BIRKENHEAD
SIXTH·FORM·COLLEGE

High Quality Education For All

Computer Services Documentation

Shibboleth Implementation {Shibboleth 2.1.5 IdP Quick Installer & Configuration for Microsoft ISA 2006 }

John Paul Szkudlapski

March 2010

Note: These case studies, prepared by member organisations of the UK federation, are provided for information purposes only and reflect the particular arrangements and experience of those concerned.

Introduction

This document provides information intended to help those installing and configuring Shibboleth (Windows installation) to sit behind a Microsoft ISA 2006 Server.

There are two parts to getting Shibboleth to work correctly with Microsoft ISA:

Part 1: ISA Configuration
Part 2: Shibboleth Configuration

This document assumes that you have IIS running on your Shibboleth server and that you have already requested a certificate (in our case from the Janet Certificate Service). We have IIS running on the box as it is very simple to request a new certificate from IIS.

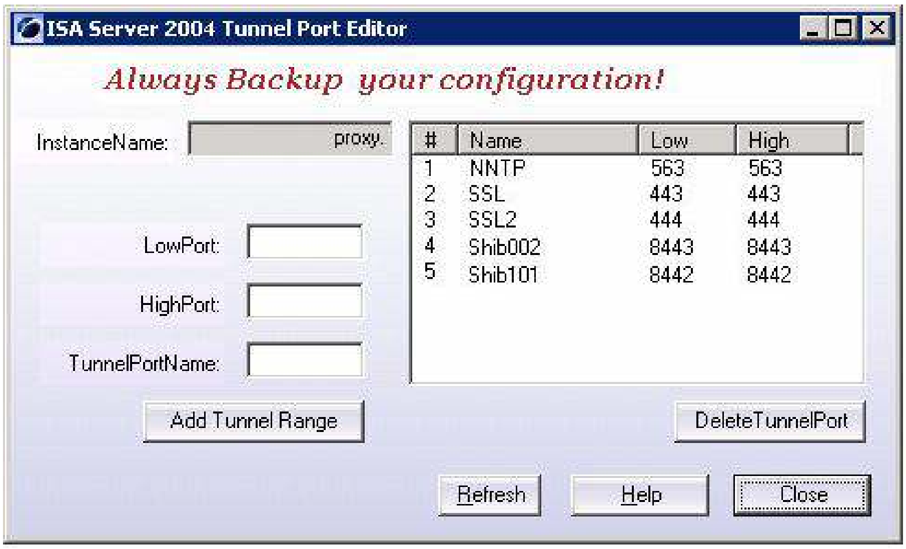
Part 1 – ISA Configuration

Microsoft ISA is often used as a web proxy server. This can cause problems when HTTPS traffic is on any port – such as 8443 – other than 443 or 563.

On the face of it, the problem is easily solved by creating new definitions for ports 8442 and 8443. For example, we might create new ports called SHIB-HTTPS1 and SHIB-HTTPS2, for ports 8442 and 8443 respectively. Then it seems it is just a matter of creating rules to allow traffic on these new ports to get through the firewall.

However, this does not work. The solution is to change the “tunnel port range” to include the port values you wish to use.

There are various scripts that can accomplish this but it may be easier (and less daunting for some people) to use a GUI. In our case we used a free utility called ISATpre (http://www.isatools.org/ISAtrpe.zip) to change the “tunnel port range”.



ISA Server 2004 Tunnel Port Editor

Always Backup your configuration!

InstanceName: proxy.

#	Name	Low	High
1	NNTP	563	563
2	SSL	443	443
3	SSL2	444	444
4	Shib002	8443	8443
5	Shib101	8442	8442

As you can see from our example, we have allowed 8443 and called it Shib002.

When you click on “Add Tunnel Range” it will restart your ISA Firewall Service – **so your users will lose connection for a minute.**

There are also some rules that need to be set up on the ISA server to allow connections from external connections to the server.

Rule 01

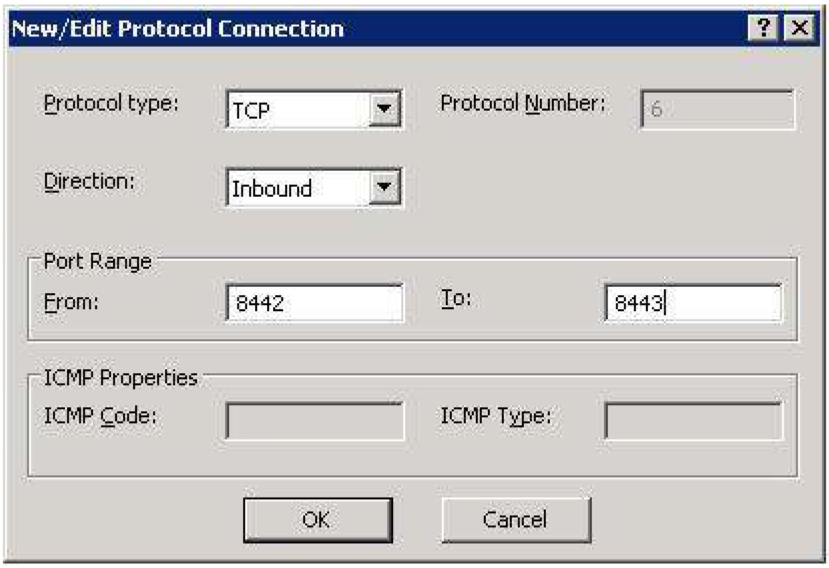
Create a new “Non-Web Server Protocol Publishing Rule”. In our example I set up:

Server Publishing Rule Name:	*Shibboleth Service 8443 Incoming*
IP Address:	*10.0.1.47* (IP of our Shibboleth Server)

Then at the “Selected Protocol” windows, I clicked “New”:

Protocol Definition Name:	*Shibboleth8443*

I then added a new Port Range:



New/Edit Protocol Connection

Protocol type: TCP

Protocol Number: 6

Direction: Inbound

Port Range

From: 8442

To: 8443

ICMP Properties

ICMP Code:

ICMP Type:

Click ‘OK’ to close this window.

I then set up the connection to use our external listener and restarted the ISA service.

Rule 02

Create a new access rule that allows all protocols from the internal server to talk outside via the ISA Server.

Access Rule Name	*Shibboleth Service Outgoing*
Action Taken when rule conditions are met	*Allow*
This rule applies to	*All outbound traffic*
Traffic from these sources	*SSO* {Shibboleth Internal Server}
Traffic to these destinations	*Anywhere*
Requests from the following user	*All Users*

Rule 03

Create a WebListener & Website Publishing Rule.

I will give a basic overview of this, but if you would like further details please drop me an e-mail.

In what follows the left-hand side is the page tab and the right-hand side gives the settings applied to that tab:

Web Listener

Name	SSO
Networks	External
Connections	Enable HTTP Connections on port 80 Enable HTTPS Connections on port 443 Do not redirect traffic from HTTP to HTTPS
Certificates	Use a single certificate for this web listener {and select certificate that was exported from IIS on the shibboleth server (if IIS is used)}

Web Site Publishing Rule

General	Shibboleth Service
Action	Allow Log requests matching this rule
From	Anywhere
To	Published Site : FQDN Computer Name : 10.0.1.47 Requests appear to come from the ISA Server
Traffic	HTTP HTTPS
Listener	SSO
Public Name	Requests for the following websites : FQDN
Bridging	Redirect requests to HTTP port 80 Redirect requests to HTTPS port 443

If you test this at this stage you will get an error – because Shibboleth is still using a self signed certificate to protect the 443 port.

Part 2 – Shibboleth Configuration

Next you need to change the default self-signed certificate that is used for Shibboleth with your real one. The best way to accomplish this is to export your real certificate from IIS and convert it to a JKS. In my testing and use, I have tried to import the PFX directly into the Shibboleth configuration files (rather than using a JKS file), but it didn't seem to work – I don't know if it was the way I was doing it, or if it was something else, so I just decided to mimic the Shibboleth configuration and use a JKS.

I will not document how to convert the certificate to JKS format – this can be accomplished by a web search. However I used this site:

http://www.agrypnia.com/2009/07/28/convert-a-pfx-to-jks-using-windows/

After you have converted your PFX certificate to JKS format it is time to put it into the Shibboleth configuration.

First of all you need to stop Tomcat. The easiest way to do this is from a command prompt:

```
net stop tomcat6
```

You now need to copy your new JKS file into the “credentials” folder inside your Shibboleth IdP. In our case we copy the sso.jks file into:

C:\Shibboleth\Shib2IdP\credentials

You then need to alter the server.xml file (**take a backup first)** located in %path to shibboleth%\CaptiveTomcat 6.0\conf\server.xml. You are looking for this section:

```
<Connector port="443"
  protocol="org.apache.coyote.http11.Http11Protocol"
          maxHttpHeaderSize="8192"
          maxSpareThreads="75"
          scheme="https"
          secure="true"
          SSLEnabled="true"
          sslProtocol="TLS"
          keystoreFile="C:/Shibboleth/Shib2IdP/credentials/idp.jks"
          keystorePass="SeCrEt"      />
```

Change the last two lines to reflect your new certificate, i.e:

```
          keystoreFile="C:/Shibboleth/Shib2IdP/credentials/sso.jks"
          keystorePass="xxxxxxxxxx"/>
```

Save the file and restart Tomcat:

```
net start tomcat6
```

You should now have a working setup of ISA and Shibboleth.

This case study is provided by JANET(UK) for general information purposes only and the JNT Association cannot accept any responsibility and shall not be liable for any loss or damage which may result from reliance on the information provided in it.