing Rule Wizard'. The main heading is 'Public Name Details' with a sub-instruction: 'Specify the public domain name (FQDN) or IP address users will type to reach the published site.' Below this, there is a dropdown menu for 'Accept requests for:' with 'This domain name (type below):' selected. A sub-instruction reads: 'Only requests for this public name or IP address will be forwarded to the published site. For example www.microsoft.com.'. Below that, a text box for 'Public name:' contains 'https://nac.sophos.com'. A text box for 'Path (optional):' is empty. A summary line states: 'Based on your selections, requests sent to this site (host header value) will be accepted:'. Below this, a text box for 'Site:' contains 'https://nac.sophos.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

8. Select the Web listener you created, and then click **Next**.

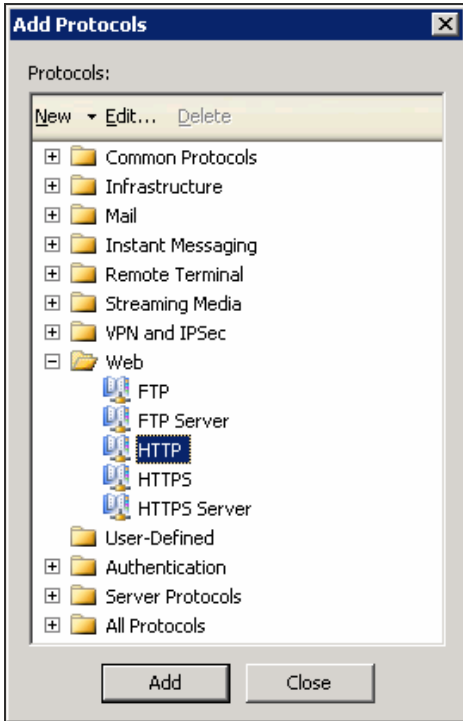


9. Add the users that can access the site on the User Sets window, and then click **Next**.  
**Note:** The default is all users, but this default can be adjusted as appropriate.
10. Click **Finish** to complete the creation of the SSL Web publishing rule.
11. Click **Apply** above the **Firewall Policy** tab to save the changes.

## Configuring ISA Server to Proxy Requests from Sophos

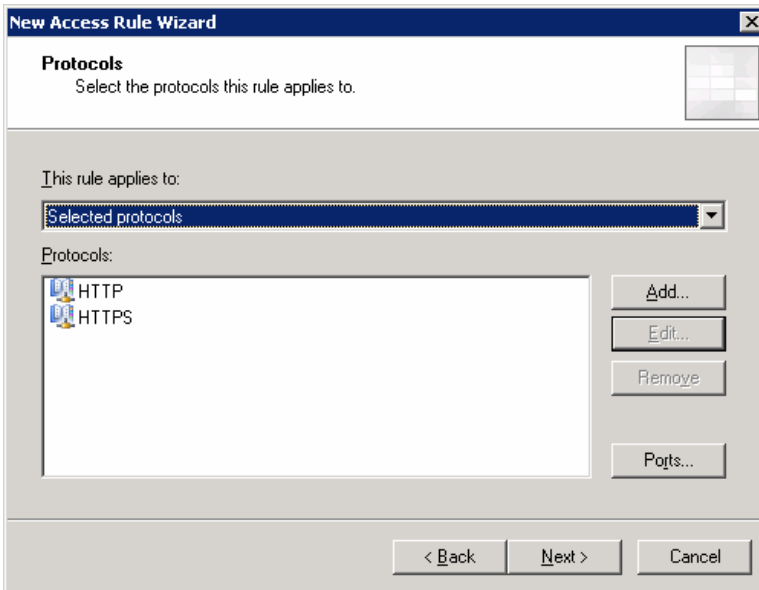
By default, the Compliance Application Server will retrieve Microsoft OS patch definition updates from the Sophos hosted Web site. To permit proper retrieval of these updates, you should configure the ISA Server to proxy all such requests from the Compliance Application Server to the Sophos hosted Web site. The Compliance Application Server automatically downloads new OS patch information every 24 hours as a scheduled task, and it needs to be able to reach the download site through the ISA firewall.

1. In the ISA Server console, right-click on **Firewall Policy** for the computer node and from the **New** menu, select **Access Rule**.
2. Type an access rule name, and then click **Next**.
3. Click the **Allow** option button in the Rule Action window, and then click **Next**.
4. Select **Selected Protocols** from the list box, and click **Add**.
5. Add **HTTP** and **HTTPS** in the Add Protocols window under the **Web** folder, and then click **Close**.

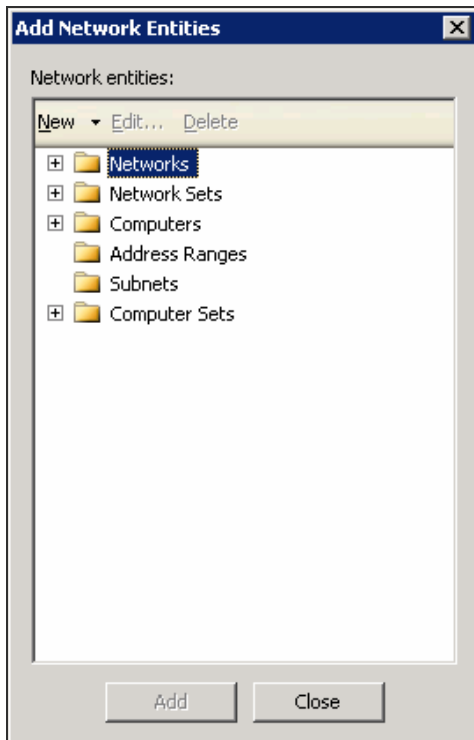


**Note:** HTTP and HTTPS display as allowed protocols.

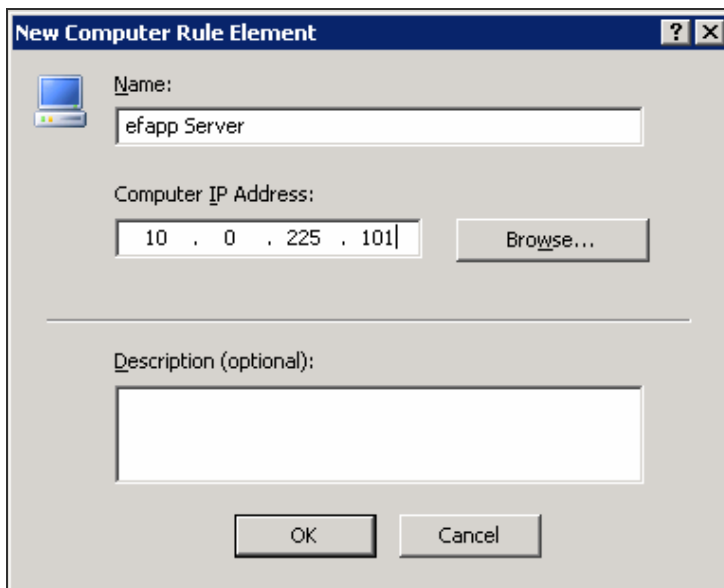
6. Click **Next**.



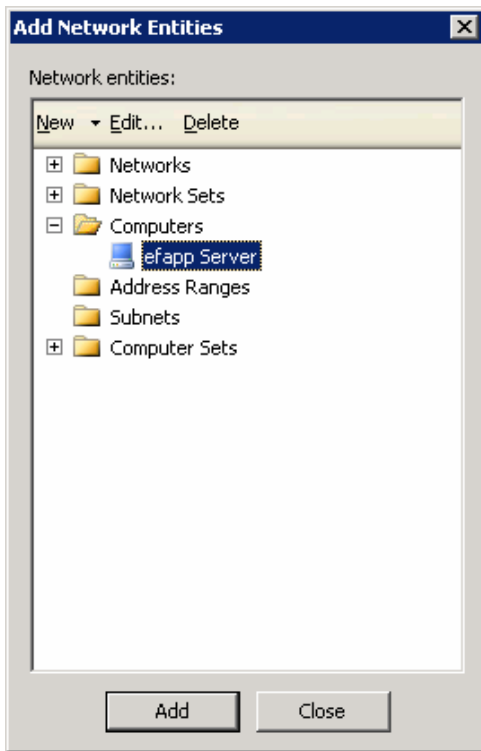
7. Click **Add** on the Access Rule Sources window to display the Add Network Entities window.



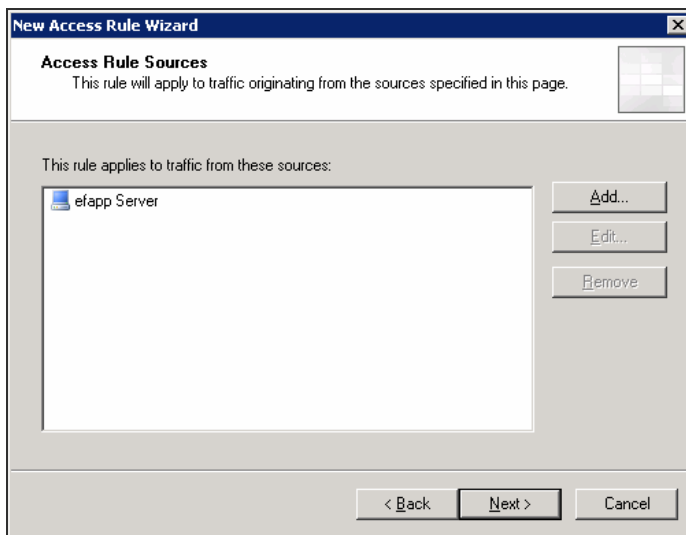
8. From the **New** menu, select **Computer** to add a new computer network entity.
9. Type the name and the IP address of the Compliance Application Server, and then click **OK**.



10. Select the server you added, click **Add**, and then click **Close** to add this computer to the Access Rule Sources.

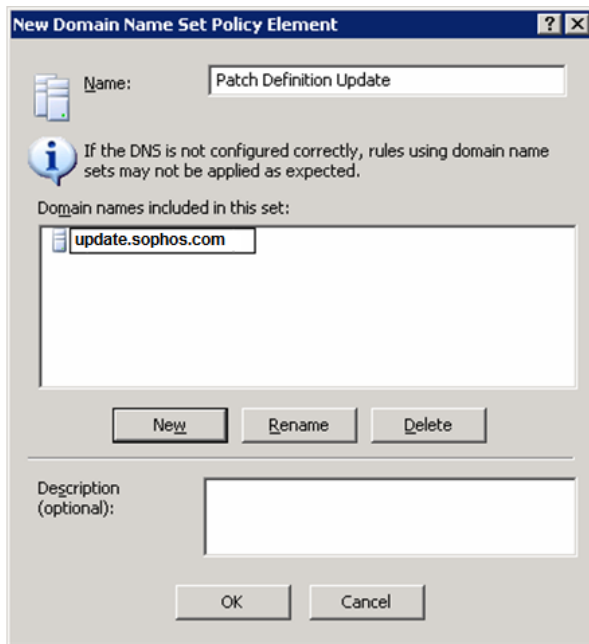


**Note:** The Compliance Application Server displays in the list of sources.

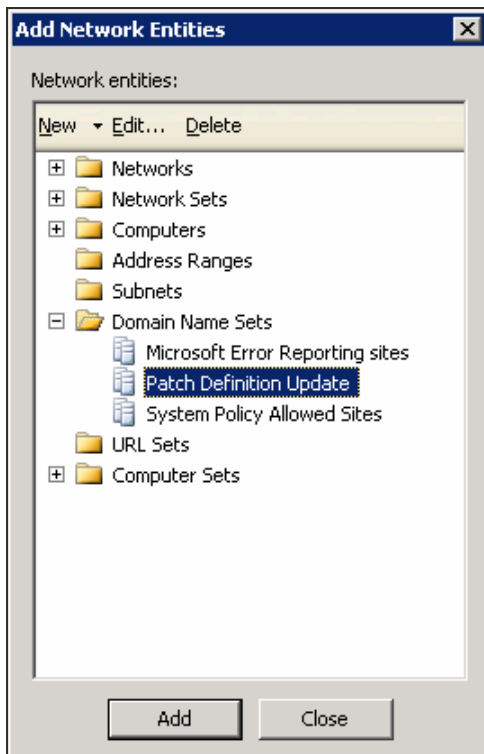


11. Click **Next**.
12. Click **Add** on the Access Rule Destinations window to display the Add Network Entities window.
13. From the new **Menu**, select **Domain Name Set** to add a new domain name network entity.
14. Type a name for the domain name set element, and then click **New**.

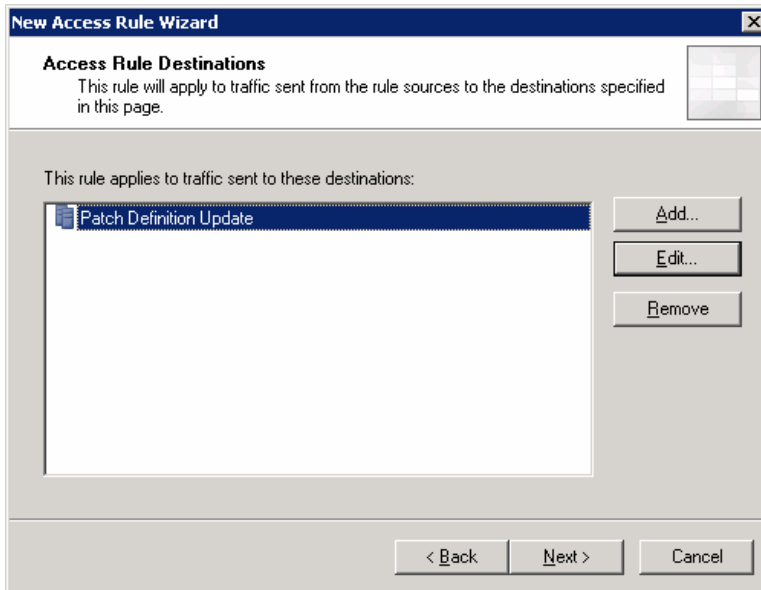
15. Type **update.Sophos.net** as the domain, and then click **OK**.



16. Select the update.Sophos.net domain name, click **Add**, and then click **Close** to add this domain to the Access Rule Destinations.

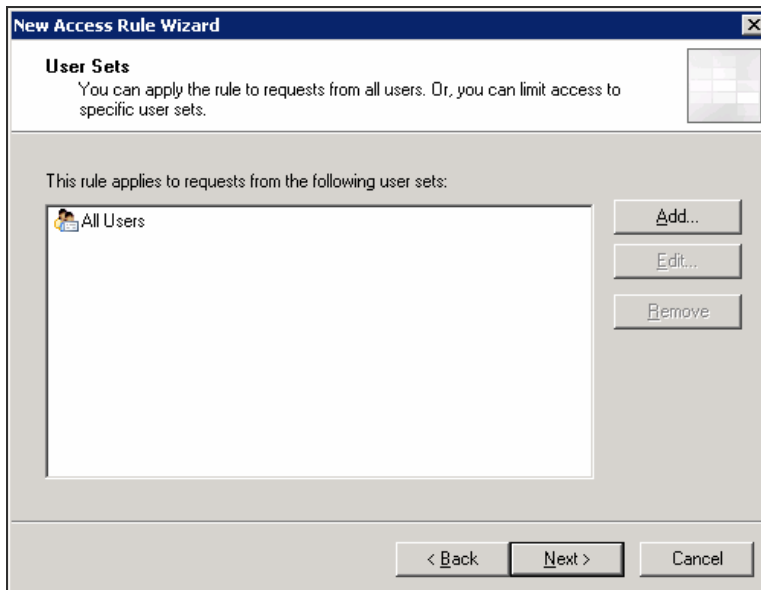


**Note:** The patch definition update server displays in the list of destinations.

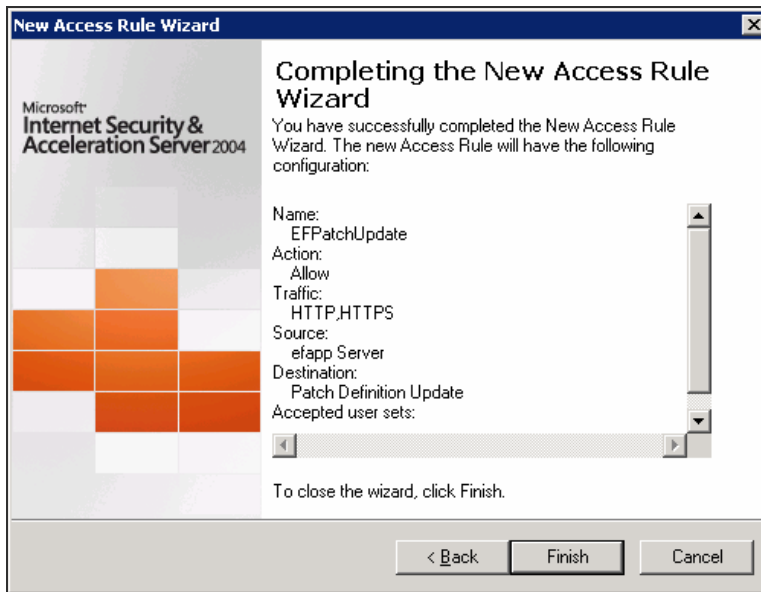


17. Click **Next**.

18. Click **Next** to accept the User Sets default setting.



19. Click **Finish** to complete the New Access Rule wizard.



20. Click **Apply** above the **Firewall Policy** tab, to save the changes.

