Oracle® Adaptive Access Manager
Proxy Web Publishing Configuration
10*g* (10.1.4.3.0)

December 2007

Oracle Adaptive Access Manager Proxy Web Publishing Configuration, 10g (10.1.4.3.0)

Contents

Preface

The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration provides information on creating web publishing rules and listeners so that Web applications and the WebUIO can be accessible from the Internet. The Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers multi-factor authentication to Web applications without requiring any change to the application code. The Oracle® Adaptive Access Manager Proxy and The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration are guides specific to the UIO deployment.

Documentation

The Oracle Adaptive Access Manager 10g documentation includes the following:

- The Oracle® Adaptive Access Manager API Integration Guide, which provides information on natively integrating the client portion of the Adaptive Risk Manager Online solutions. In an API integration, the client application invokes the Adaptive Risk Manager Online APIs directly and manages the authentication and challenge flows.
- The Oracle® Adaptive Access Manager Database Installation Guide (Oracle), which provides information about installing the Adaptive Access Manager schema into an Oracle database. Access to the Adaptive Access Manager schema is a requirement of the Adaptive Access Manager Application Server, which hosts the Adaptive Strong Authenticator and the Adaptive Risk Manager. Note that the Adaptive Manager Access Manager schema needs to be installed into the Oracle database before proceeding to the installation of the proxy.
- The Oracle® Adaptive Access Manager Database Installation Guide for SQL Server 2005, which provides information about installing the Adaptive Access Manager schema into SQL Server 2005. Access to the Adaptive Access Manager schema is a requirement of the Adaptive Access Manager Application Server, which hosts the Adaptive Strong Authenticator and the Adaptive Risk Manager. Note that the Adaptive Manager Access Manager schema needs to be installed into SQL Server 2005 before proceeding to the installation of the proxy.
- The Oracle® Adaptive Access Manager Proxy Integration Guide, which provides programming information and instructions on the installation of the Adaptive Access Manager proxy, one of the components in the Adaptive Access Manager UIO deployment. The Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers multi-factor authentication to Web applications without requiring any change to the application code. The Oracle® Adaptive Access Manager Proxy and The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration are guides specific to the UIO deployment.
- The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration, which provides information on creating web publishing rules and listeners so that Web applications and the WebUIO can be accessible from the Internet. The Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers multi-factor authentication to Web applications without requiring any change to the application code. The Oracle® Adaptive Access Manager Proxy and The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration are guides specific to the UIO deployment.

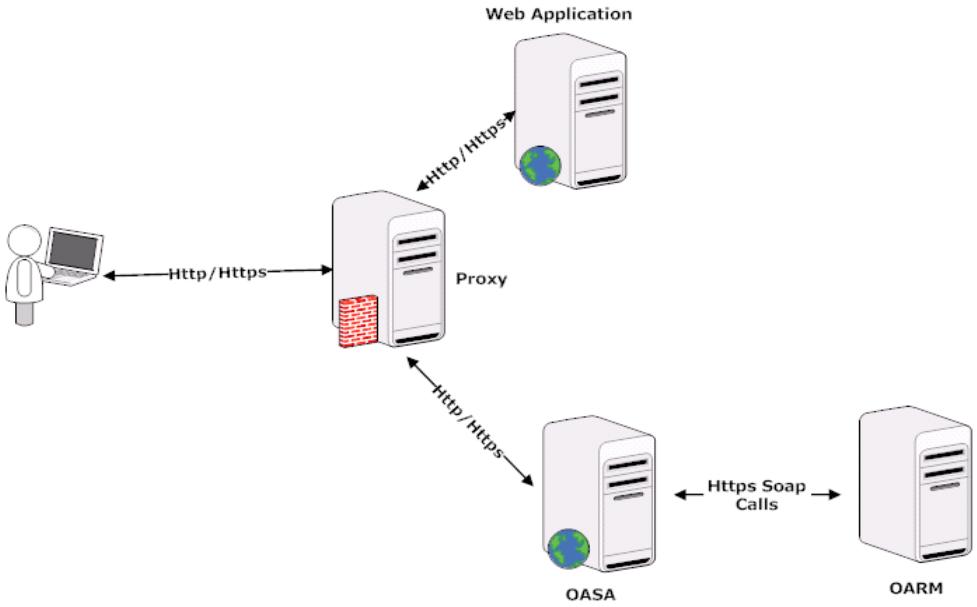
- The Oracle® Adaptive Risk Manager Online Installation Guide, which provides information on the installation of the administration user interface of Oracle Adaptive Access Manager. Adaptive Risk Manager Online is the administration user interface of Oracle Adaptive Access Manager, a set of web-based administration tools that provides sophisticated fraud monitoring, analysis, and tracking by user location, device, time of day, type of transaction, as well as a host of other factors, and evaluates these factors against a set of customizable rules.
- The Oracle® Adaptive Access Manager LDAP Configuration Guide, which provides information on how to configure the Oracle Adaptive Access Manager Application Server to allow a user to be authenticated via a user identifier and password. The intended audience of this manual are users of WebLogic and Tomcat who want to use LDAP to set up users instead of the functionality in WebLogic and Tomcat.
- The Oracle® Adaptive Access Manager Import/Export Manual, which provides information importing groups, rule templates, and models from the Adaptive Access Manager schema.
- The Oracle® Adaptive Risk Manager Online Customer Care API Guide, which provides information about the Adaptive Risk Manager Online Customer Care API and provides the XML definition for each of the APIs.
- The Oracle® Adaptive Access Manager Database Tables Archiving and Purging Procedure, which provides information on the purge and archive scripts in the Oracle Adaptive Access Manager Database Tables of Microsoft SQL Server 2005. The procedure to trigger the scripts and information on verification and validation of script results are also provided.
- The Oracle® Adaptive Access Manager SQL Server Maintenance Guide, which provides instructions to set up The Oracle Adaptive Access Manager Maintenance Plan to purge and archive scripts in the Oracle Adaptive Access Manager database tables of Microsoft SQL Server 2005. The manual also discusses in detail how to trigger the scripts and provides information on the verification and validation of script results.
- The Oracle® Adaptive Risk Manager™ Administrator's Guide, which provides step-by-step instructions for creating and managing groups, creating models that contain rules, and customizing and managing rules.
- The Oracle® Adaptive Risk Manager™ Dashboard and Reporting Guide, which provides detailed instructions on how to use the dashboard and reporting functionality within the Oracle® Adaptive Risk Manager Online. The Oracle® Adaptive Risk Manager Online includes a dashboard that provides a high-level overview of users and devices that have generated alerts and the alerts themselves, and it contains a comprehensive collection of reports on users, locations, devices, and security alerts.
- The Oracle® Adaptive Risk Manager™ Customer Care Administration Guide, which provides information on creating new customer cases and administering them.

Introduction

Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers added multi-factor authentication to Web applications without requiring any change to application code. The purpose of this document is to explain the creation of web publishing rules and listeners in Microsoft ISA for Adaptive Access Manager Applications. This document is intended for integrators who install and configure Microsoft ISA to support multiple Web applications.

Architecture

The following diagram shows an Adaptive Access Manager UIO deployment.



The Adaptive Access Manager proxy intercepts the HTTP traffic between the client (browser) and the server (web application) and performs appropriate actions, such as redirecting to the Adaptive Strong Authenticator, to provide multi-factor authentication and authorization. The Adaptive Strong Authenticator in turn communicates with Adaptive Risk Manager to assess the risk and takes the appropriate actions, such as permitting the login, challenging the user, blocking the user, and other actions.

The Adaptive Access Manager Proxy uses the API provided by Microsoft ISA Server to monitor the HTTP traffic and perform various actions. Microsoft ISA Server 2006 or 2004 Standard Edition should be installed and web publishing rules for web applications should be created before installing the Adaptive Access Manager Proxy. For the details on installing and configuring ISA server, refer to the Microsoft ISA Server setup documentation. Web publishing rule creation and listener creation are explained further in this document.

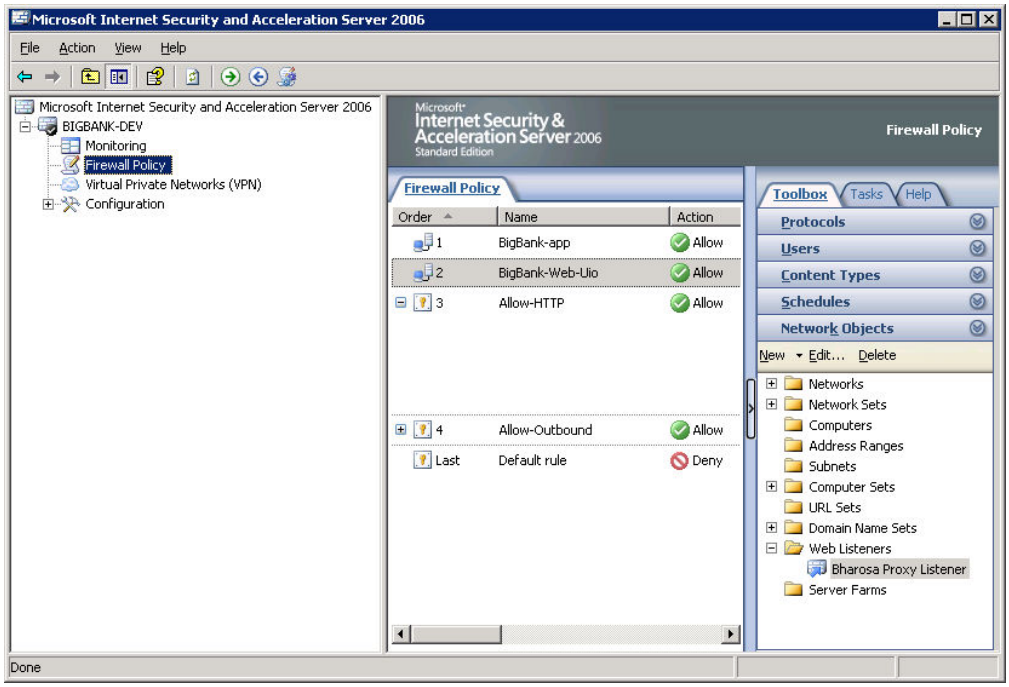
Web Publishing Rule Creation

In a typical deployment, Web applications and the Adaptive Access Manager WebUIO run on machines in an internal network and are not directly accessible from the Internet. Only the Adaptive Access Manager Proxy machine, which runs Microsoft ISA Server, will be accessible from the Internet. Web applications can be made accessible from the Internet via Web publishing rules in the Microsoft ISA Server. This section provides steps-by-step instructions to create Web publishing rules.

To create a new web publishing rule:

1. **Start Microsoft ISA management console: Start Menu > All Programs > Microsoft ISA Server > ISA Server Management.**

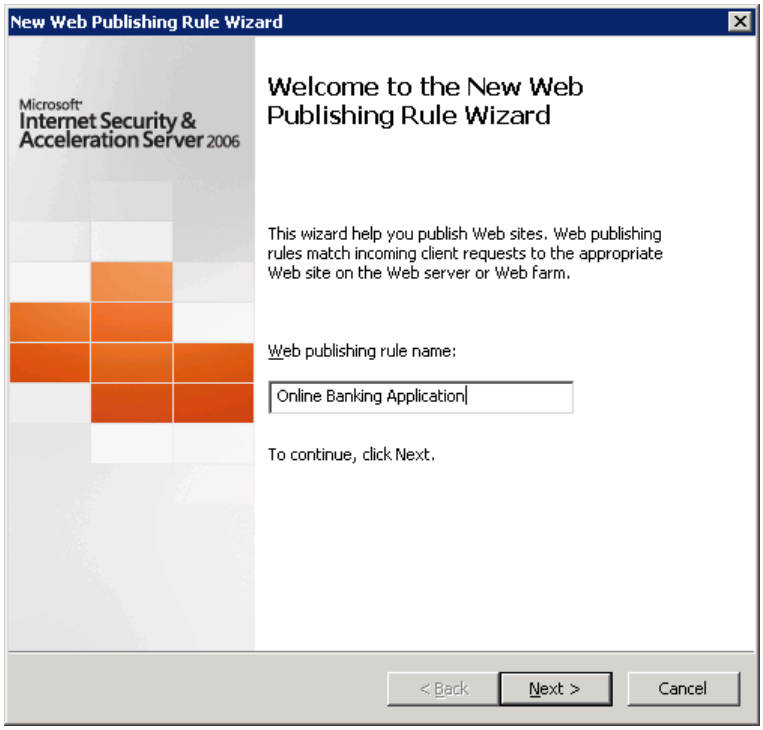
   The Internet Security & Acceleration Server screen appears.



2. **In the left pane, expand the local machine name to display its sub tree.**

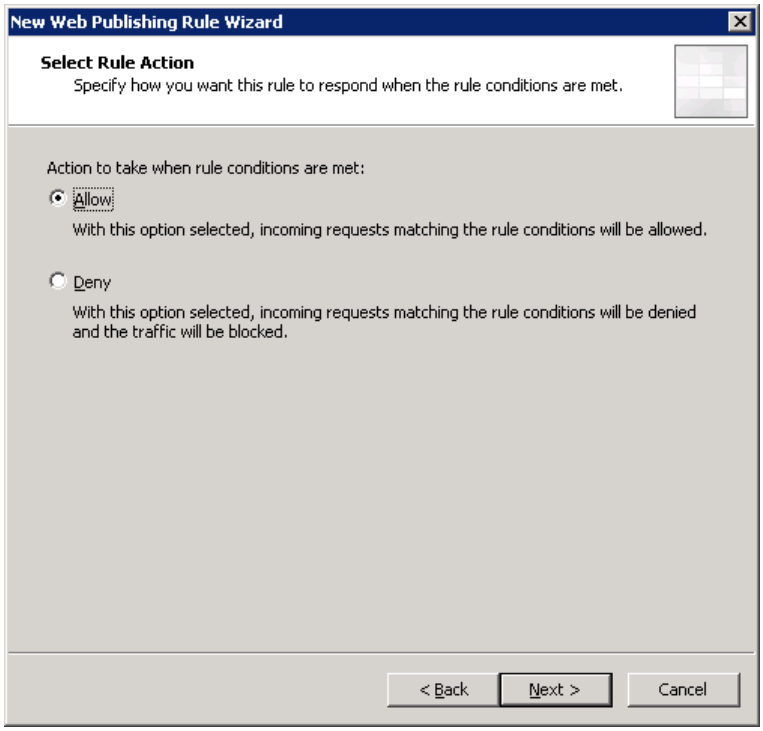
3. **Right click Firewall Policy and select New/Web Site Publishing Rule.**

   The New Web Publishing Rule Wizard appears.



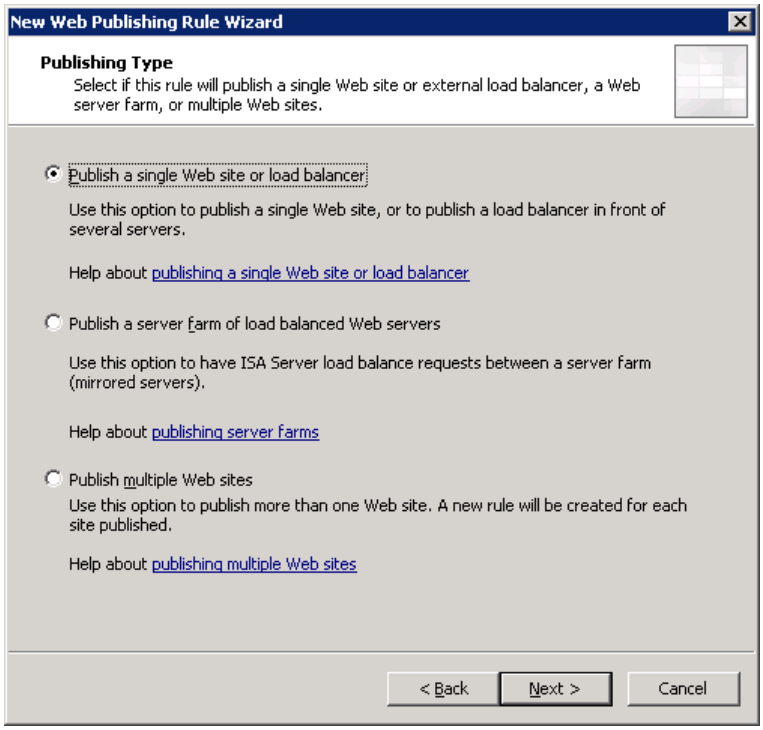
4. **When the New Web Publishing Rule Wizard appears, enter a name for the rule such as "Bharosa WebUIO" or "Online Banking Application" and click Next.**

   The Select Rule Action screen appears.



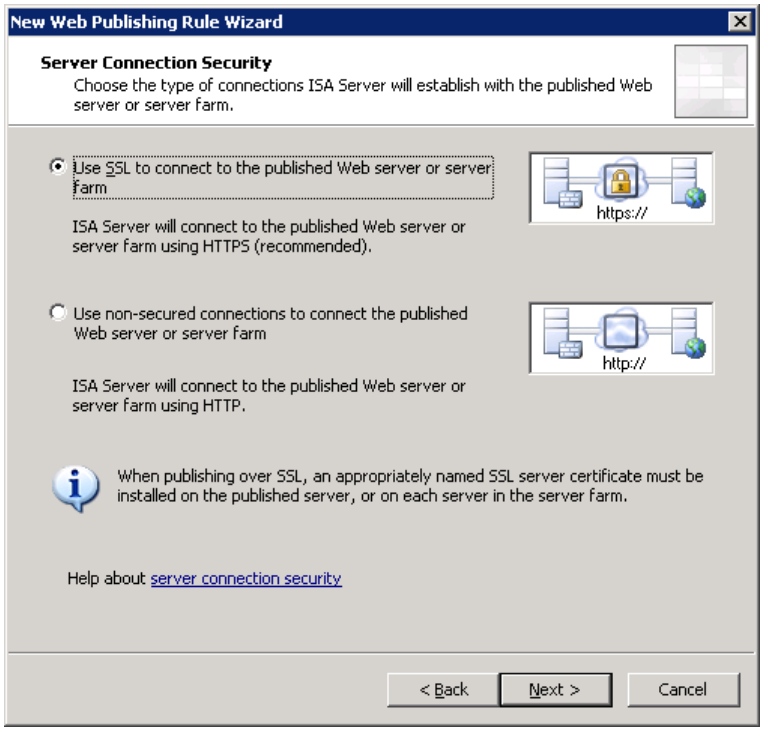
5. **Select Allow and click Next.**

   The Publishing Type screen appears.



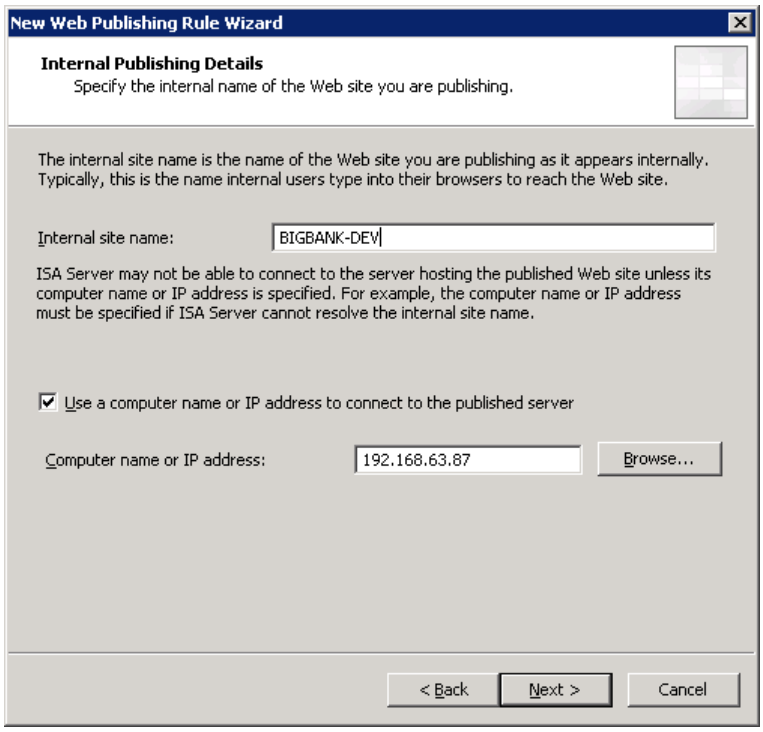
6. **Select "Publish a single web site or load balancer" and click Next.**

   The Server Connection Security screen appears.



7. **Select one of the connection options and click Next.**
   - If the Web application is listening on SSL, select "Use SSL to connect to the published Web server or server farm."
   - If the Web application is not listening on SSL, select "Use non-secured connections to connect to the published Web server or server farm."

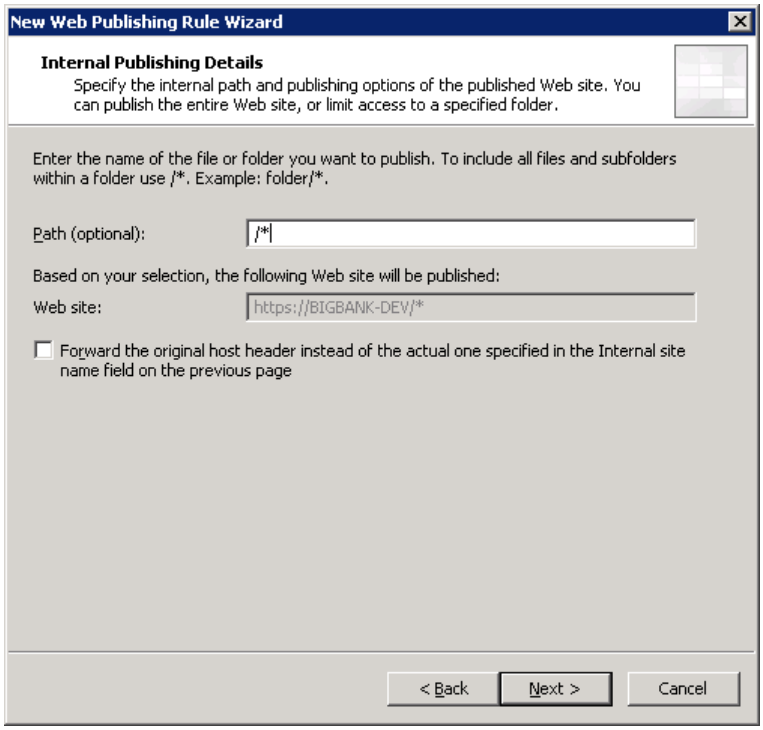
   The Internal Publishing Details screen appears for specifying the internal site name.



8. **Enter the internal site name for the Web application to be published.**

   For a single Web site, this is typically the machine name where the Web server runs.
9. **If the IP address or the machine name of the Web application to be published is known, select the checkbox "Use a computer name or IP address…" and enter the IP address or the machine name.**
10. **Click Next.**

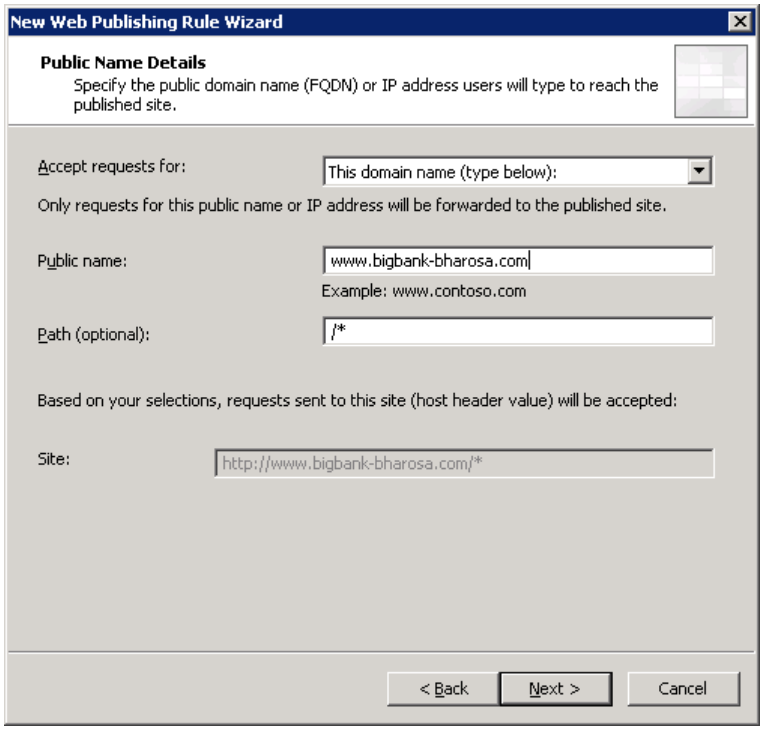
The Internal Publishing Details screen appears for specifying the path.



11. Enter the name of the file or folder you want to publish and click Next.

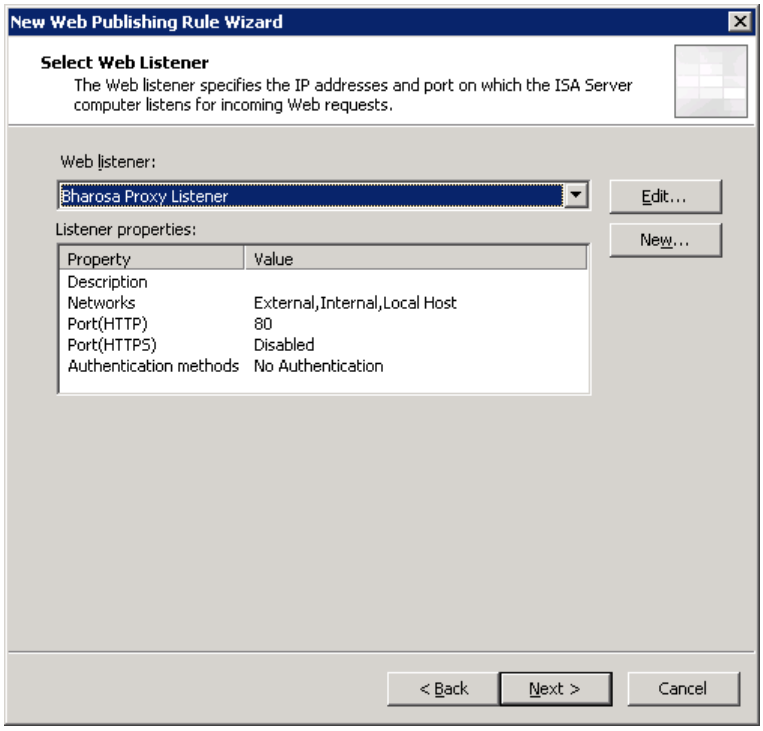
To include all files and subfolders within a folder, enter /*. If you need to publish more than one file or folder, enter only the first file/folder. The remaining files can be entered later by editing the rule.

The Public Name Detail screen appears.



12. **Enter the path entered in the previous step in the Path field.**
13. **From the Accept request for list, select one of the following items:**
    - To restrict access to the application using certain domain name(s) only, select “This domain name” and enter the domain name in the “Public name” field. If more than one domain needs to be permitted, enter only the first domain name. The remaining name can be entered later by editing the rule.
    - To permit access without restriction on the domain name, select "Any domain name.”
14. **Click Next.**

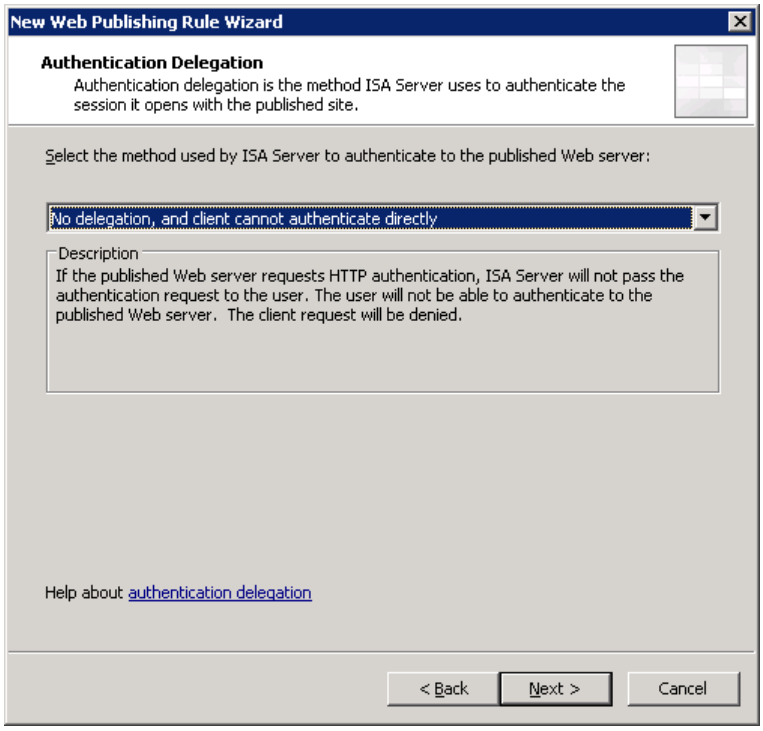
The Select Web Listener screen appears.



15. **From the Web Listener list, select Bharosa Proxy Listener and click Next.**

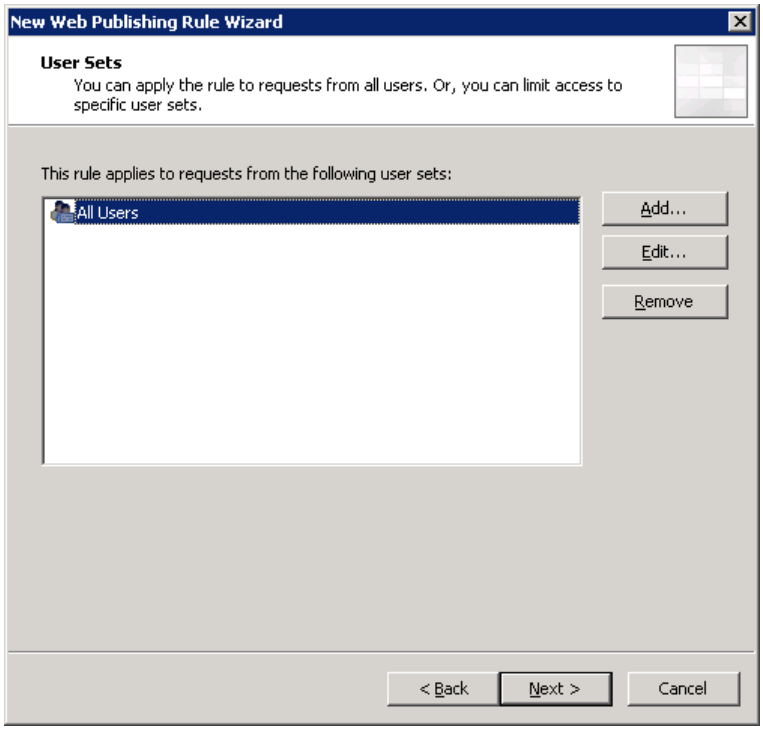
    If the list is empty, create the listener by clicking “New” and following the instructions in the next section.

    The Authentication Delegation screen appears.



16. **Select "No delegation and client cannot authenticate directly" from the list and click Next.**

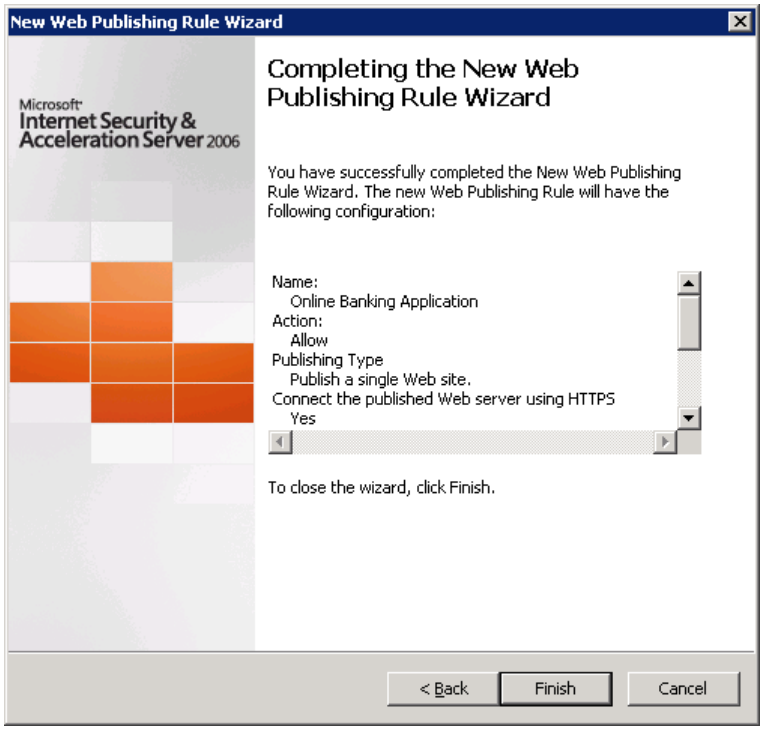
    The User Sets screen appears.



17. **Confirm that only All Users is in the box and click Next.**

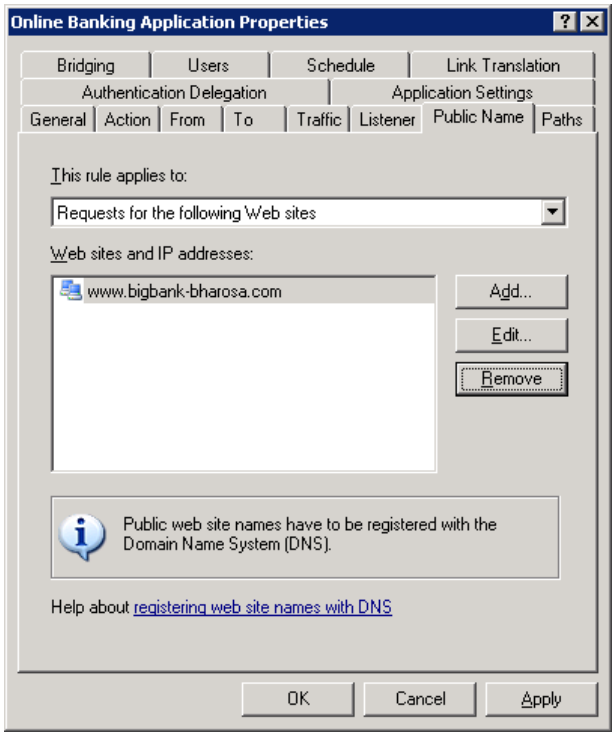
    If All Users is not in the list, update the User Sets using the Add and Remove buttons and click Next.

The Completing the New Web Publishing Rule Wizard screen appears.

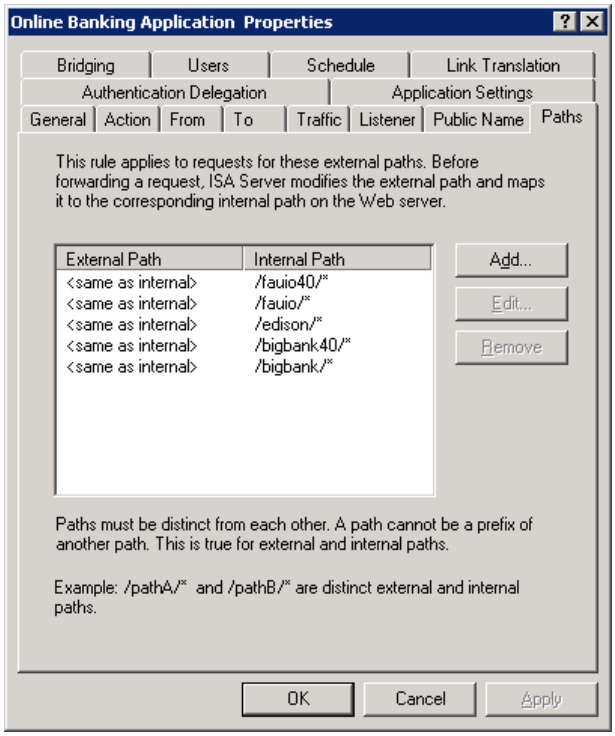


18. **Double click the newly created rule.**

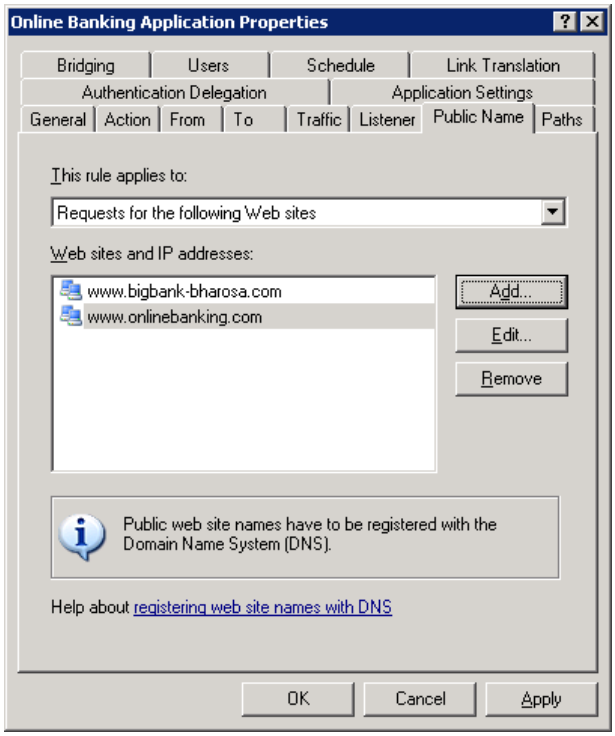
The Online Banking Application Properties screen appears.



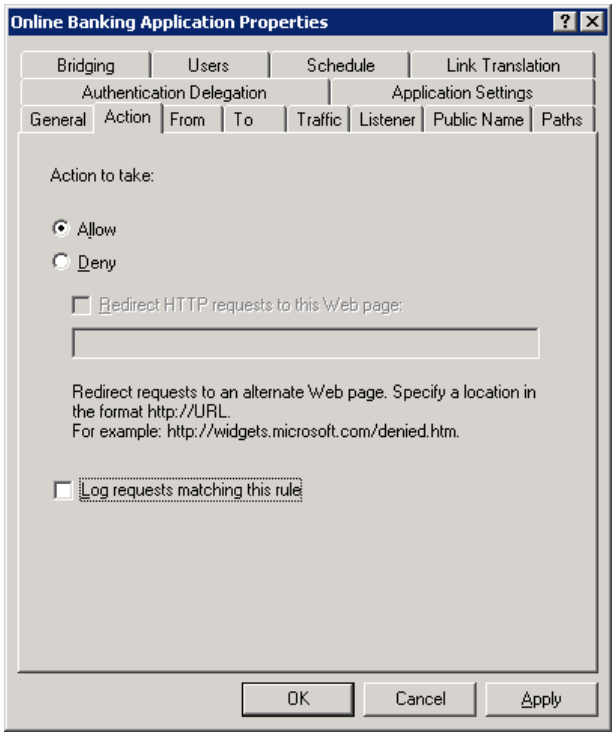
19. **If more than one file or folders need to be published, select the Paths tab and add all the paths.**



20. **To allow more than one domain name to be used to access the application, select the Public Name tab and add all the domain names.**

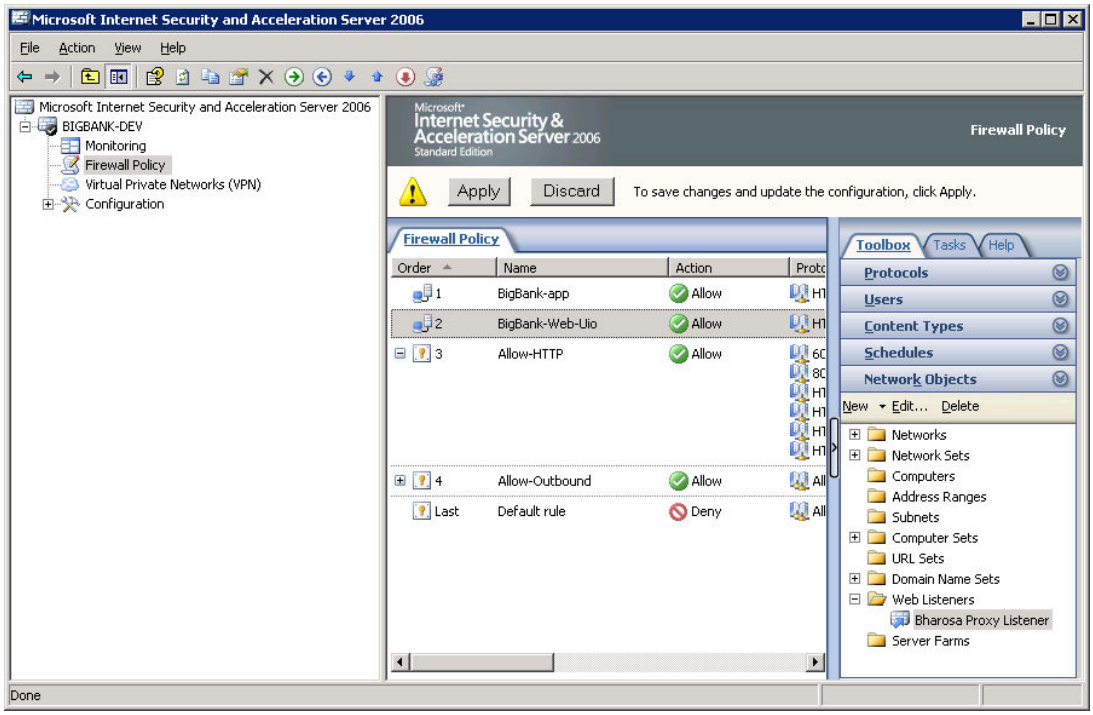


21. **Select the Action tab.**



22. **Click the checkbox next to "Log requests matching this rule" to deselect it and click OK.**

    You return to the Internet Server & Acceleration Server screen.



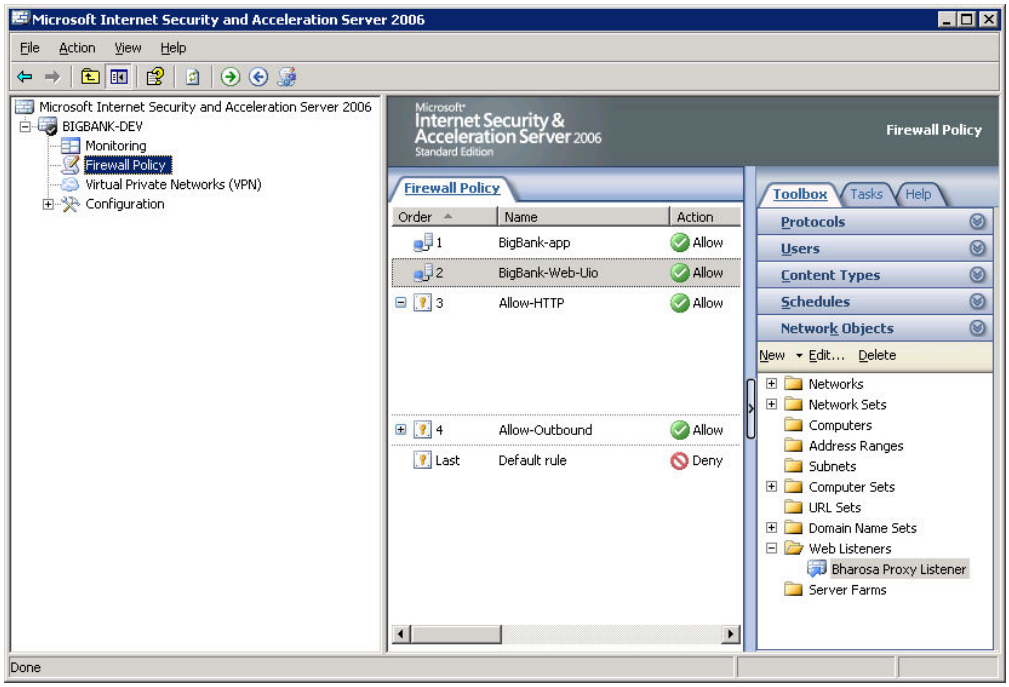
23. **Click Apply.**

Web Listener Creation

To create a web listener:

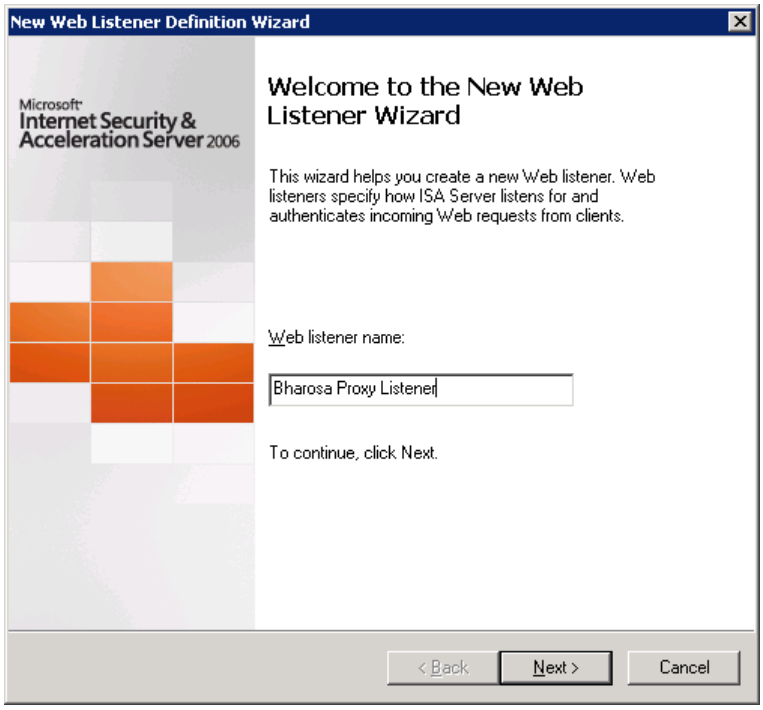
1. **Start Microsoft ISA management console: Start Menu > All Programs > Microsoft ISA Server > ISA Server Management.**

   The Internet Security & Acceleration Server screen appears.



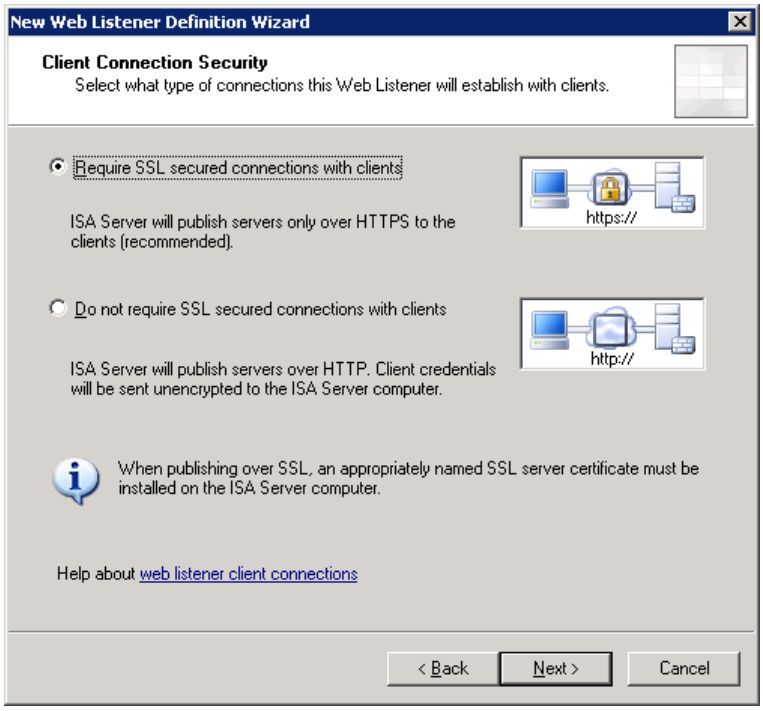
2. **In the left pane, expand the local machine name to display its sub tree.**
3. **Select Firewall Policy.**
4. **Click the Toolbox tab in the right pane.**
5. **Right click on Web Listeners and select New Web Listener.**

The Welcome to the New Web Listener Wizard appears.



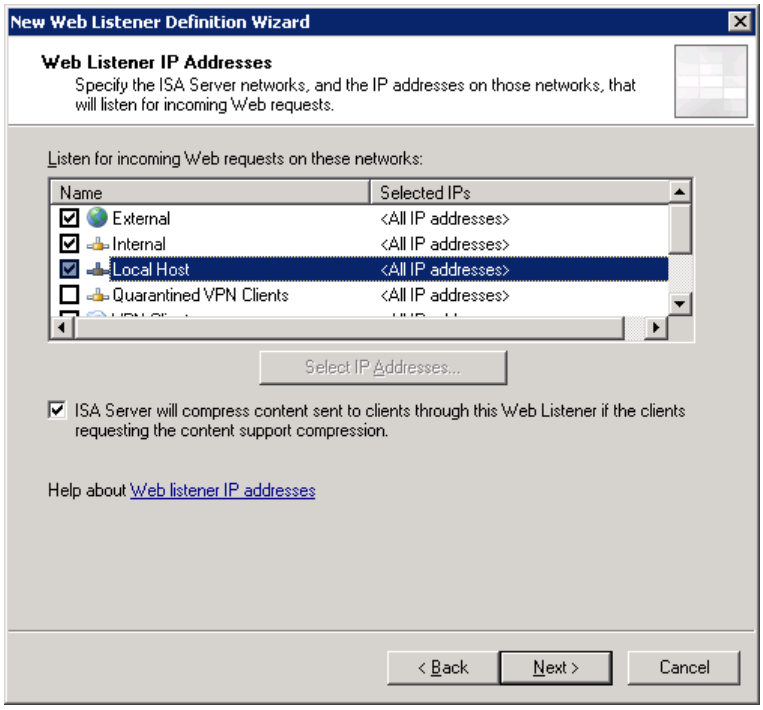
6. **Enter Bharosa Proxy Listener in the Web Listener Name field and click Next.**

The Client Connection Security screen appears.



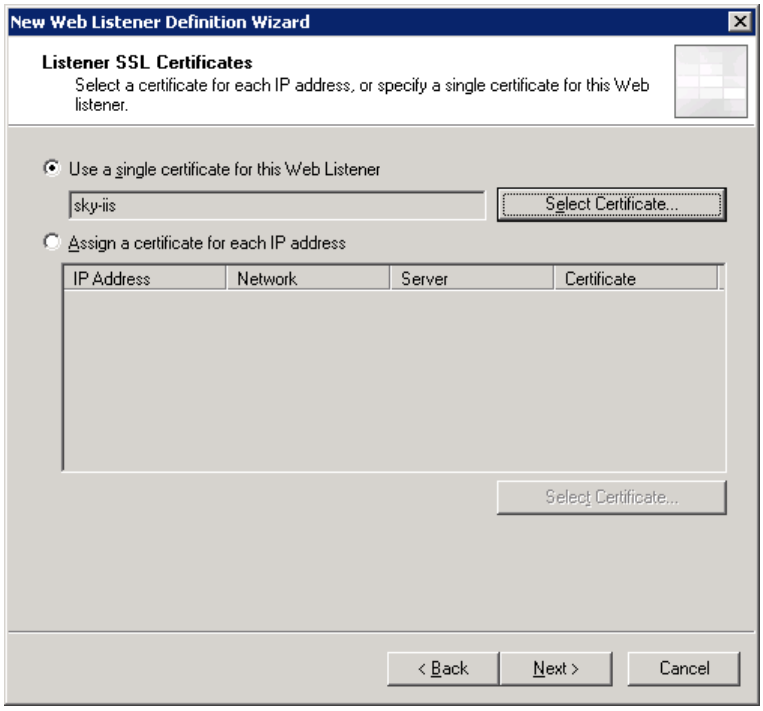
7. **Select "Require SSL secured connections with clients" and click Next.**

The Web Listener IP Addresses screen appears.



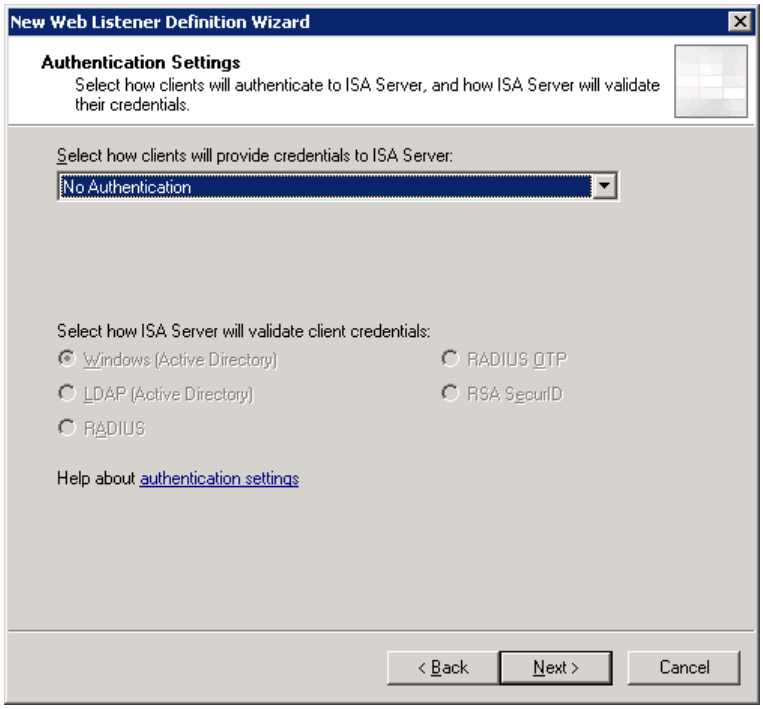
8. **Select External, Internal, and Local host and click Next.**

The Listener SSL Certificates screen appears.



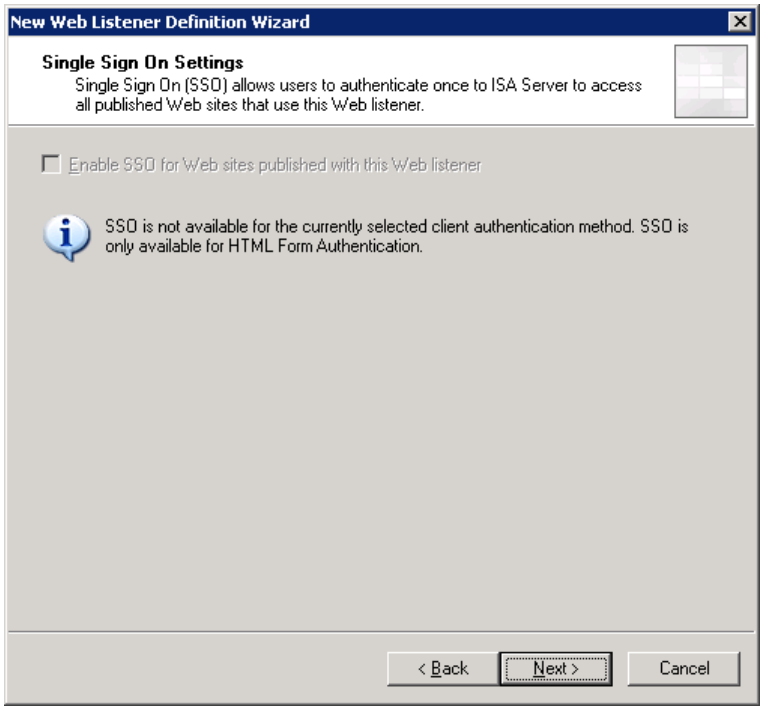
9. **Select "Use single certificate for this Web Listener."**
10. **Click Select Certificate and install the certificate.**
11. **Click Next.**

The Authentication Settings screen appears.



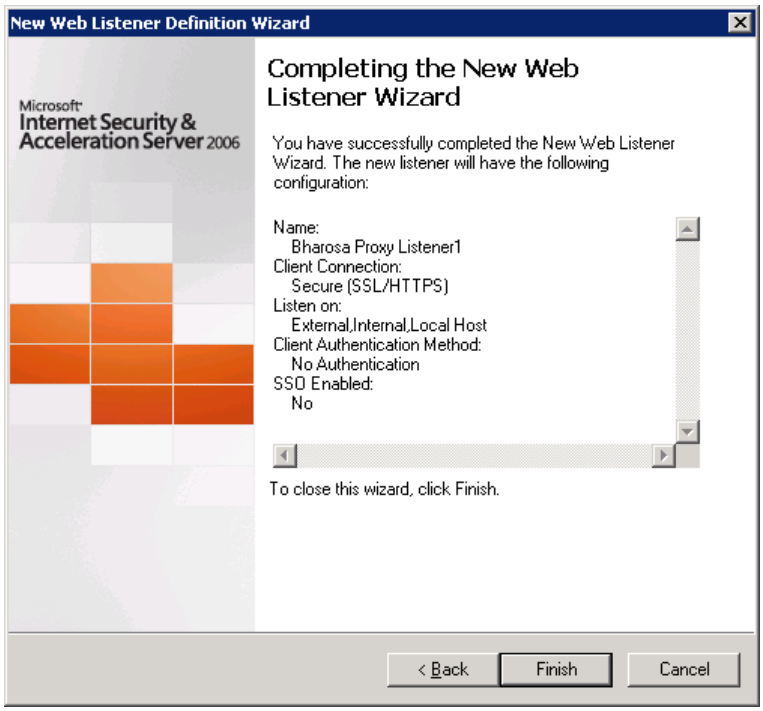
12. **Select No Authentication from the list and click Next.**

The Single Sign On Settings screen appears.



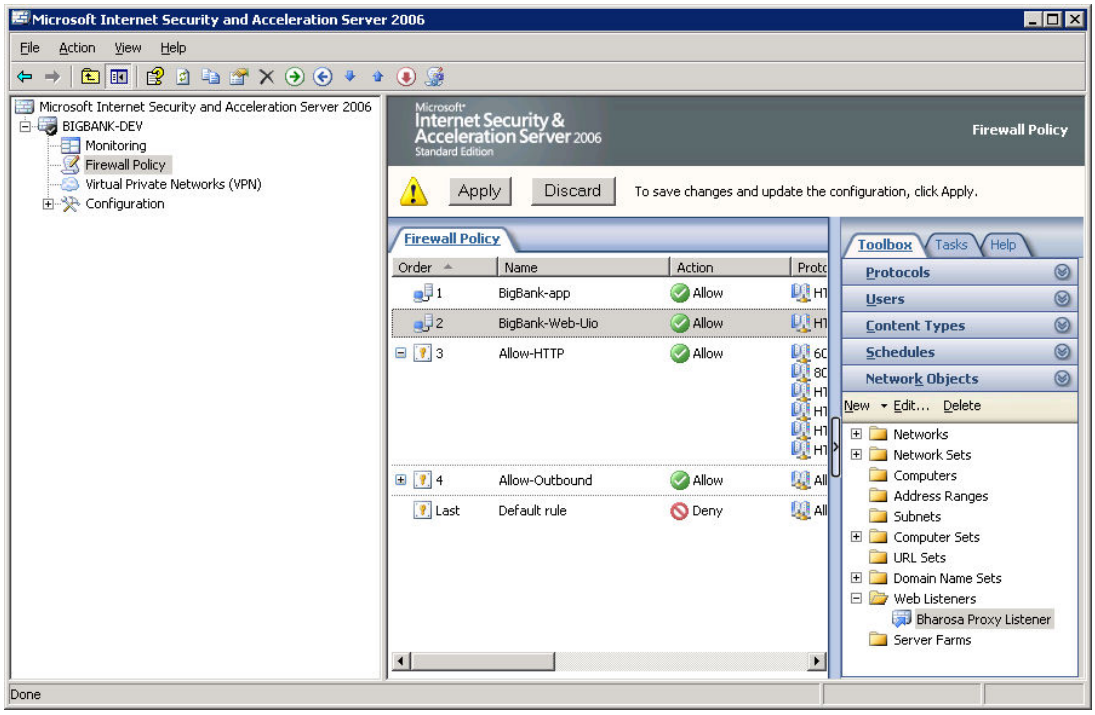
13. **Click Next.**

The Completing the New Web Listener Wizard screen appears.



14. **Click Finish.**

The Internet Security & Acceleration Server screen appears.



15. **Click Apply.**

The Listener you just created is located under Network Objects/Web Listener.

Troubleshooting

If you experience any problems:

- .Net2.0 Framework should be installed and enabled to successfully register the Bharosa Proxy DLL.
- Ensure the database access credentials are correct when the Firewall logging properties in Microsoft ISA use SQL Database as the Log Storage Format.
- It is recommended that you define IP Exceptions for Trusted IPs (like Router IP) when Flood Mitigation settings are enabled to mitigate flood attacks and worm propagation.