SMALLBIZSERVER
frequently asked questions

How to publish Small Business Server 2008 using a Windows Server 2003 computer with ISA 2006 Standard

TERMS

This document and what comes with it are provided as-is with blunt warning: Use at your own risk, buyer beware. You break your system; you own the resolution as well. We have no liability for what you do, or can't do, or fail to do with this information. Your entire protection is to start over again with a protected backup, or from protected system. If you don't want to accept this idea, please don't use this document.

DISTRIBUTION AND DUPLICATION GUIDELINES

This document is not free.

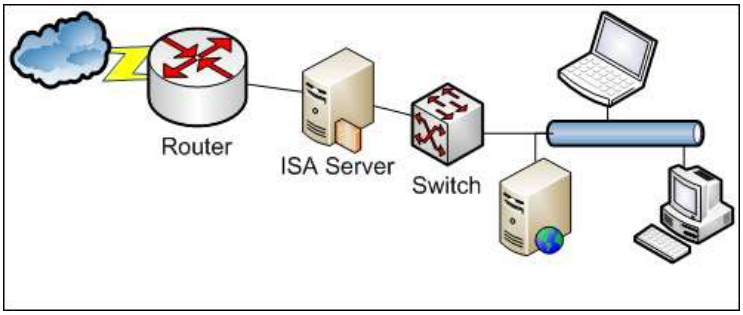
If you received this document from any other source than Smallbizserver.Net, please contact us to become a subscription member. Smallbizserver.Net Tech Docs are licensed per technician.

- Smallbizserver.Net understands your need to protect your investment in the tools and documentation provided in your Smallbizserver.Net Tech Docs. We consider it fair and reasonable use for you to make as many backup copies of any of these items as is necessary to protect yourself from loss or damage. We also understand that you may wish to maintain multiple copies for the purpose of keeping references and tools in more than one location you can work from in the course of a project, or on more than one device, or for continuing use. We expect at all times that you would have the thought in mind that each copy you make is either for a backup to protect against loss, or a copy you have made to facilitate your active work process, but for no other reasons. Leaving copies for others to use is not a permitted use.
- You may not place any hard copy or electronic copy of any portion of a Smallbizserver.Net Tech Docs documentation or tool (or tool code) in a location that provides anonymous access.
- You may not store or locate the Smallbizserver.Net Tech Docs tools or documents in a manner which encourages, or permits violation of the license agreement or copyright such as with file swapping technologies.
- Under no circumstances are you permitted to abstract portions of this document and share them with anyone else, without obtaining specific and written authorization from Smallbizserver.Net for that purpose, and on that occasion, such as for a periodical review. This means that posting sections of documentation to the Internet or public network, or a chat room, or a private network are all examples in violation of our license and copyrights because they do not represent a backup or reasonable use.

For this article I will assume you have followed the steps in "How to publish Small Business Server 2008 using a Windows Server 2003 computer with ISA 2006 Standard Edition - part 1".

Your ISA Server will have two NIC's

- Internal 192.168.80.10 / 255.255.255.0
- External 192.168.178.10 / 255.255.255.0

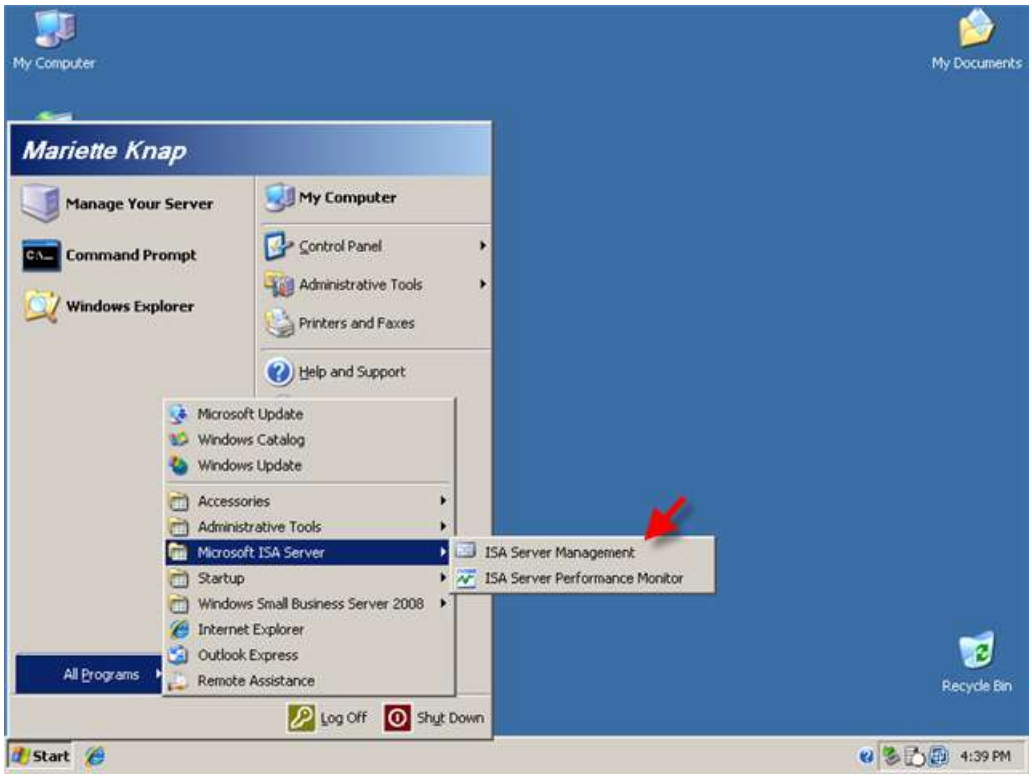


Your SBS Server will have the IP address 192.168.80.5 / 255.255.255.0. Your internet Router will have the internal IP address 192.168.178.1 / 255.255.255.0. You will have run the 'Setup your Internet Address' wizard using the default 'remote.domain.com' (where domain.com is your public domain name). You will have a public DNS record setup for 'remote.domain.com' pointing to the external IP (WAN IP address) of your Internet Router.
This article has the following chapters:

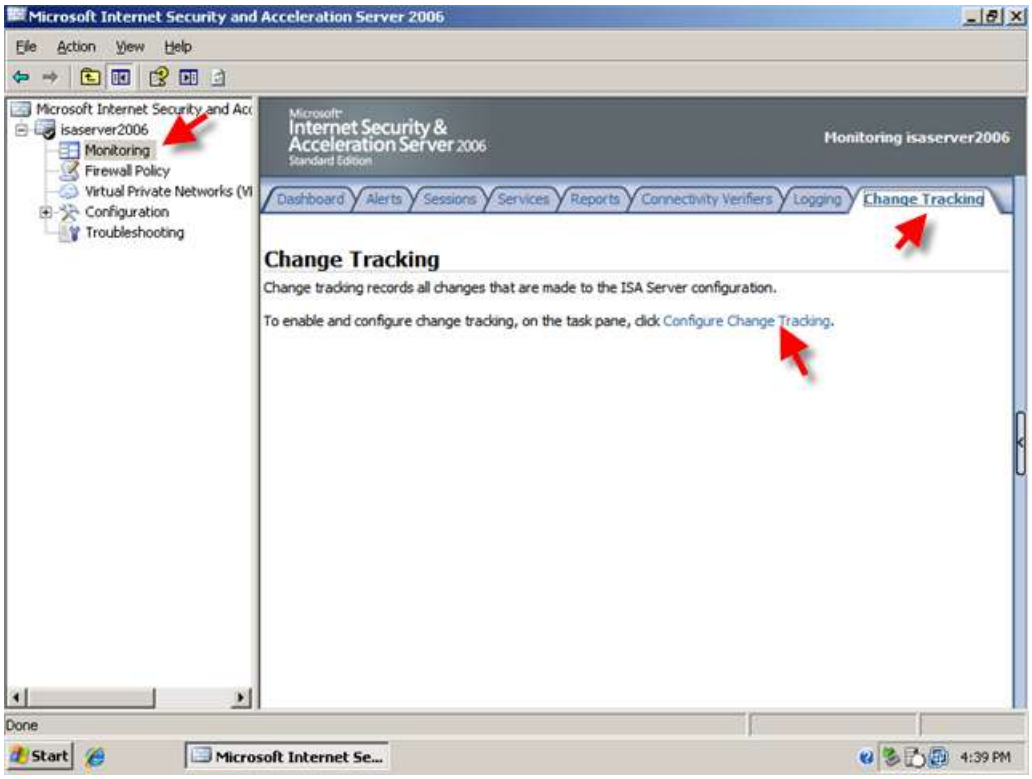
Enabling Change Tracking for ISA Server

Change tracking is a great new feature for ISA 2006, it allows you to enter a comment every time you apply new changes to the ISA Server Firewall policy. If used correctly this can be a great help when troubleshooting, or simply to provide a log of the changes you have made along the way.

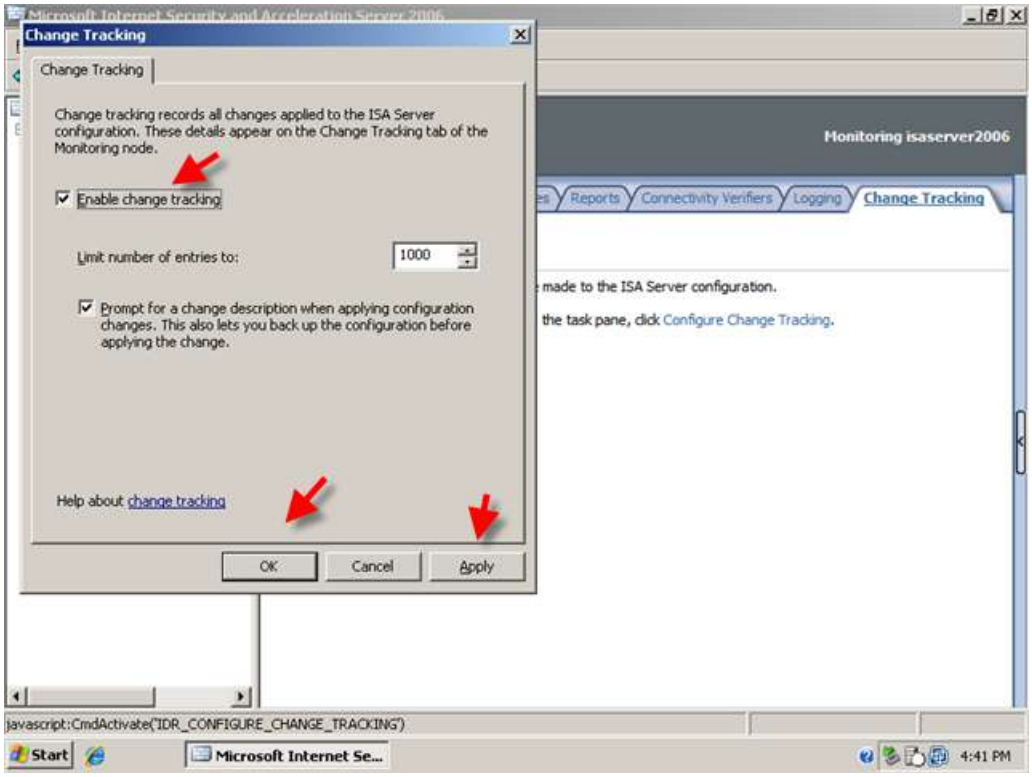
1. To enable change tracking, open ISA Server Management.



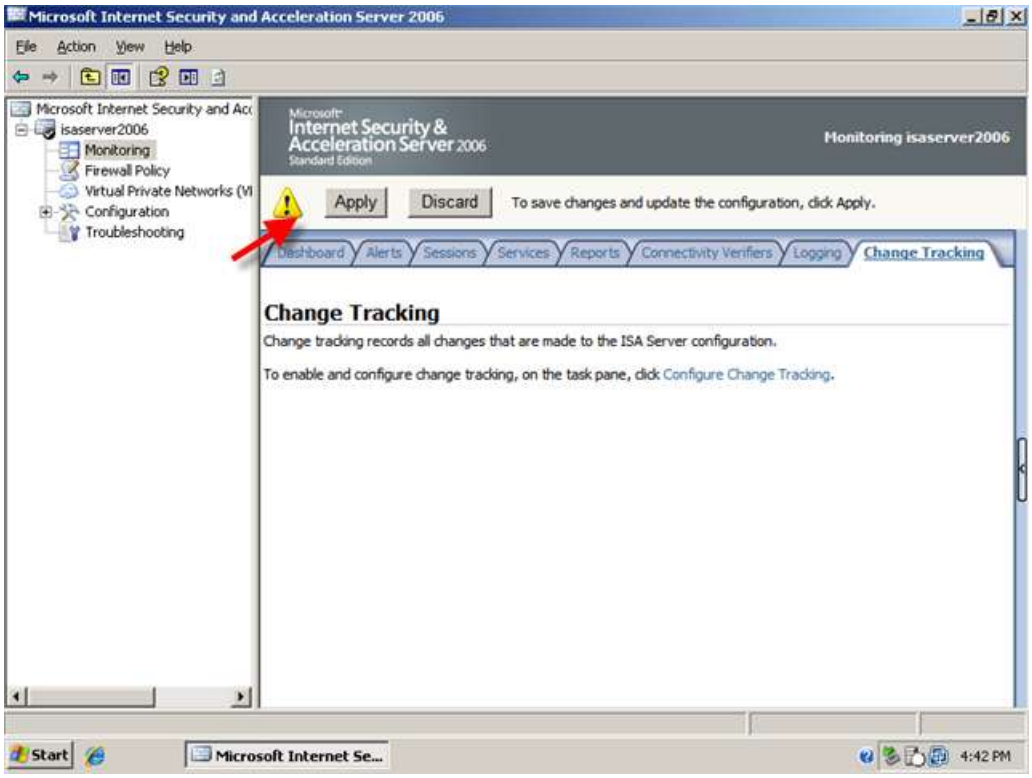
2. Go to the Monitoring component. This should open the Dashboard tab. Click on the tab named Change Tracking. Click Configure Change Tracking



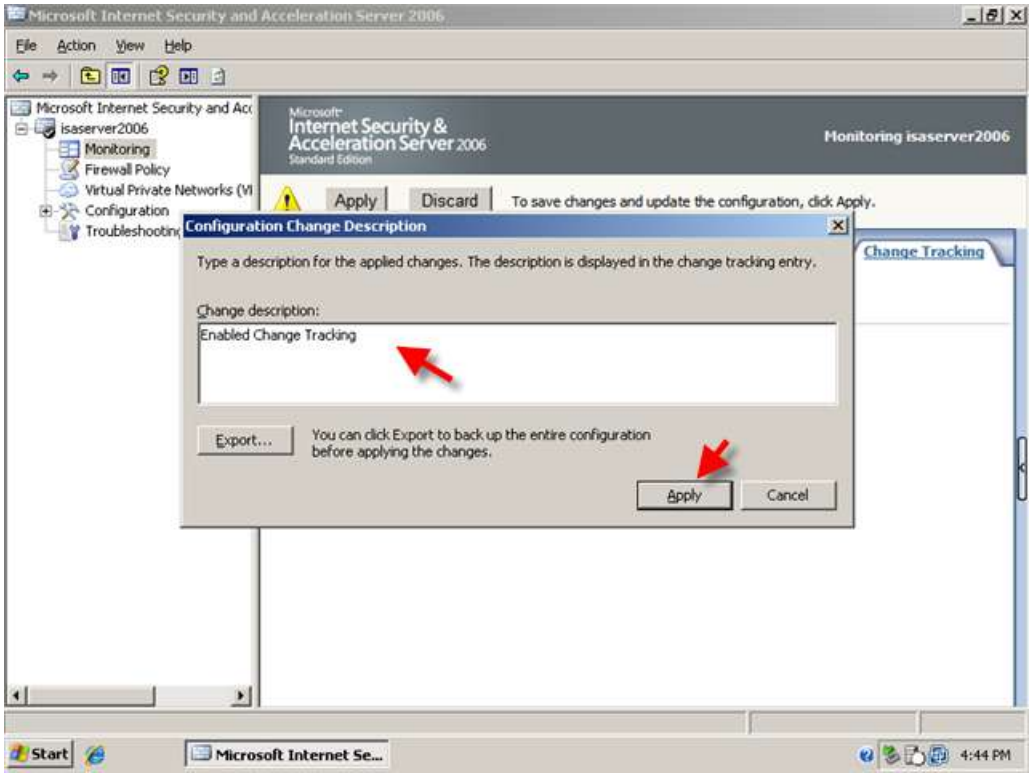
3. Tick the Box to enable change tracking, and set a value for the number of entries you want to see, the default is 1000. Leave the box to prompt for a change description checked. Click Ok. Click Apply to save your changes.



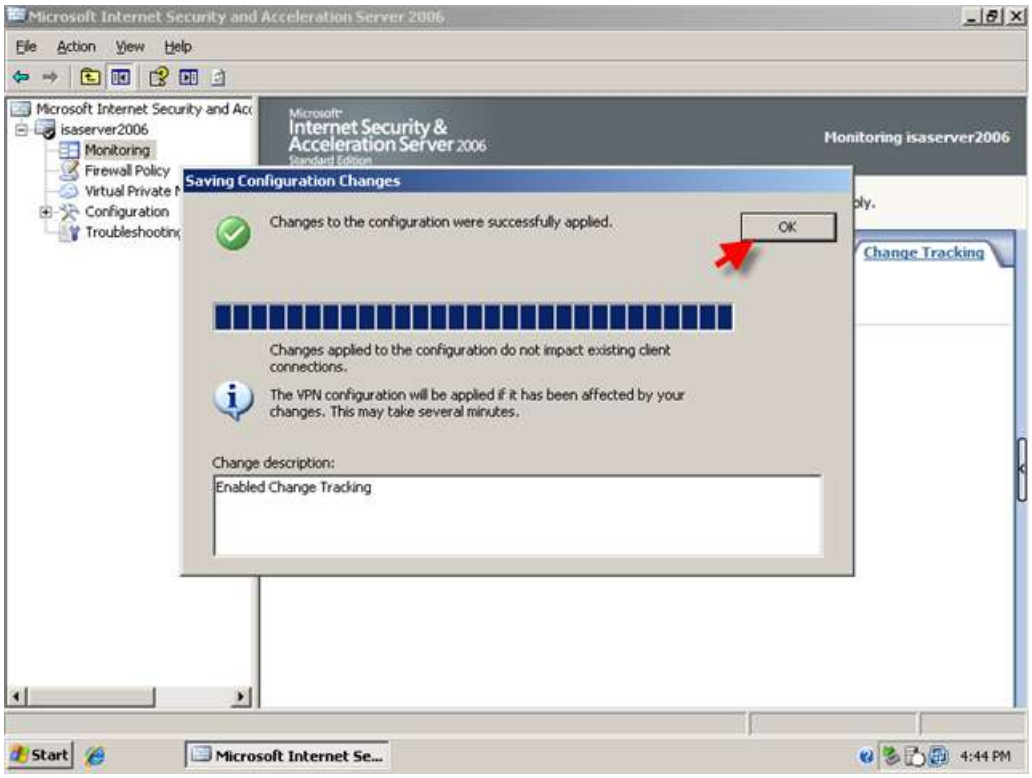
4. Click Apply.



5. You will be prompted to enter a description about your changes – Enter ' Enabled Change Tracking'. You may notice the 'Export' button. Clicking this will allow you to export your Firewall Configuration before the change is applied, this is great for rolling back a change which had adverse effects to your system. We will go through ISA Server backup in the next section.



6. Click OK

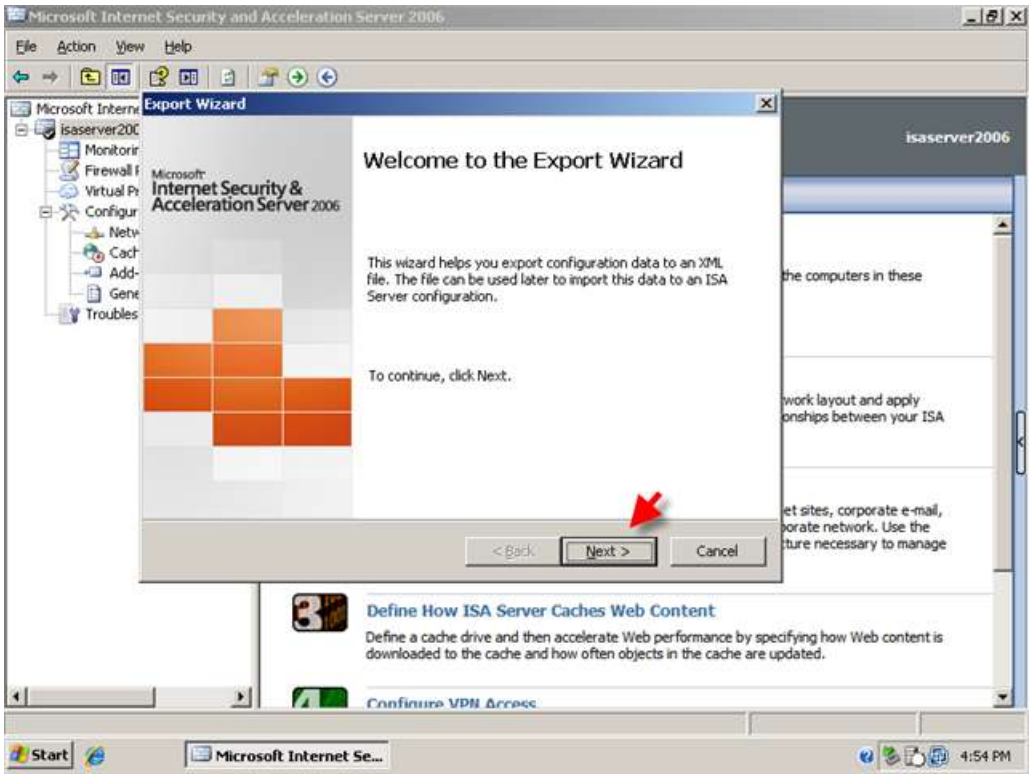

Microsoft Internet Security and Acceleration Server 2006
File Action View Help
Microsoft Internet Security and Acc
isaserver2006
Monitoring
Firewall Policy
Virtual Private N
Configuration
Troubleshooting
Internet Security & Acceleration Server 2006
Monitoring isaserver2006
Saving Configuration Changes
Changes to the configuration were successfully applied.
OK
Change Tracking
Changes applied to the configuration do not impact existing client connections.
The VPN configuration will be applied if it has been affected by your changes. This may take several minutes.
Change description:
Enabled Change Tracking
Start
Microsoft Internet Se...
4:44 PM

Creating a Backup of the ISA Server Configuration

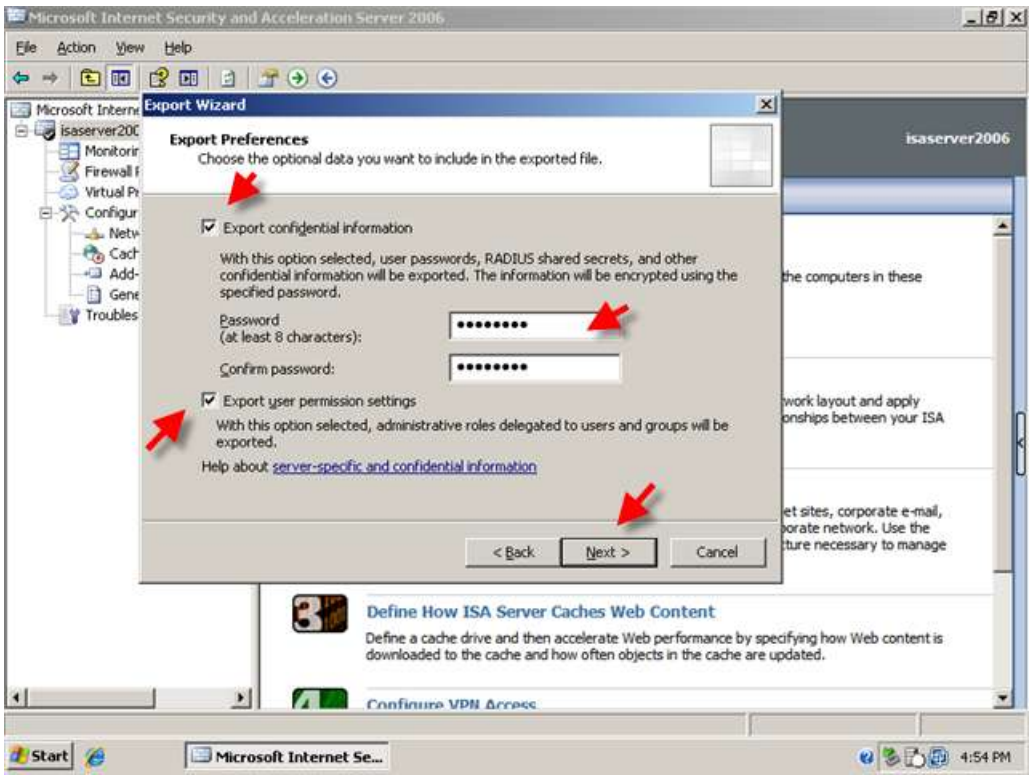
Backing up your ISA Server configuration periodically is a very good idea, backing it up before you make any changes is, I think, a best practice. How many times have you made a change to something, only to realize the situation is now worse? It always seems to happen at the most inconvenient times and you can bet your life you can never find your notes (you have notes right?) on how to set things correctly. Fortunately we can backup and restore the ISA Server config in a matter of seconds hopefully to avoid any situations like this.

1. From ISA Server Management, Right click your server name and click Export (Backup)

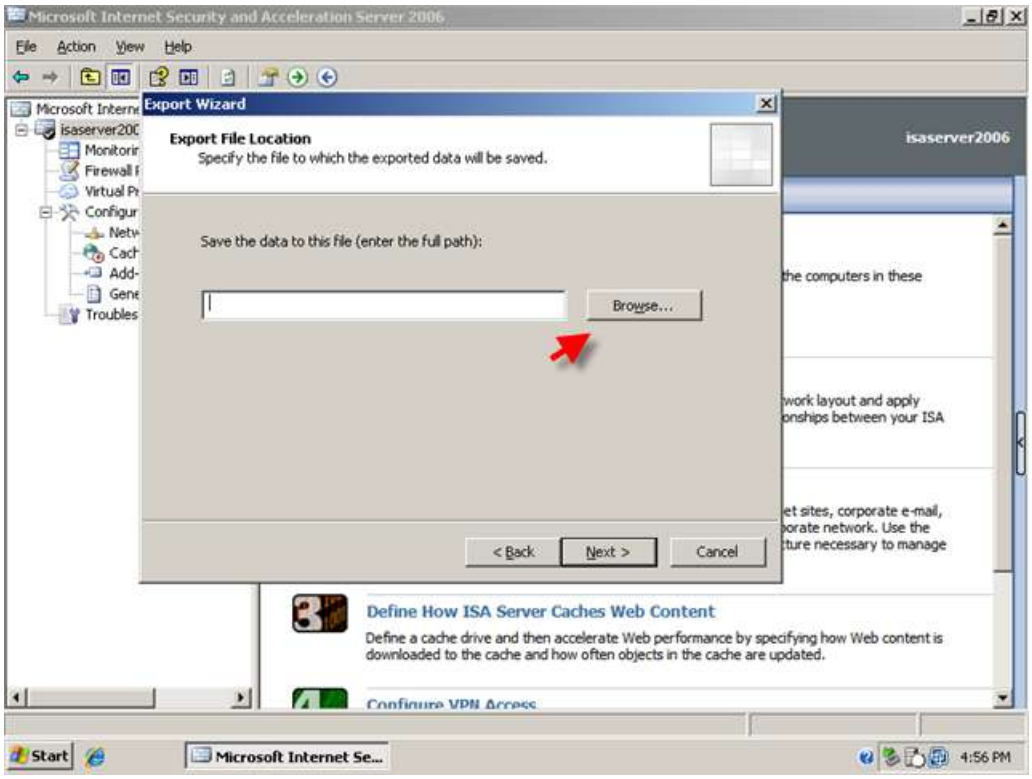
2. This will start the Export Wizard, Click Next.



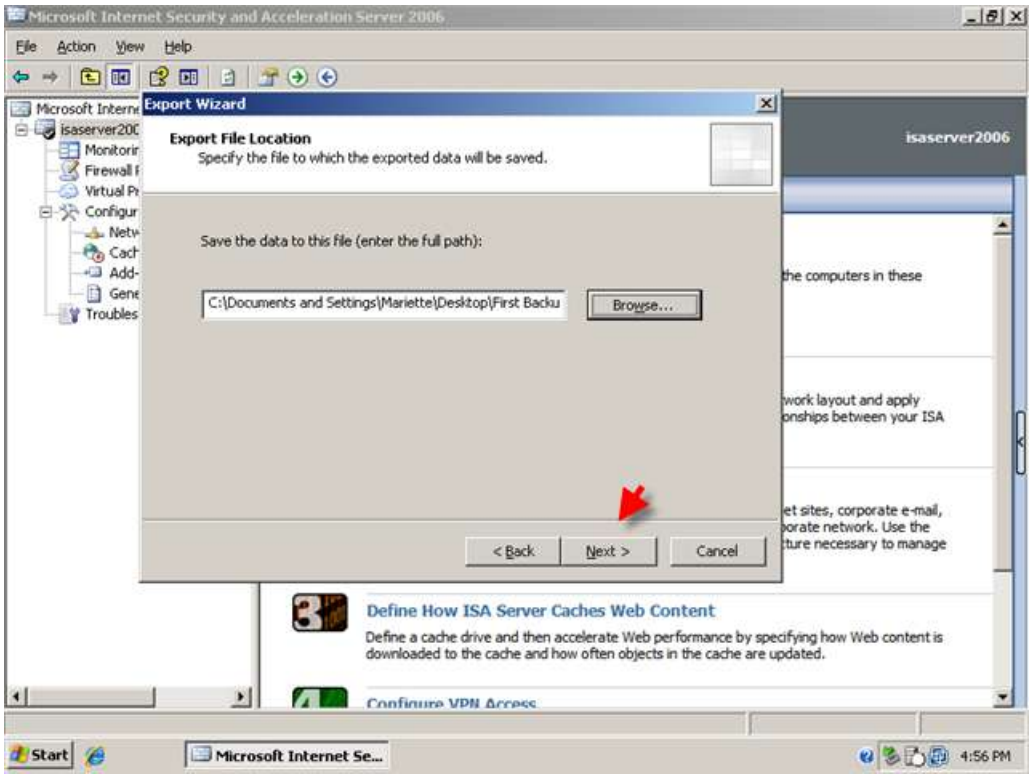
3. Check the boxes to Export Confidential Information and enter a password to encrypt the backup file. Also check the box to export user permission settings. Then click next.



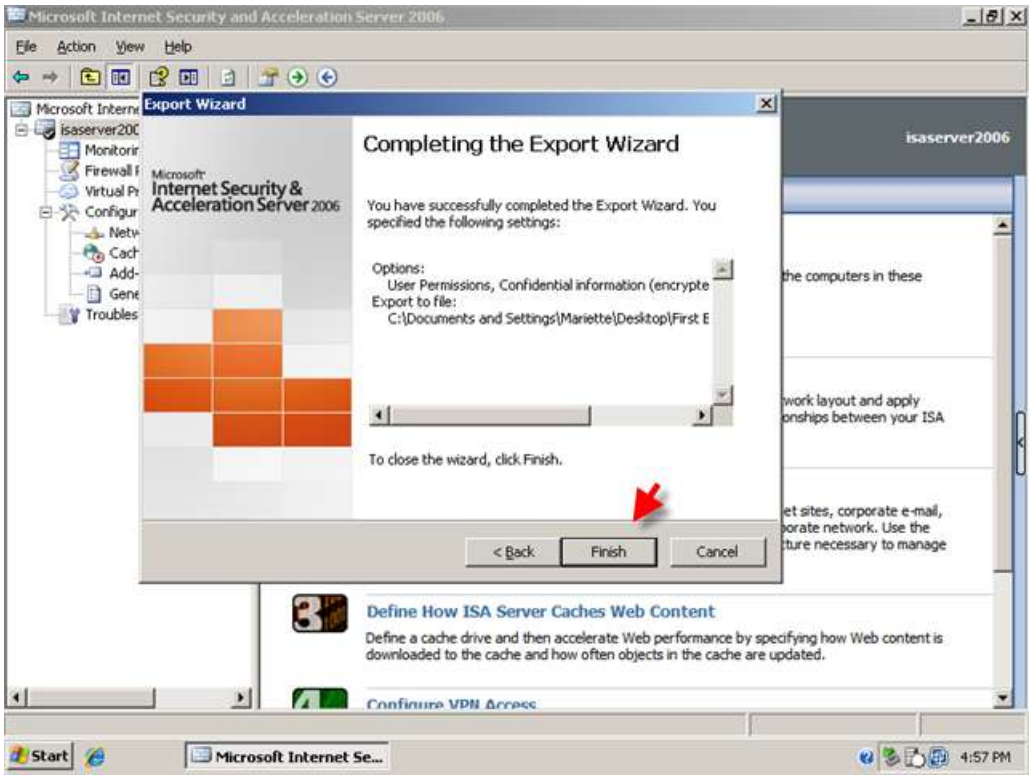
4. The next page asks you for a path to export your backup to. You can click browse to find the folder you wish to place your backups in. On some occasions you might want to use removable media in case of hardware failure.

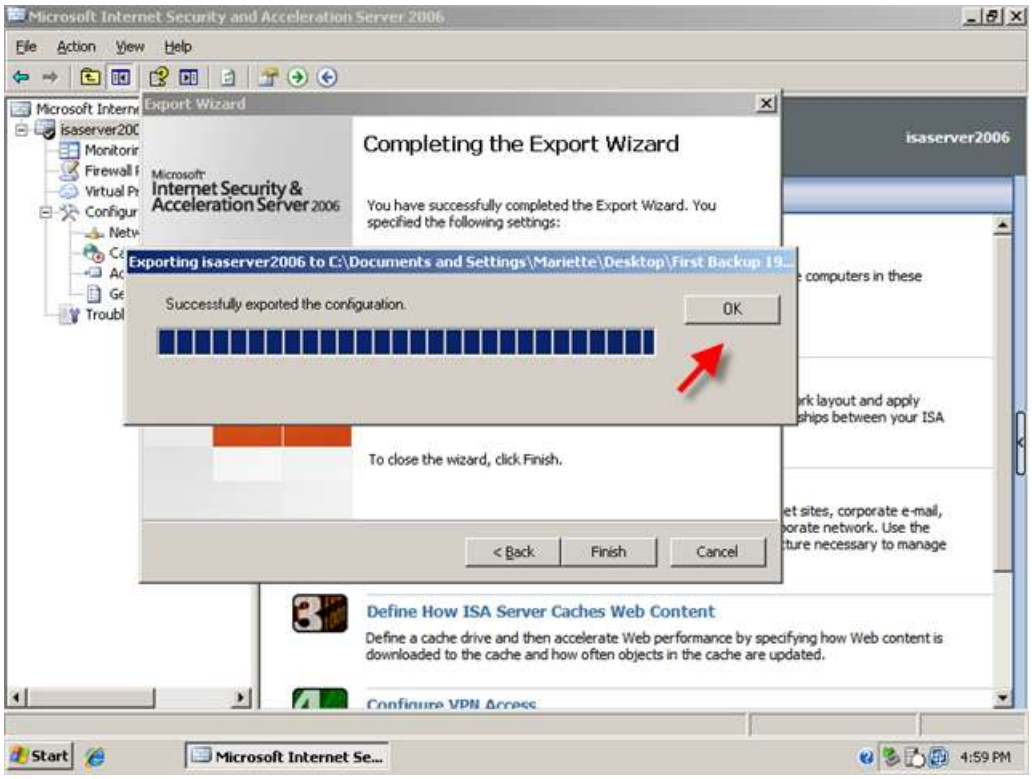


5. Find your location and enter a descriptive name for the backup file. I am calling my file 'First Backup 190209-1153am' as it is the first backup I have done, it is the 19th of February 2009 at 11:53 am. Click Open when you have entered your file name. You are taken back to the Export file location page, and the path information is now filled in. Click next.



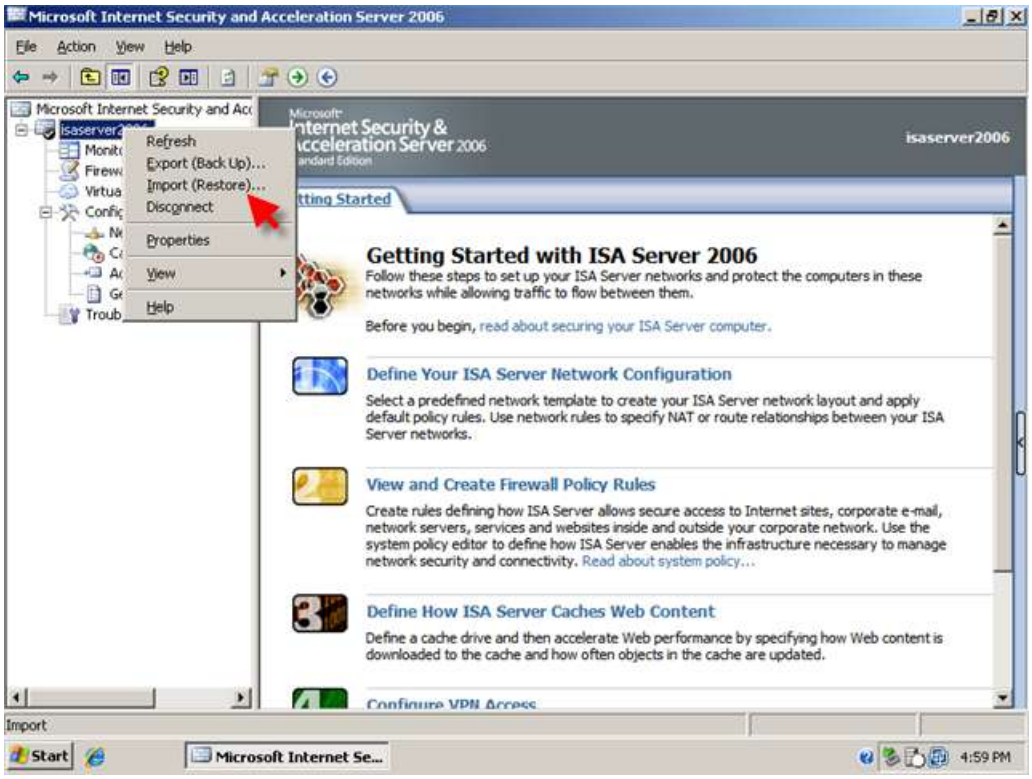
6. You can review your export settings and click Finish to export your configuration. Click OK when the export has finished to be returned to ISA Management.

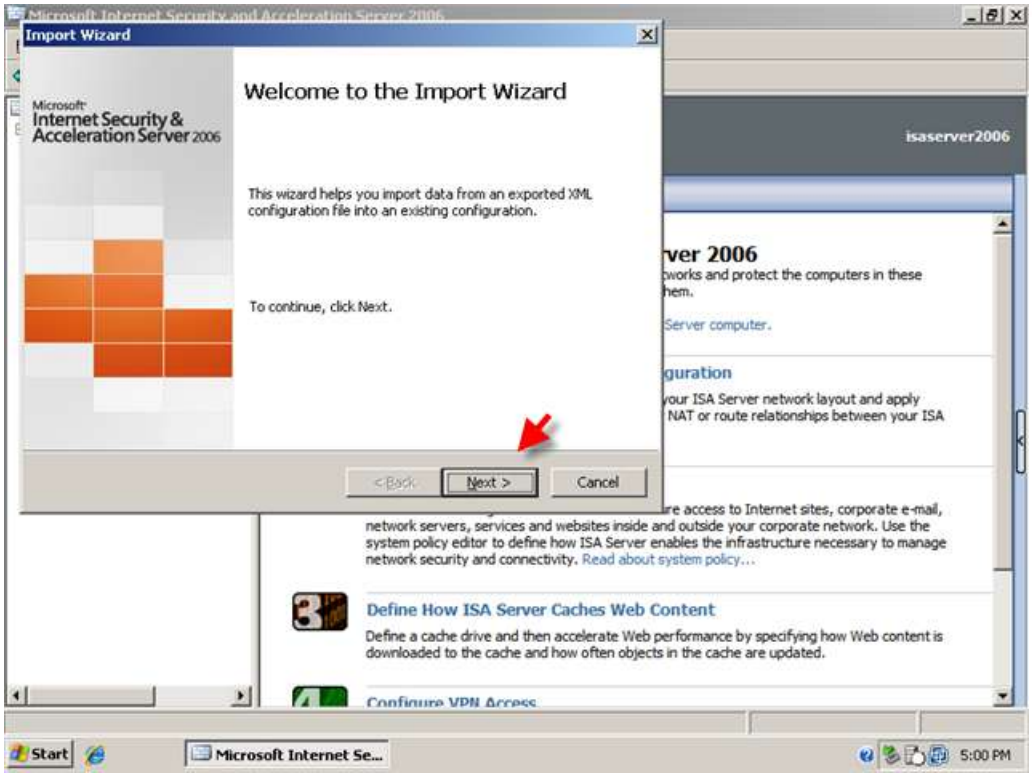




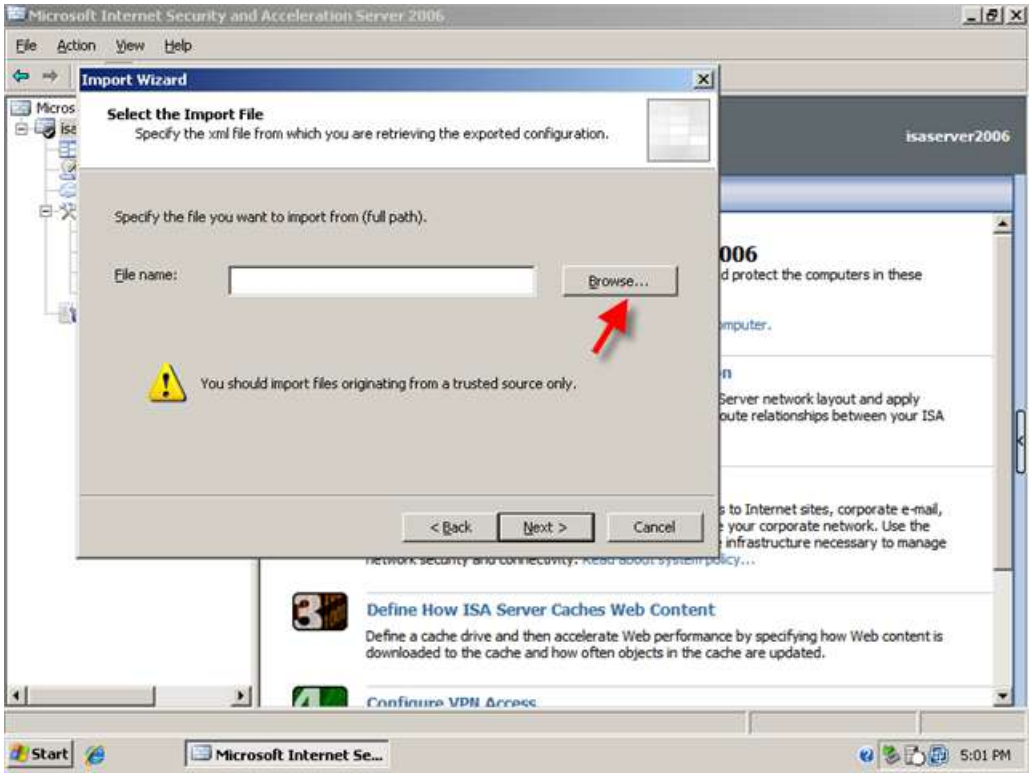
The restore procedure has two options. Import or Overwrite. You will need to decide for yourself at the time, whether the situation requires an import or overwrite. The import function can also be used to import specific objects that you may have exported from ISA server, Such as rules, web listeners or address ranges. That is beyond the scope of this article more information can be found on technet.

1. To restore your ISA Config:Right click your server name and click 'Import (Restore)'. This starts the Import Wizard. Click Next.

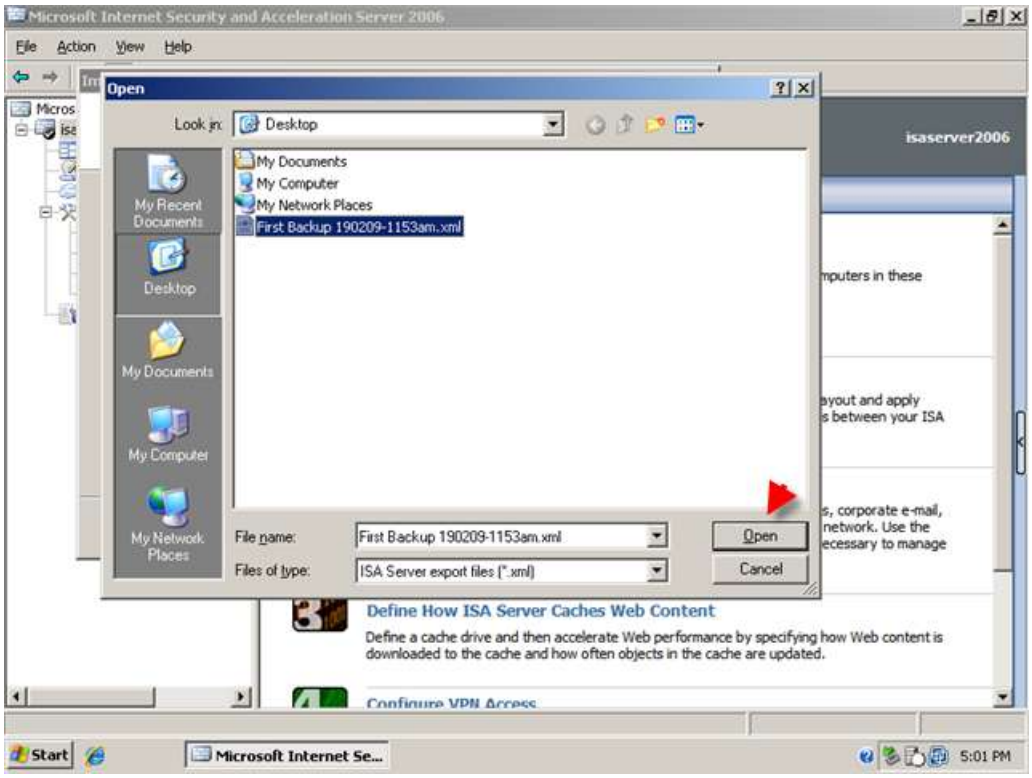




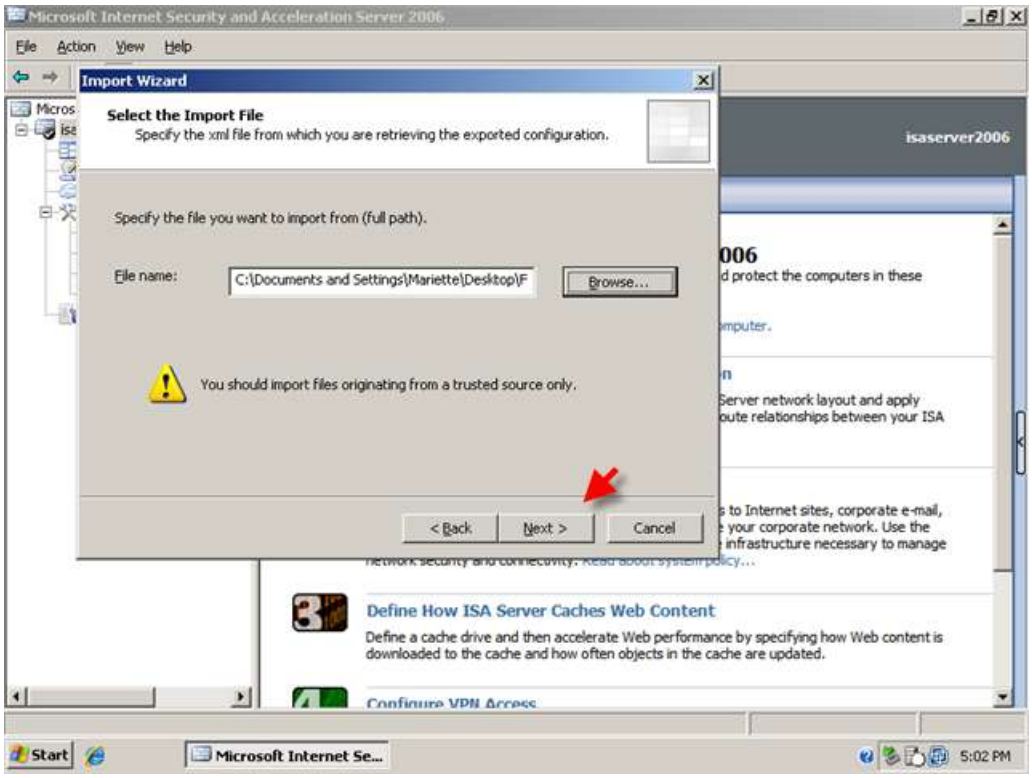
2. Click Browse to find your backup file. (usually it will default to the location of your last backup)



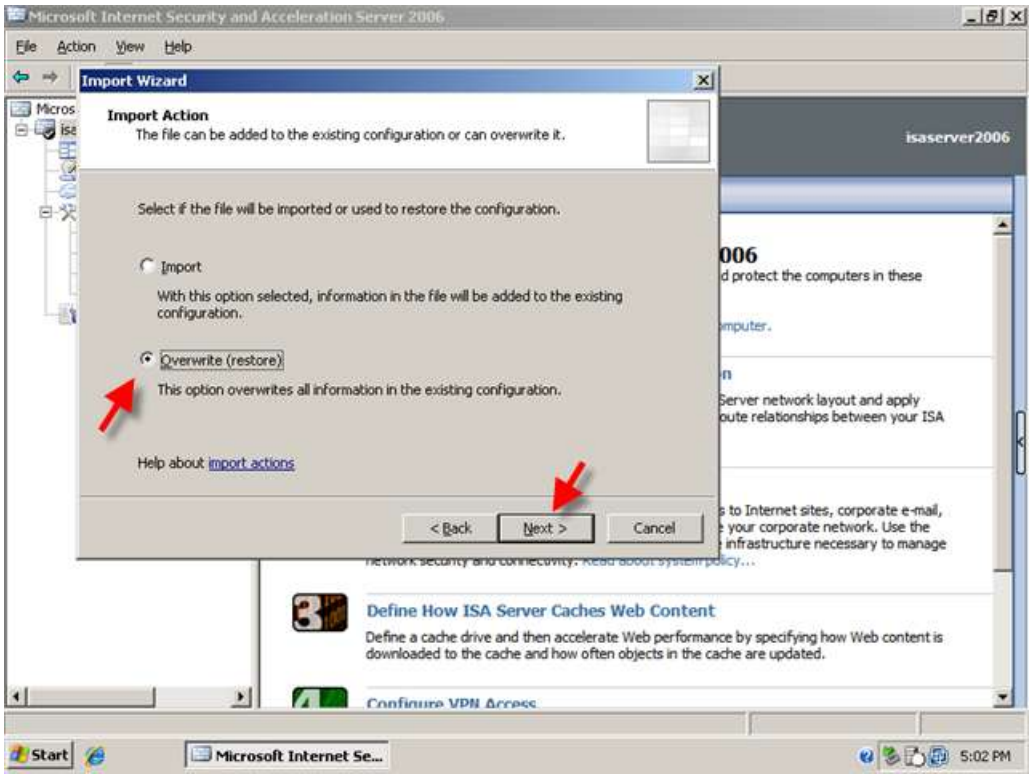
3. Select your file and click Open.



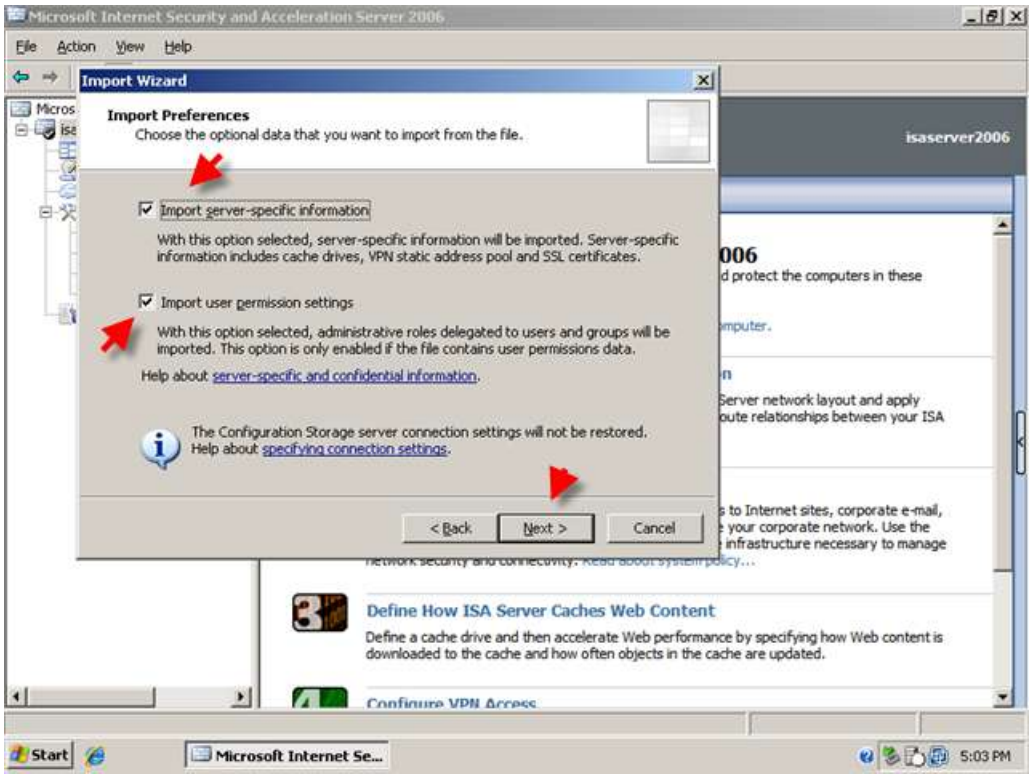
4. You are then returned to the Select import file page and the path information is filled in. Click Next.



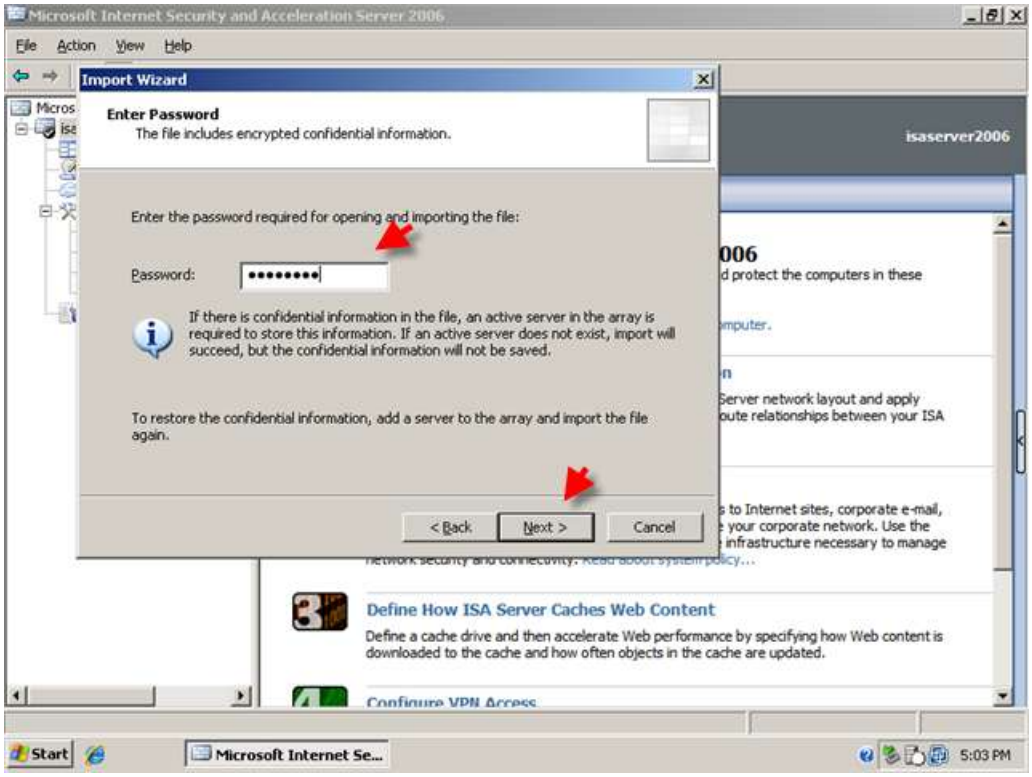
5. You are then asked to choose, Import or Overwrite (restore) Choose Overwrite. Click Next.



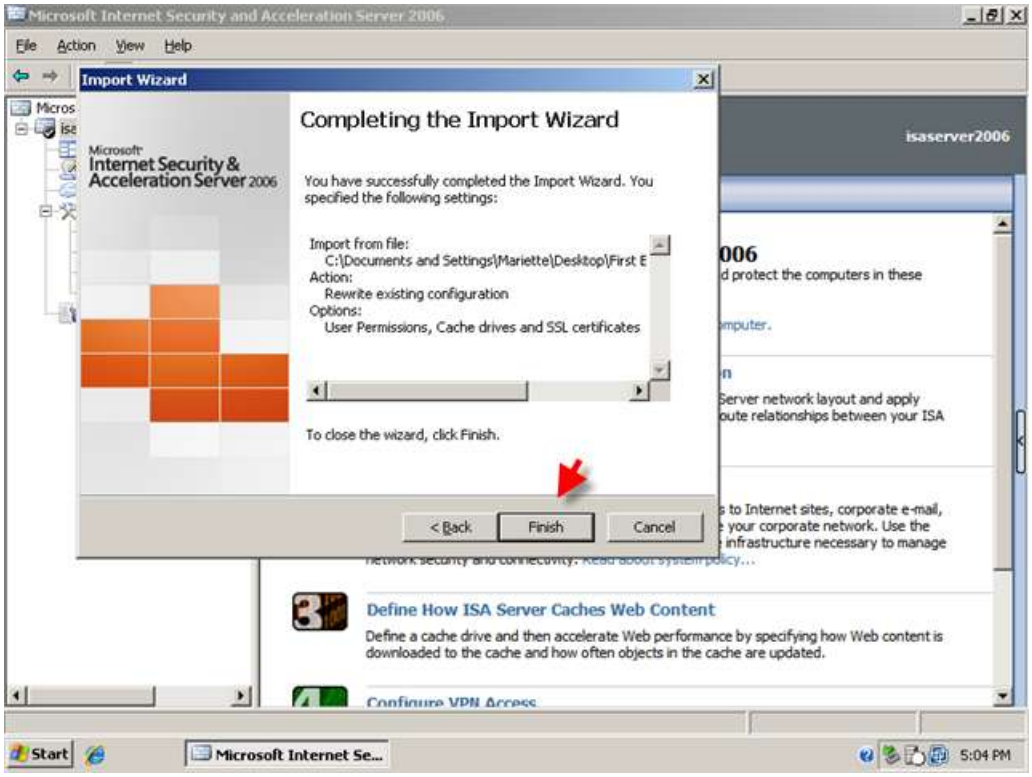
6. Check both boxes to import Server specific information and user permissions. Click Next.

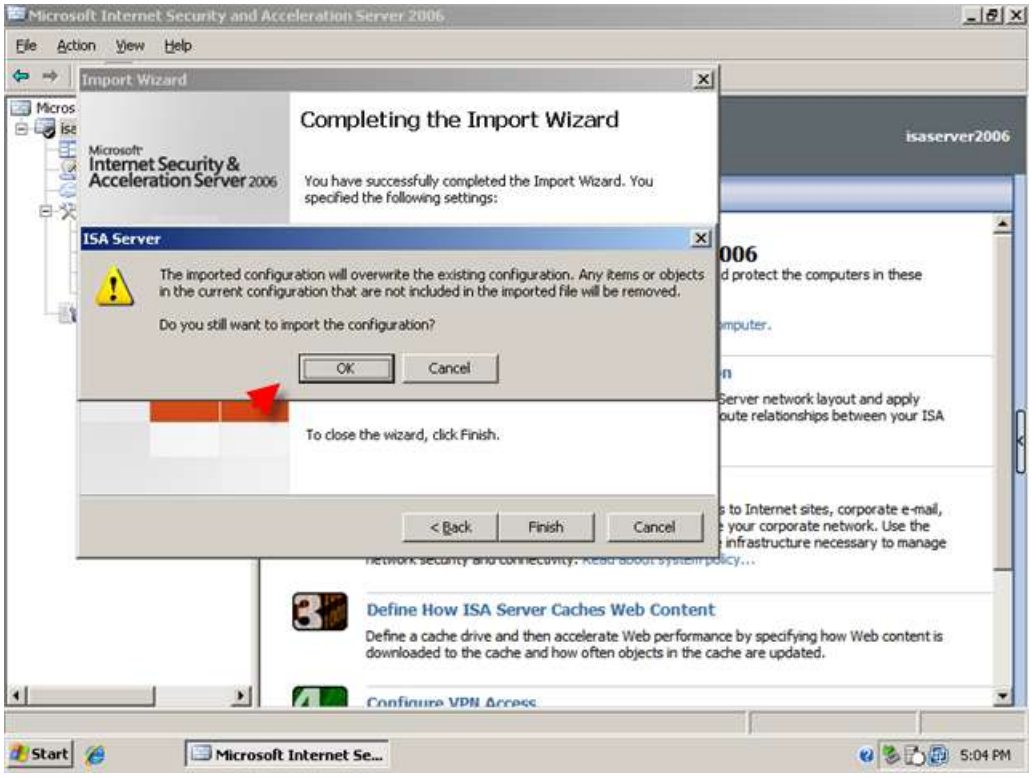


7. Enter your password and click Next

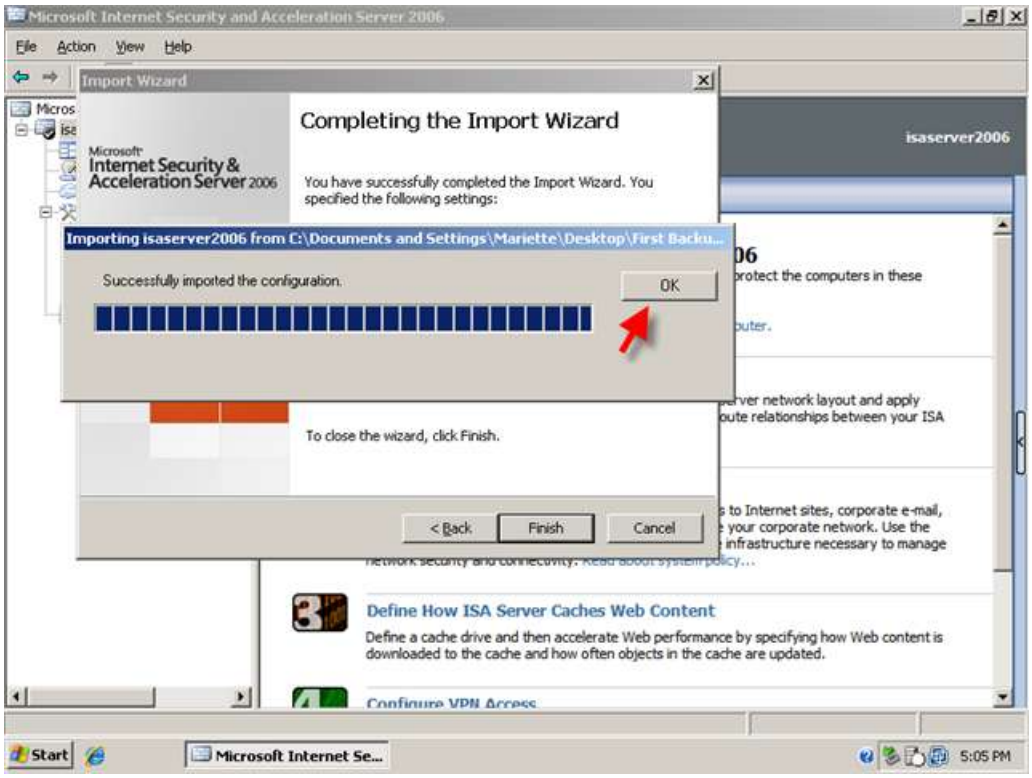


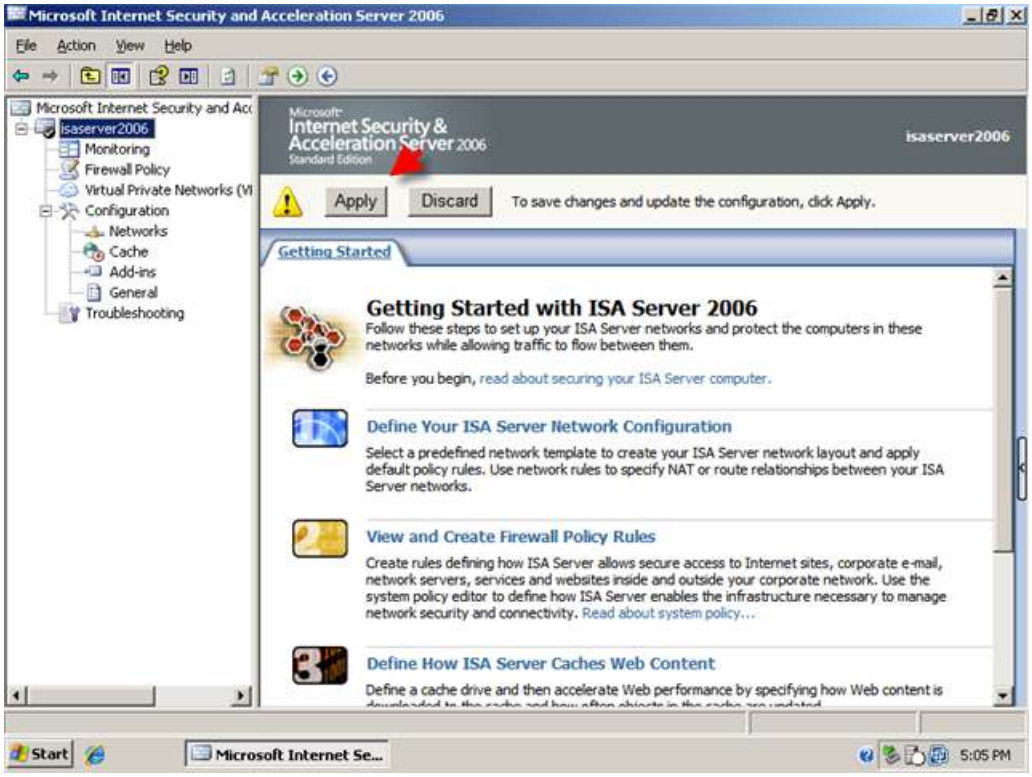
8. Review your import settings and click Finish to import your configuration. You will see a warning, explaining you are about to overwrite your firewall policy, click OK.

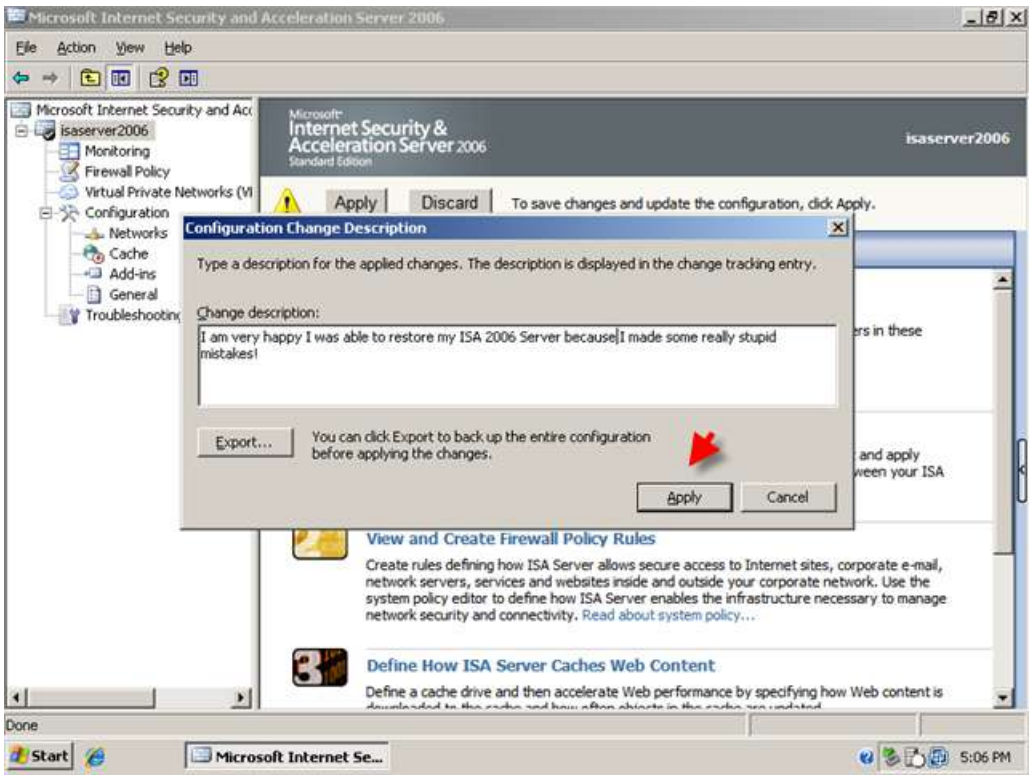


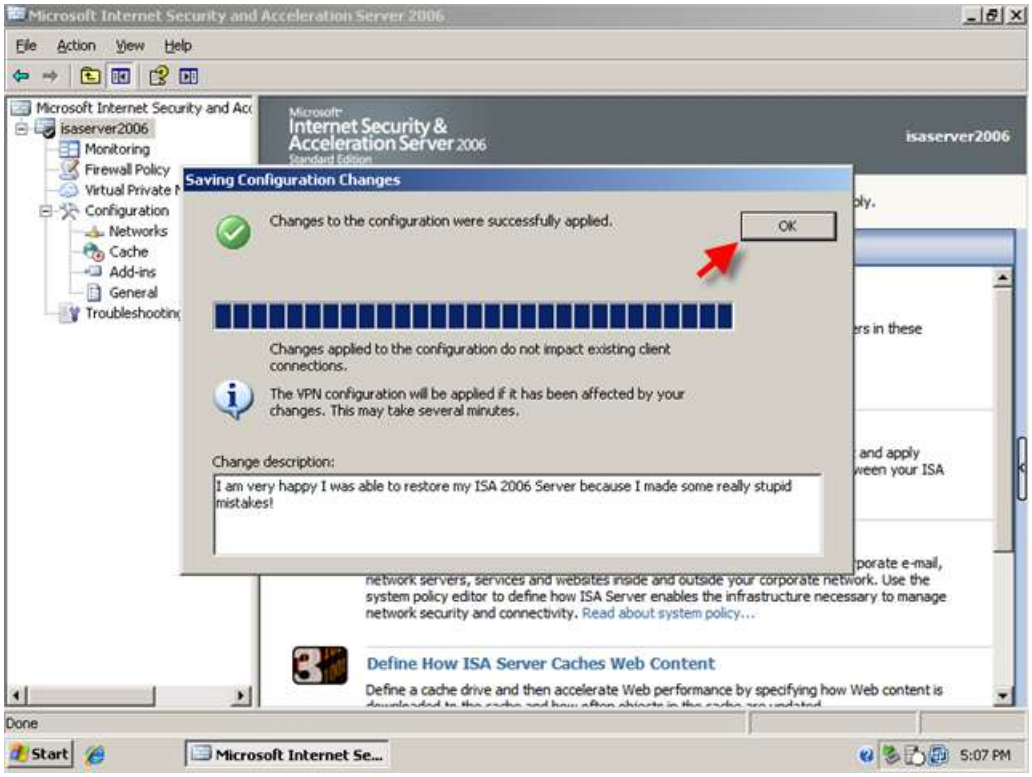


9. When the import is finished click OK to be returned to ISA Management, You will then need to click Apply to save your newly restored firewall policy. Enter a Change Description and click Apply. Click Ok when the changes have been saved.




Microsoft Internet Security and Acceleration Server 2006
File Action View Help
Microsoft Internet Security and Acc
isaserver2006
Monitoring
Firewall Policy
Virtual Private Networks (VI
Configuration
Networks
Cache
Add-ins
General
Troubleshooting
Internet Security & Acceleration Server 2006
Standard Edition
isaserver2006
Apply
Discard
To save changes and update the configuration, click Apply.
Getting Started
Getting Started with ISA Server 2006
Follow these steps to set up your ISA Server networks and protect the computers in these networks while allowing traffic to flow between them.
Before you begin, read about securing your ISA Server computer.
Define Your ISA Server Network Configuration
Select a predefined network template to create your ISA Server network layout and apply default policy rules. Use network rules to specify NAT or route relationships between your ISA Server networks.
View and Create Firewall Policy Rules
Create rules defining how ISA Server allows secure access to Internet sites, corporate e-mail, network servers, services and websites inside and outside your corporate network. Use the system policy editor to define how ISA Server enables the infrastructure necessary to manage network security and connectivity. Read about system policy...
Define How ISA Server Caches Web Content
Define a cache drive and then accelerate Web performance by specifying how Web content is
Start
Microsoft Internet Se...
5:05 PM

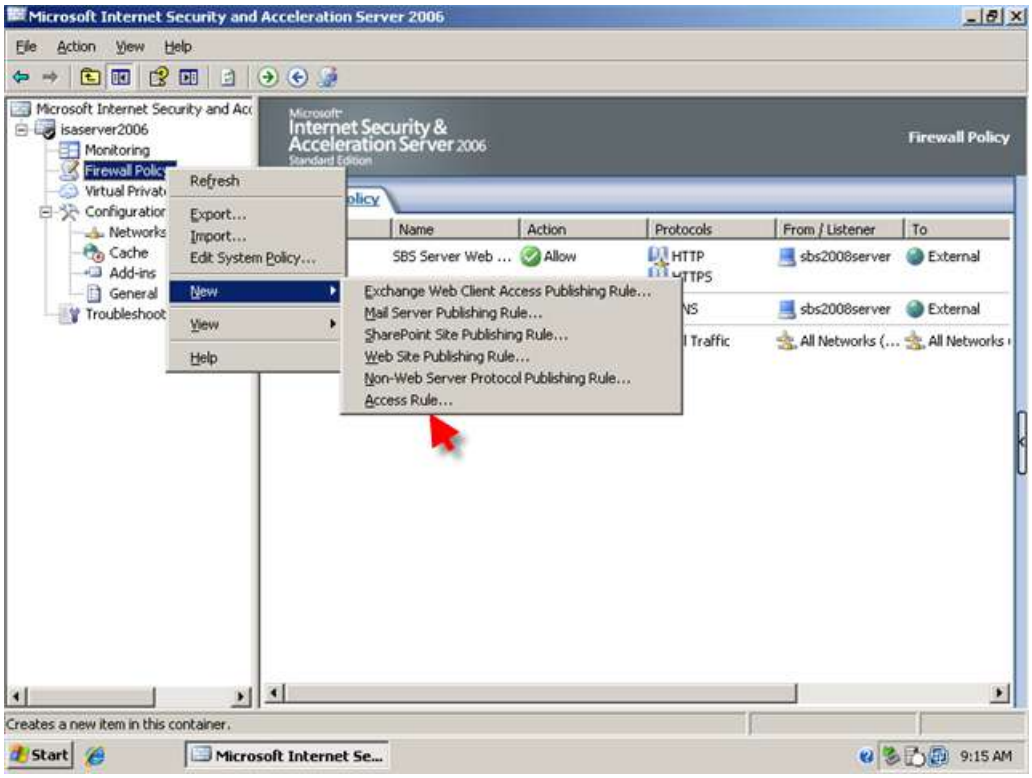

Microsoft Internet Security and Acceleration Server 2006
File Action View Help
Microsoft Internet Security and Acc
isaserver2006
Monitoring
Firewall Policy
Virtual Private Networks (VI
Configuration
Networks
Cache
Add-ins
General
Troubleshooting
Internet Security & Acceleration Server 2006
Standard Edition
isaserver2006
Apply
Discard
To save changes and update the configuration, click Apply.
Configuration Change Description
Type a description for the applied changes. The description is displayed in the change tracking entry.
Change description:
I am very happy I was able to restore my ISA 2006 Server because I made some really stupid mistakes!
Export...
You can click Export to back up the entire configuration before applying the changes.
Apply
Cancel
View and Create Firewall Policy Rules
Create rules defining how ISA Server allows secure access to Internet sites, corporate e-mail, network servers, services and websites inside and outside your corporate network. Use the system policy editor to define how ISA Server enables the infrastructure necessary to manage network security and connectivity. Read about system policy...
Define How ISA Server Caches Web Content
Define a cache drive and then accelerate Web performance by specifying how Web content is
Done
Start
Microsoft Internet Se...
5:06 PM


Microsoft Internet Security and Acceleration Server 2006
File Action View Help
Microsoft Internet Security and Acc
isaserver2006
Monitoring
Firewall Policy
Virtual Private N
Configuration
Networks
Cache
Add-ins
General
Troubleshooting
Microsoft Internet Security & Acceleration Server 2006
Standard Edition
isaserver2006
Saving Configuration Changes
Changes to the configuration were successfully applied.
OK
Changes applied to the configuration do not impact existing client connections.
The VPN configuration will be applied if it has been affected by your changes. This may take several minutes.
Change description:
I am very happy I was able to restore my ISA 2006 Server because I made some really stupid mistakes!
network servers, services and websites inside and outside your corporate network. Use the system policy editor to define how ISA Server enables the infrastructure necessary to manage network security and connectivity. Read about system policy...
Define How ISA Server Caches Web Content
Define a cache drive and then accelerate Web performance by specifying how Web content is
Done
Start
Microsoft Internet Se...
5:07 PM

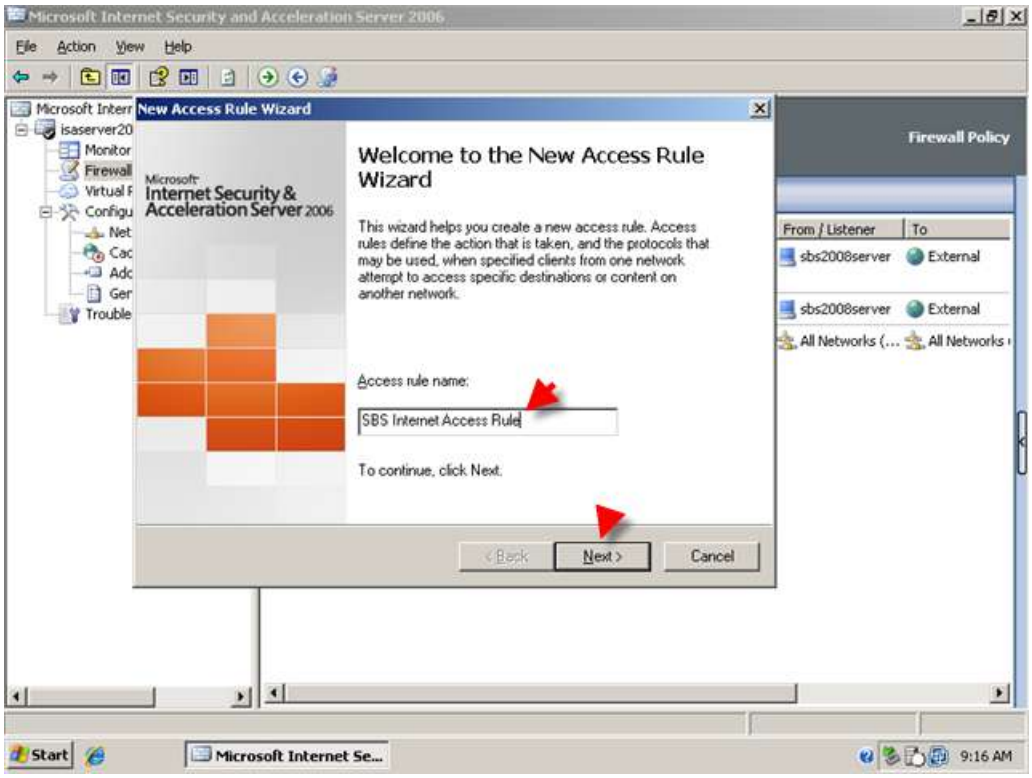
Allowing HTTP/HTTPS Access to your internal clients.

So we have configured ISA Server to allow our SBS Server to query external DNS Servers, and access the websites configured in the' system policy allowed sites' domain name set (part 1 of this guide). No one else can access the internet so lets setup a rule to allow HTTP and HTTP access.

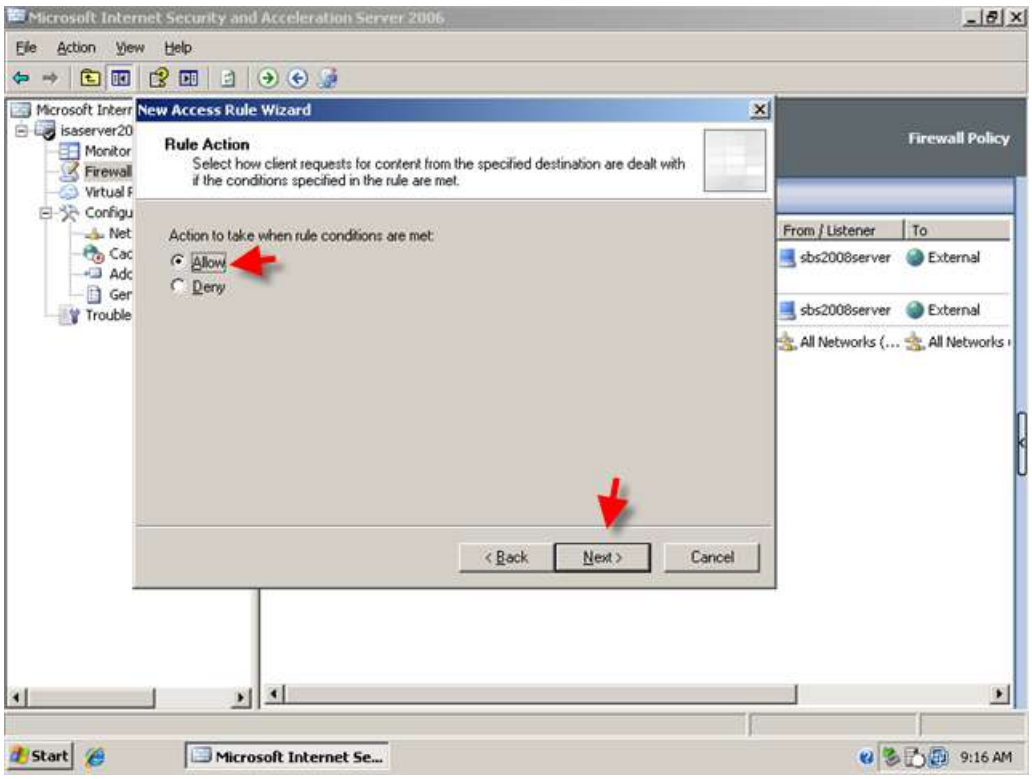
1. From ISA Management, Right click the Firewall Policy and click New > Access Rule.



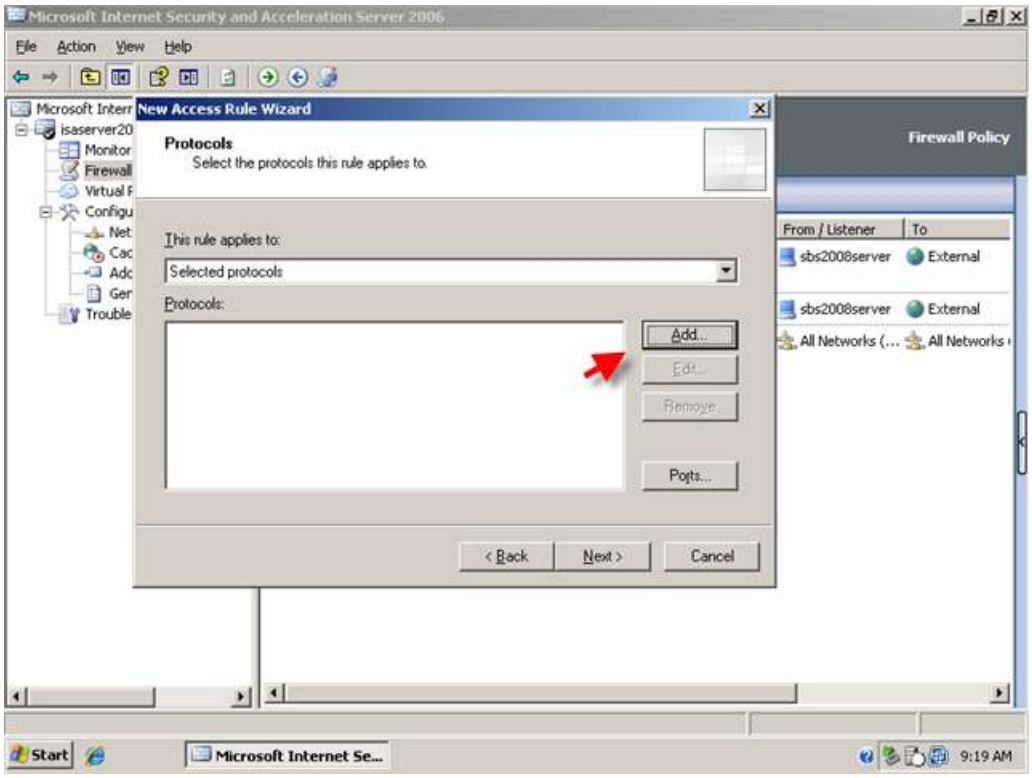
2. In the New Access Rule Wizard, Enter a Name for your Rule. I will call my rule 'SBS Internet Access Rule'.



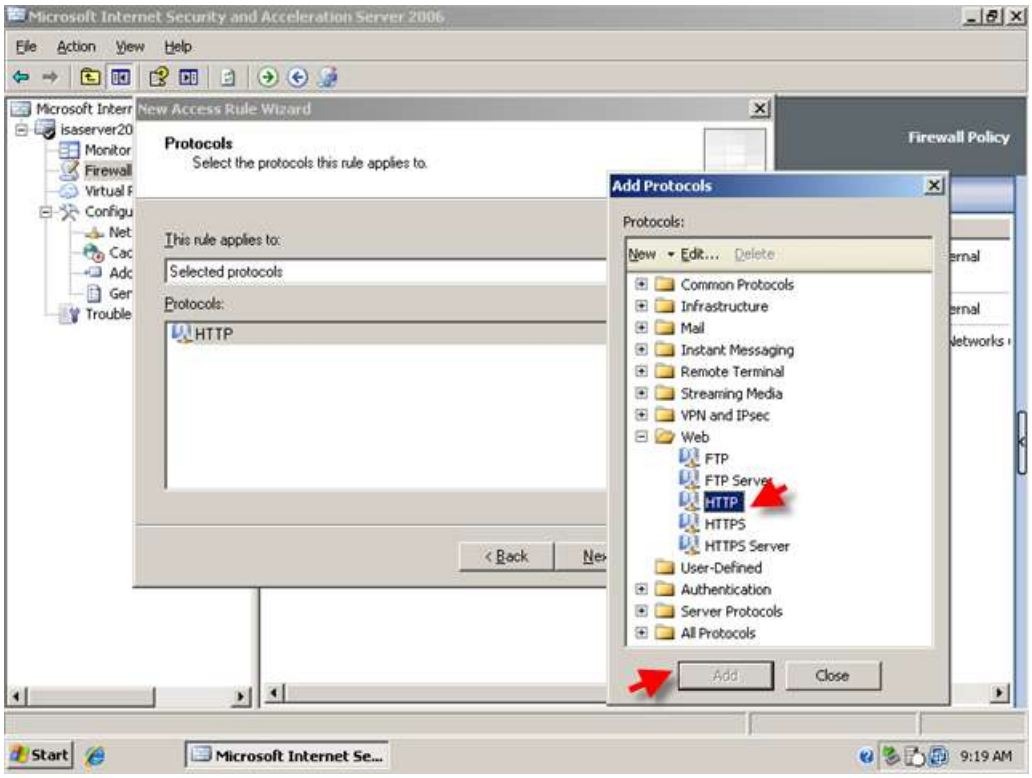
3. In SBS 2003, this rule allowed outbound access to any defined protocol (all outbound protocols) but with this rule we will just allow HTTP and HTTPS. Set the Rule to Allow and click Next.



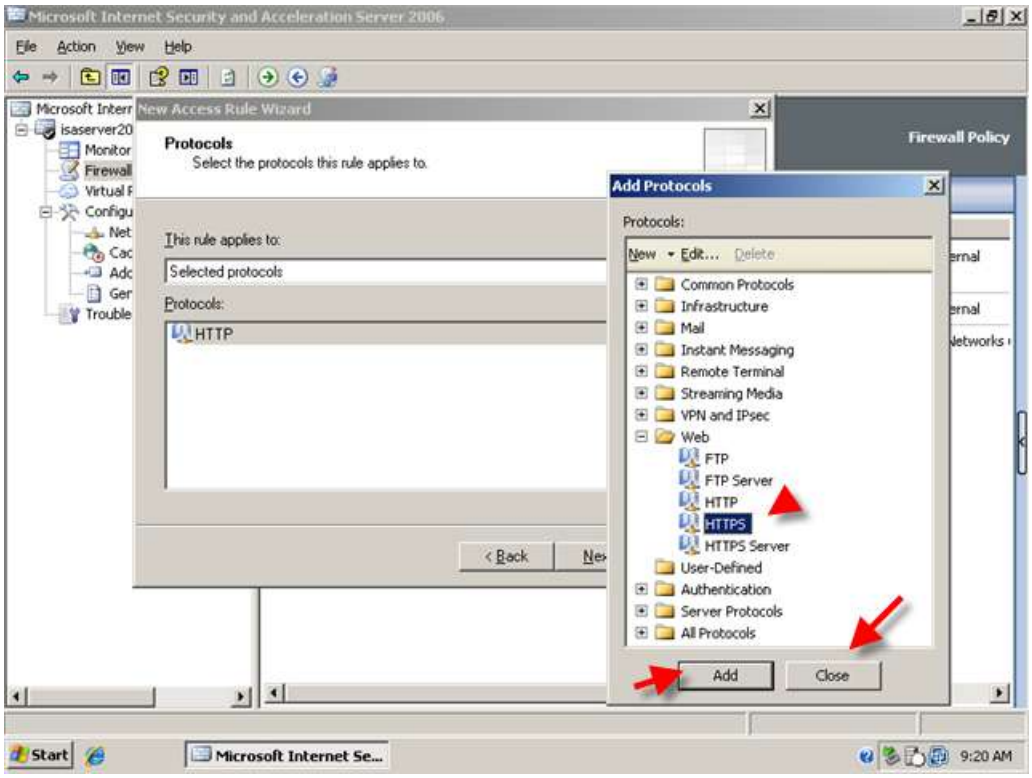
4. On the Protocols page, click Add.



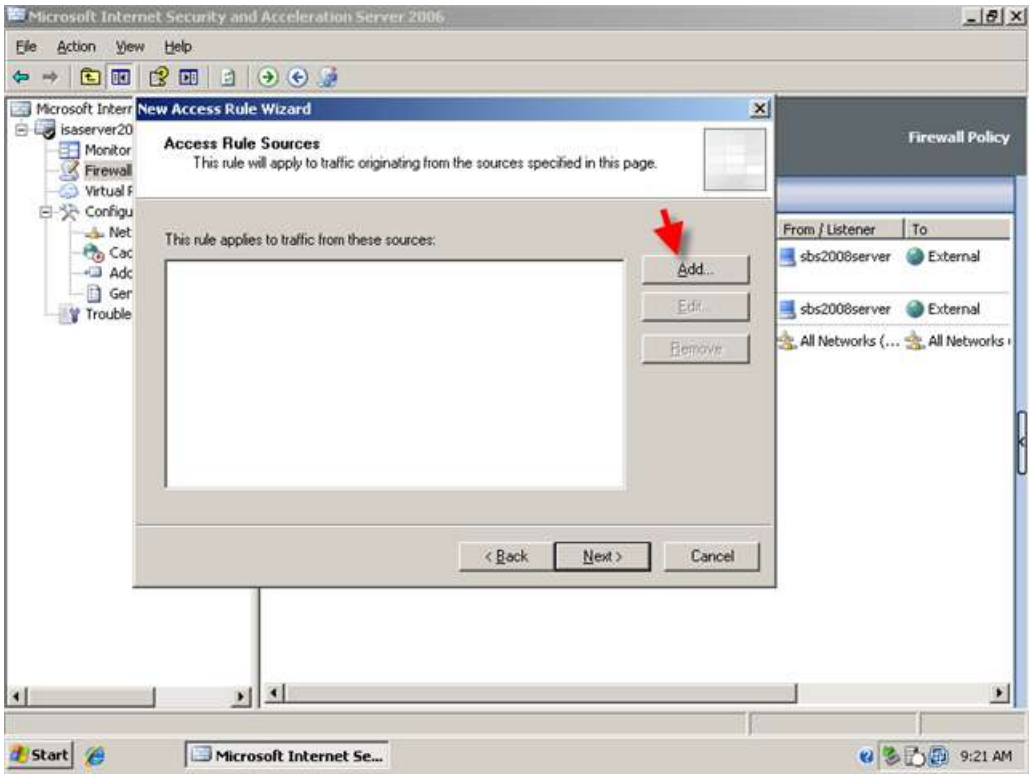
5. Expand Web, and select HTTP. Click Add.



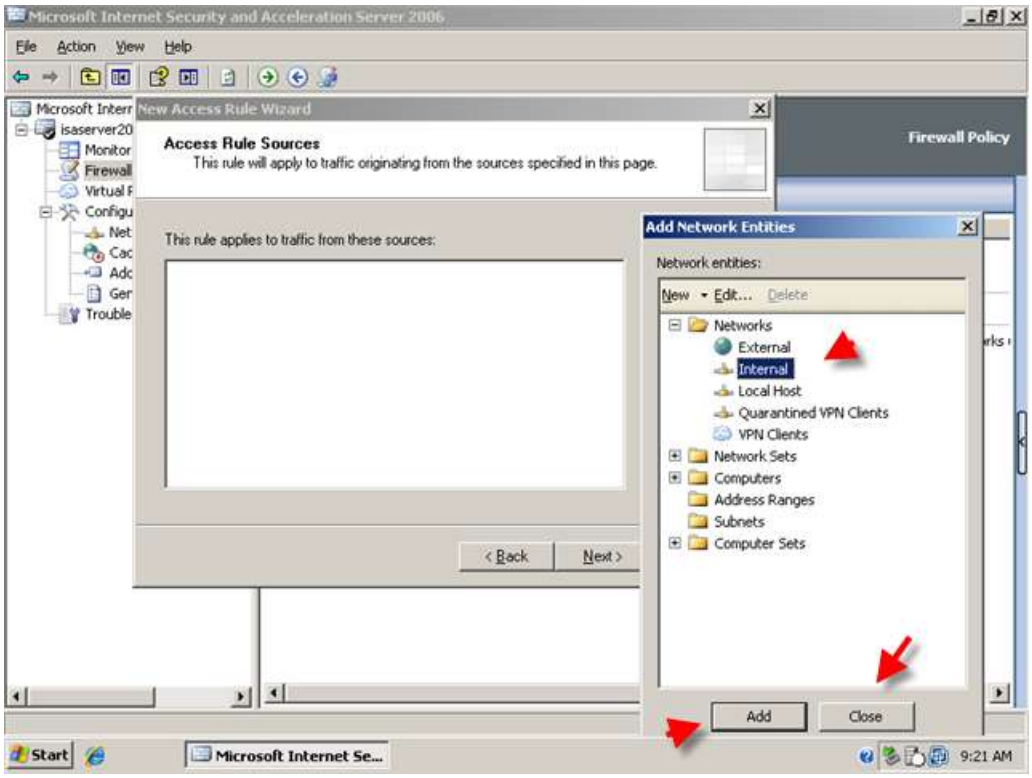
6. Then select HTTPS. Click Add. Then Click Close. The two protocols are now displayed in the list, click Next.



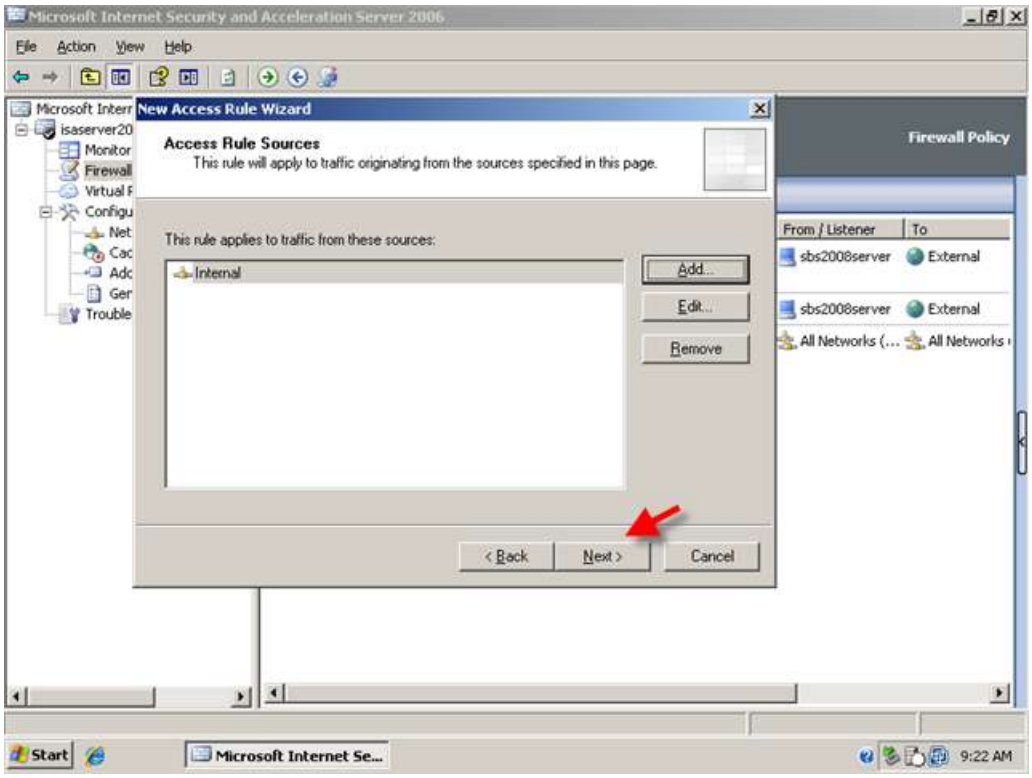
7. On the Access Rule Sources page, click Add.



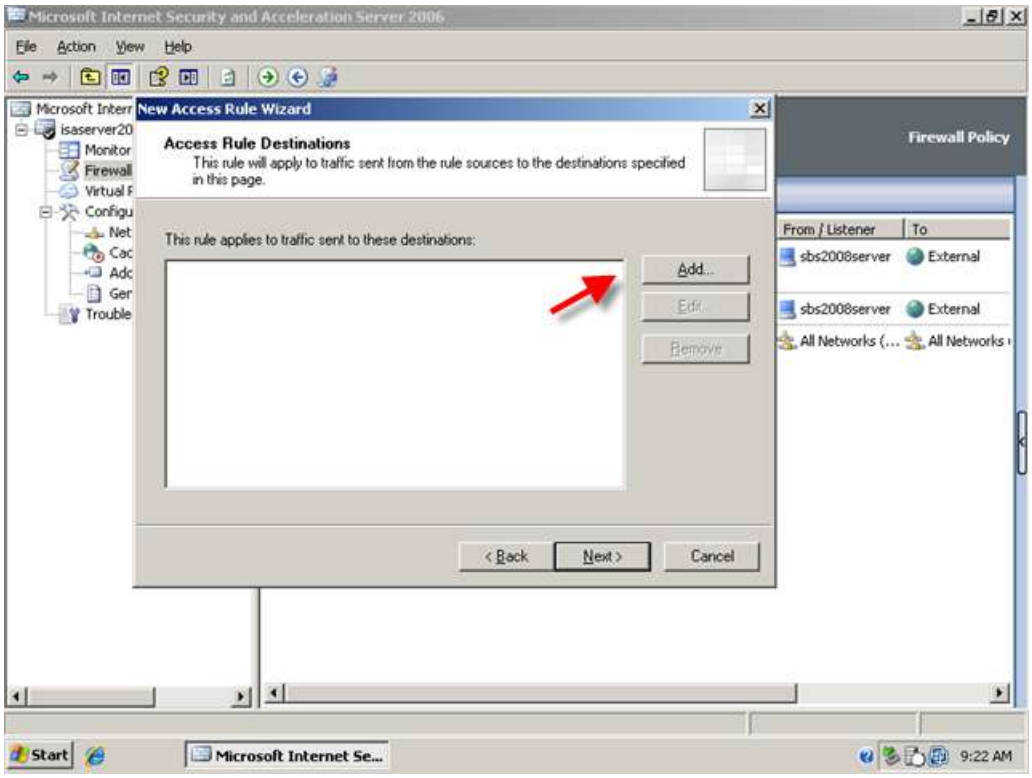
8. Expand Networks. Select the Internal Network. Click Add. Then click Close.



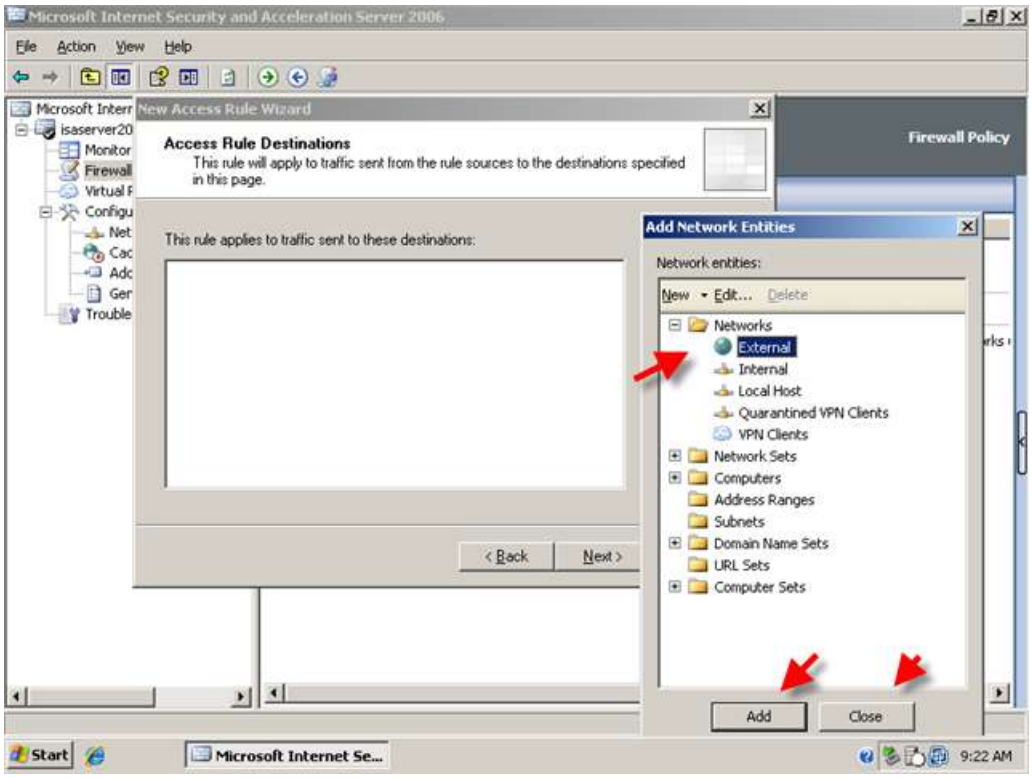
9. The Internal network object is displayed in the list, Click Next.



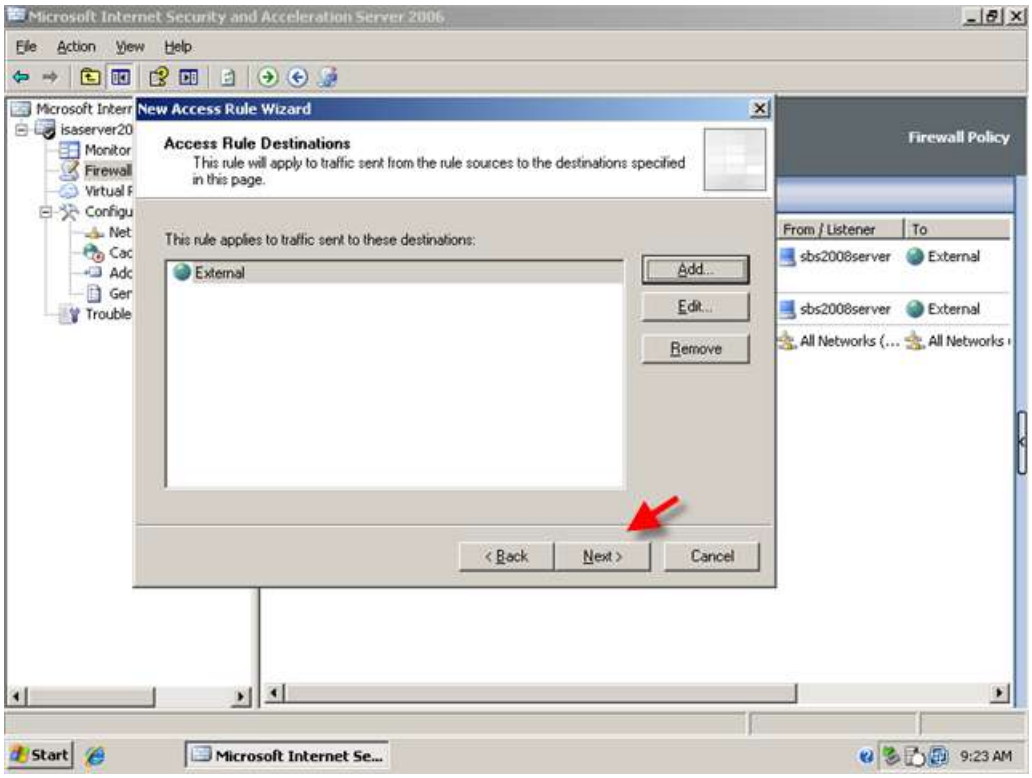
10. On the Access Rule Destinations page, click Add.



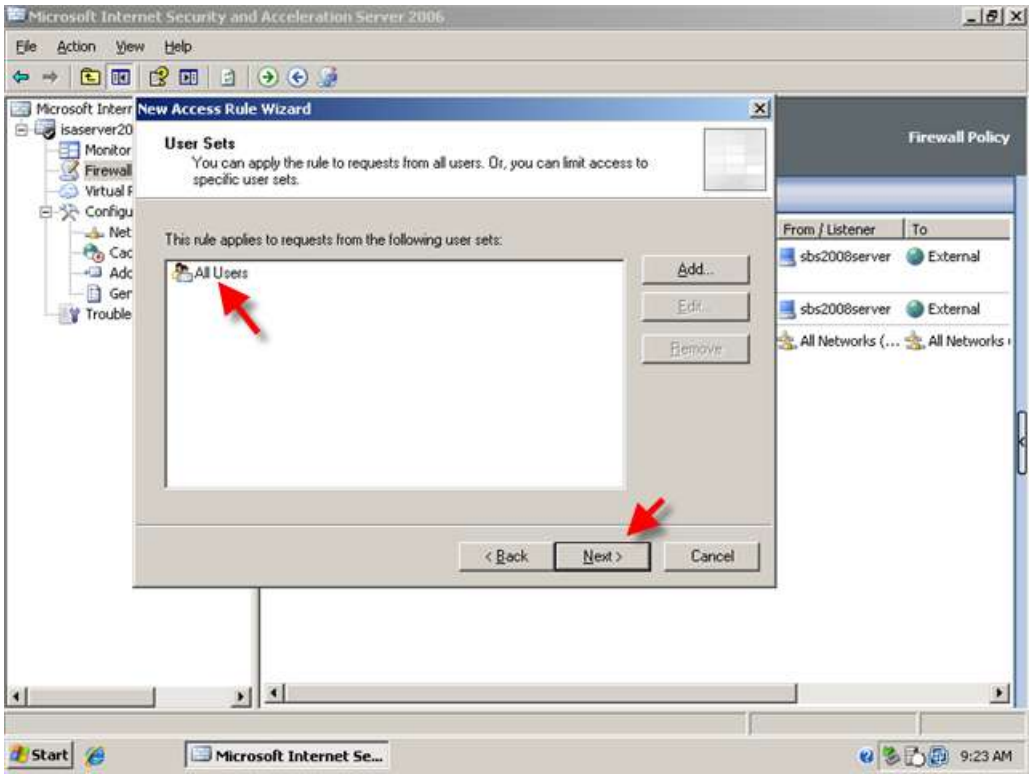
11. Expand Networks, Select the External Network. Click Add. Then click Close.



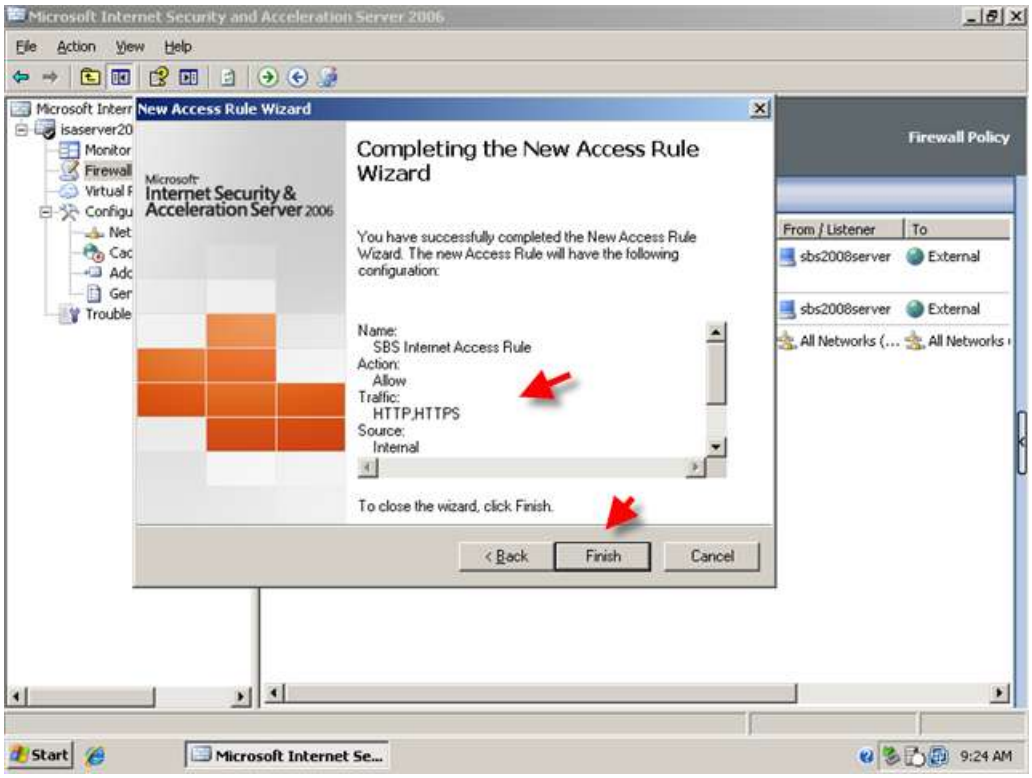
12. The External Network Object is displayed in the list, Click Next.



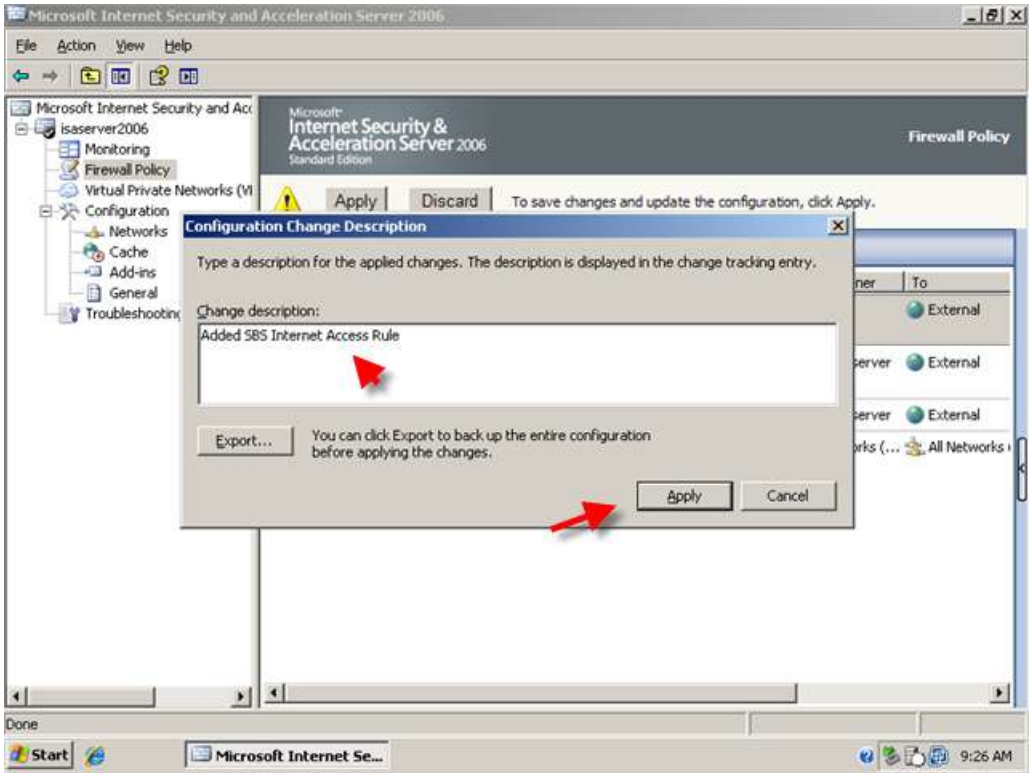
13. On the User Sets page, Leave the default 'All Users' and click Next.



14. On the next page you can review your Access Rule settings, and click Finish to add them to the firewall policy.



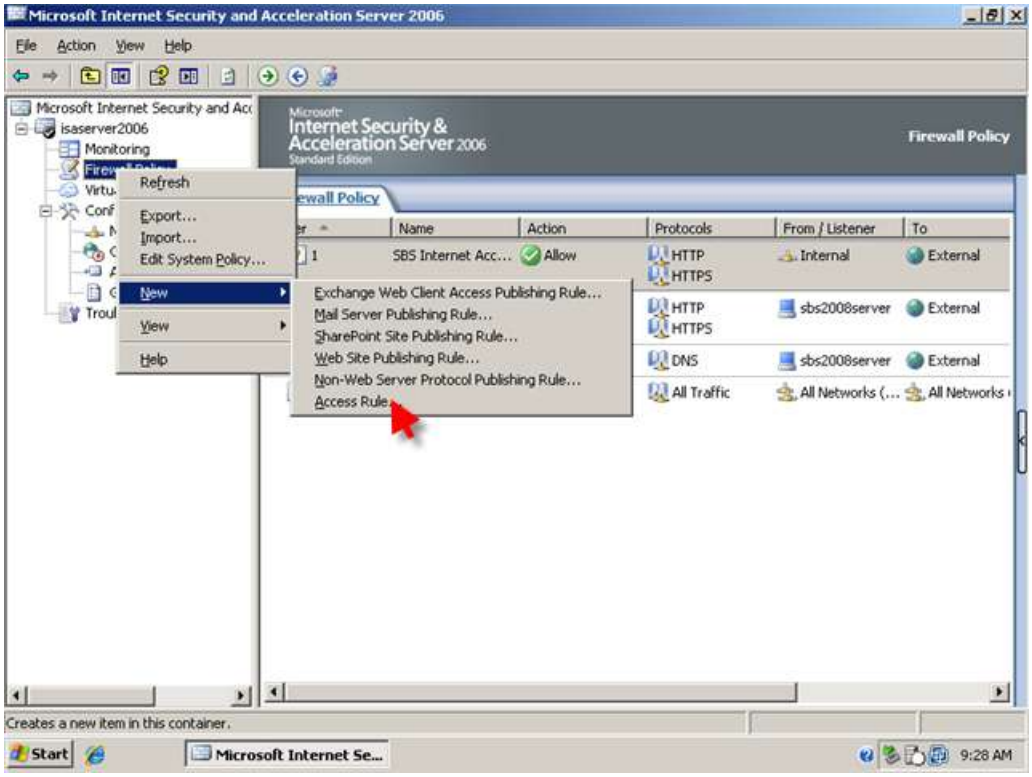
15. Switching to the Firewall Policy view, you can see your rule is added at the top of the list. Click Apply to save your changes to the Firewall Policy. Enter a comment in the change tracking description box, and click Apply. When the changes are applied, Click OK.



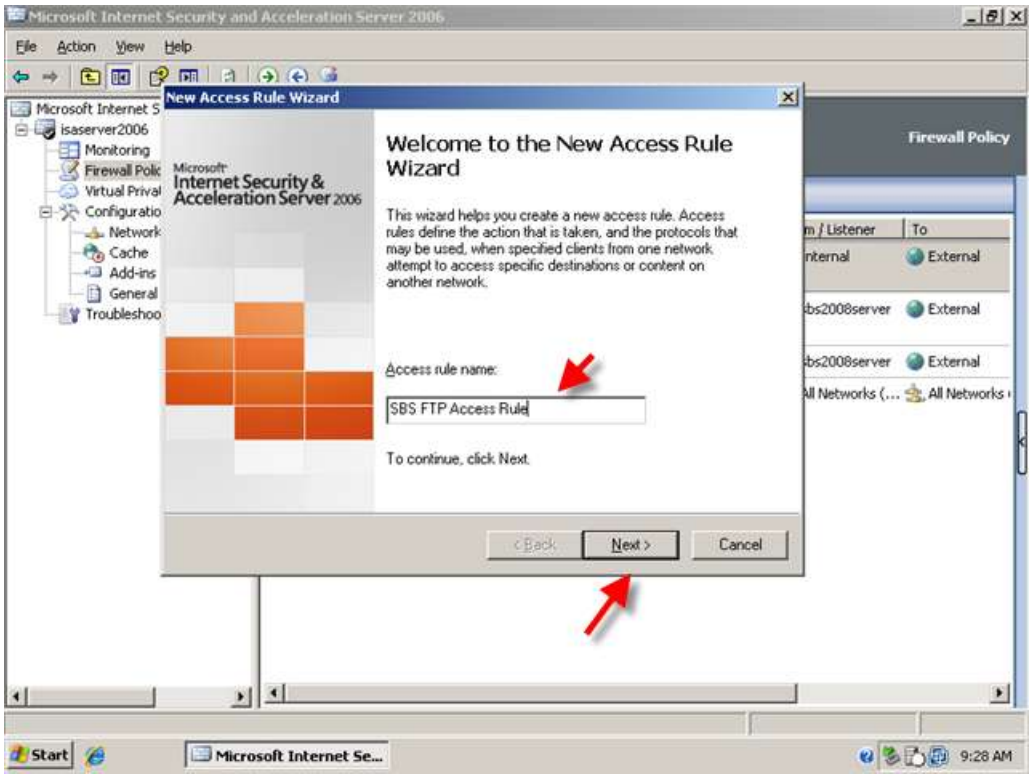
Allowing FTP Access to your Internal Clients

To allow FTP Access for your internal clients you must create an FTP access rule. If you want to allow FTP uploads you must further configure the rule as by default FTP rules are Read Only.

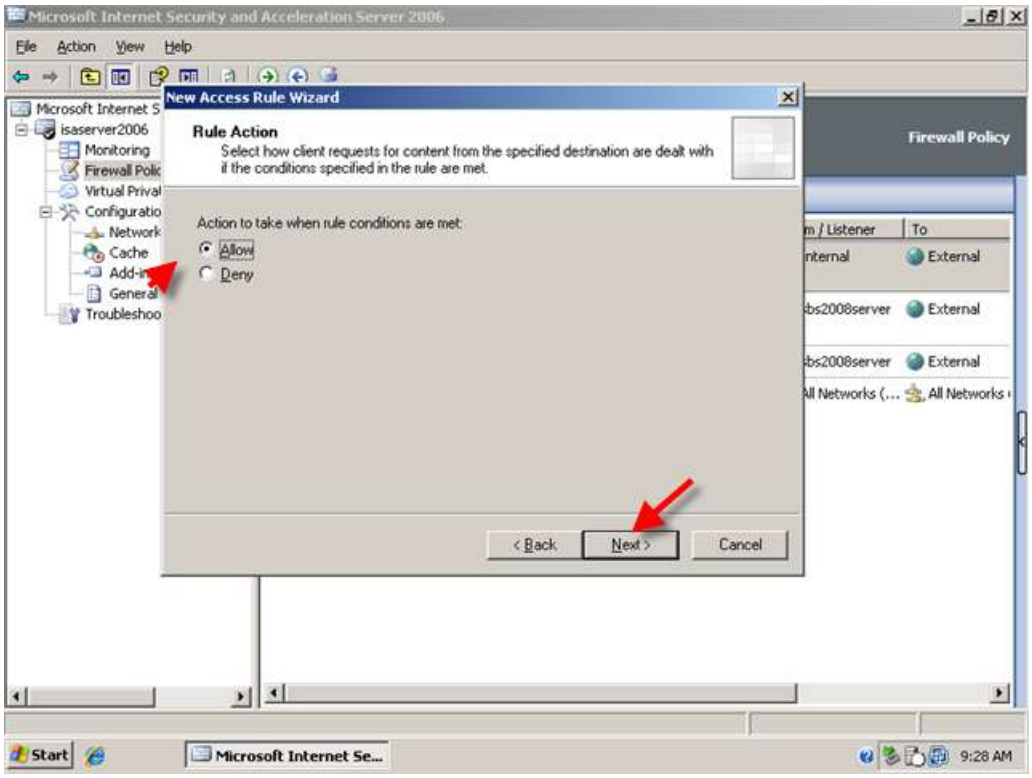
1. From ISA Management, Right click the Firewall Policy and click New > Access Rule.



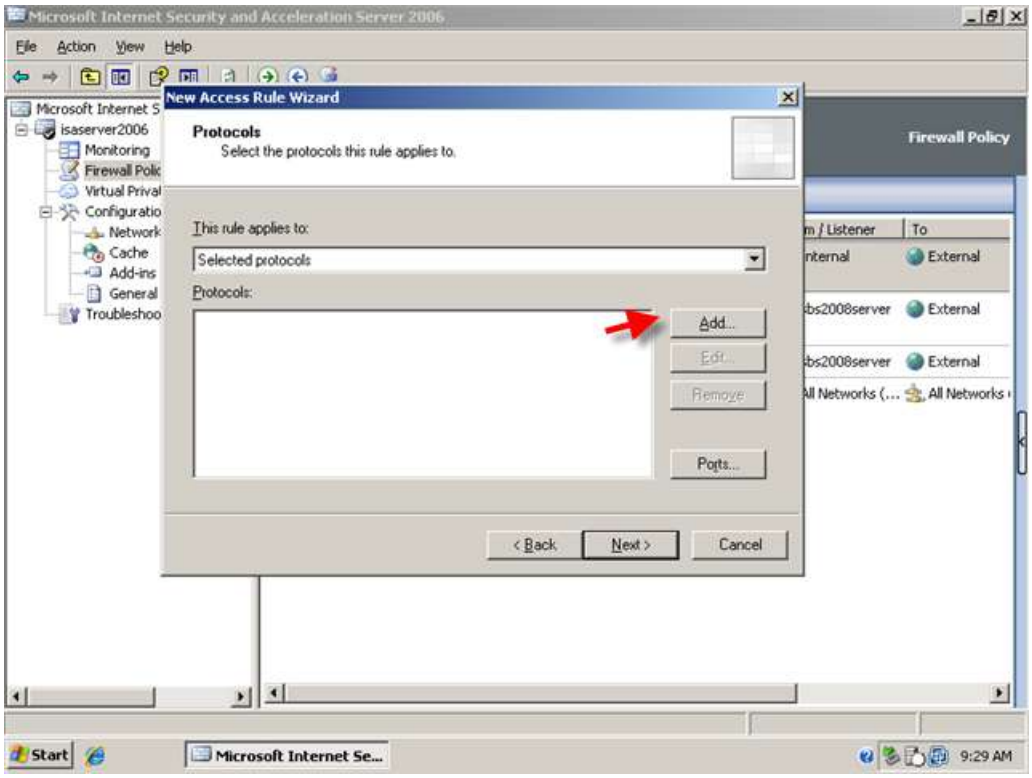
2. In the New Access Rule Wizard, Enter a Name for your Rule. I will call my rule 'SBS FTP Access Rule'.



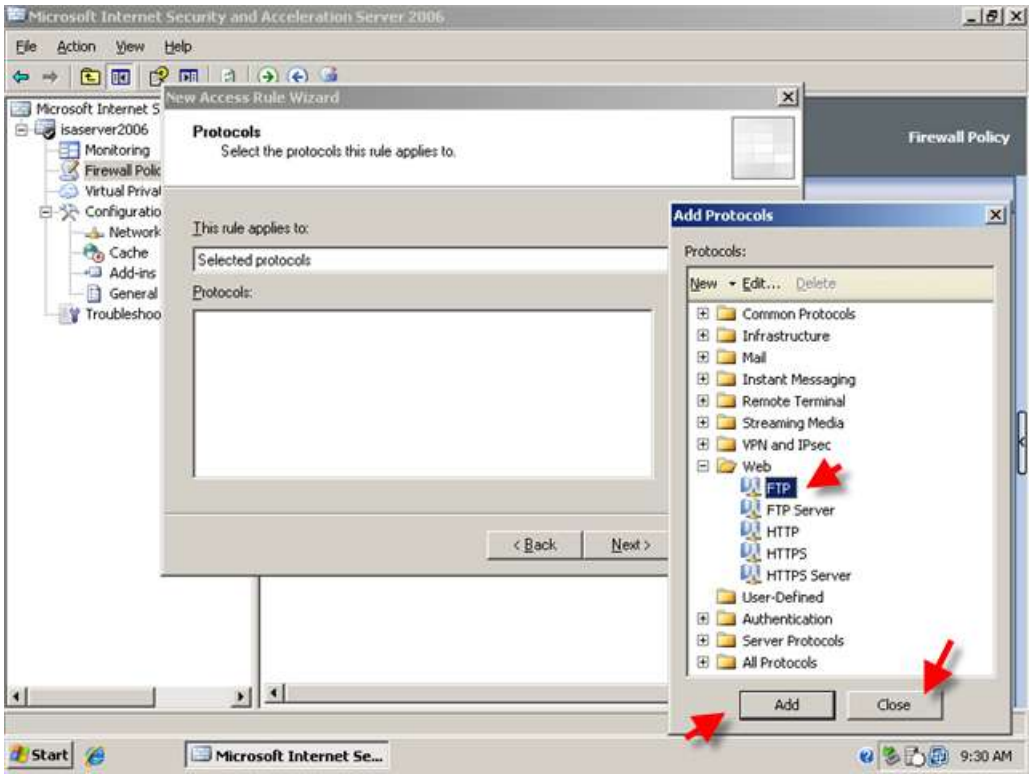
3. Set the Rule to Allow and click Next.



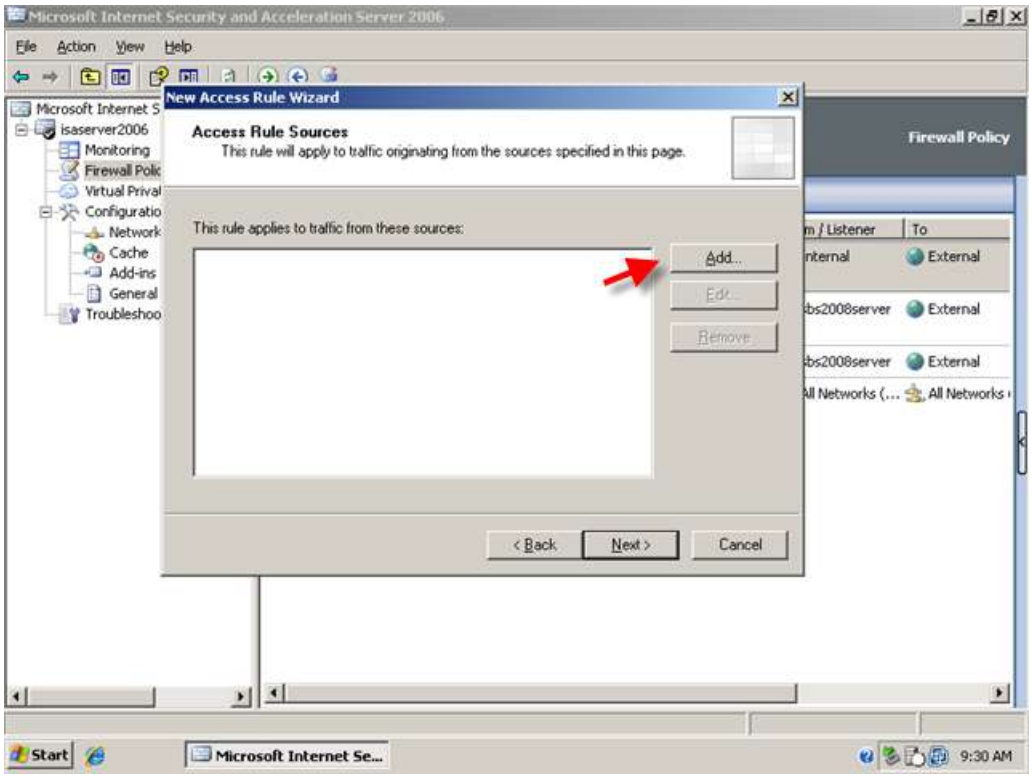
4. On the Protocols page, click Add.



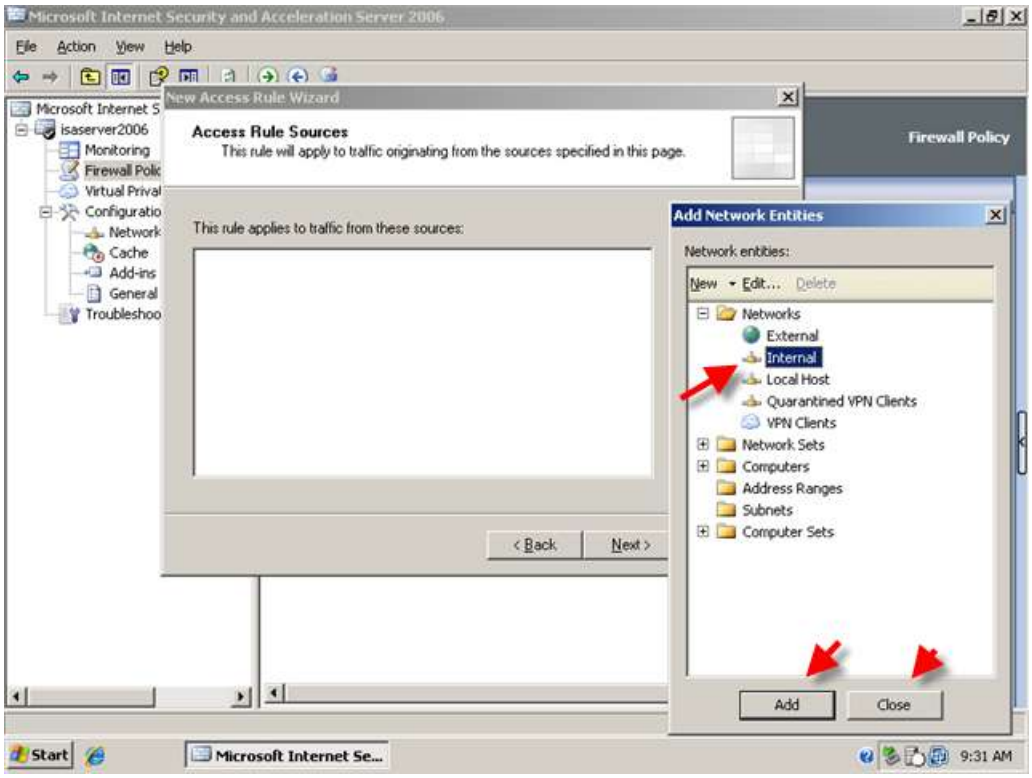
5. Then select FTP. Click Add. Then Click Close. FTP is now displayed in the list, click Next.



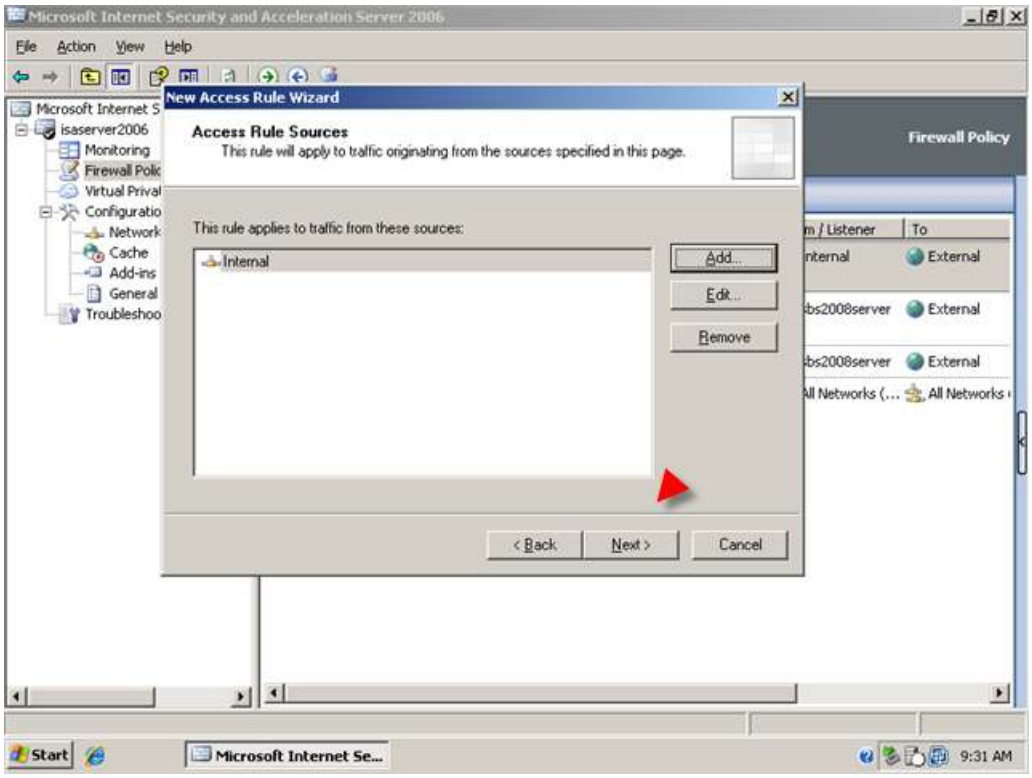
6. On the Access Rule Sources page, click Add.



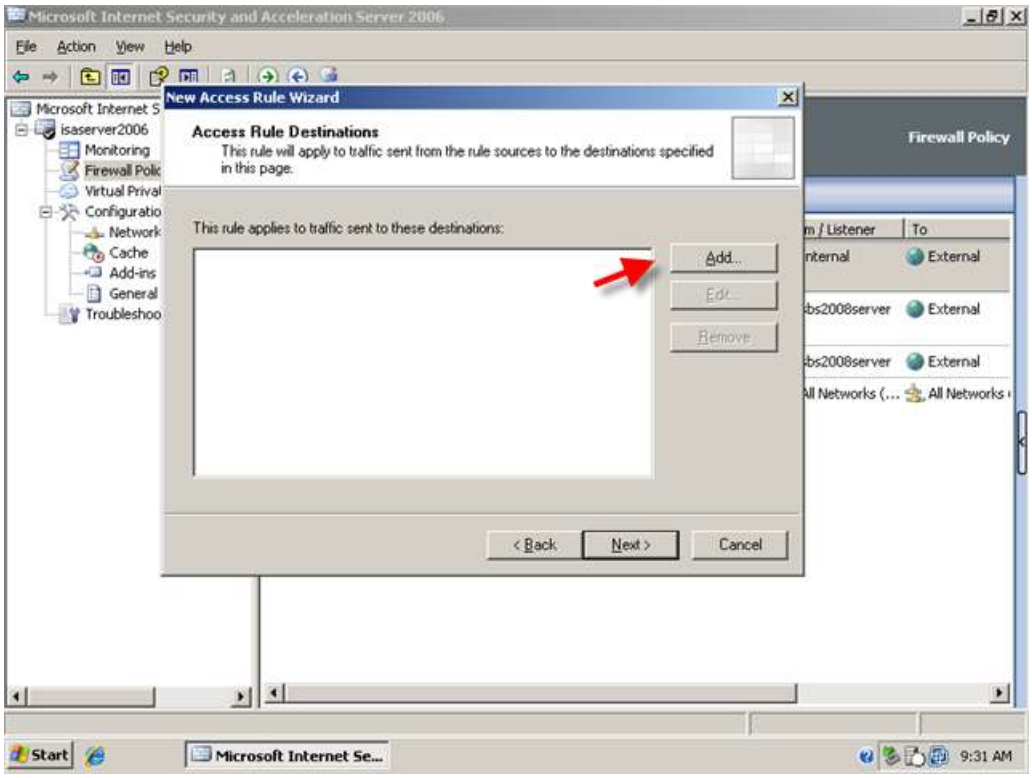
7. Expand Networks. Select the Internal Network. Click Add. Then click Close.



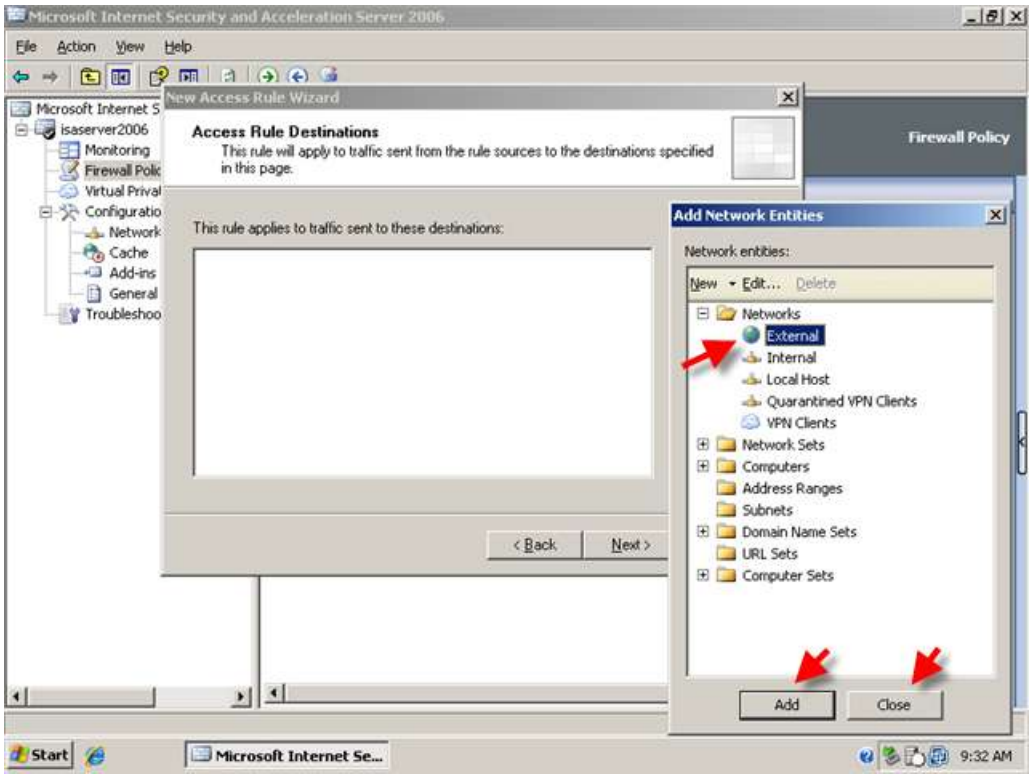
8. The Internal network object is displayed in the list, Click Next.



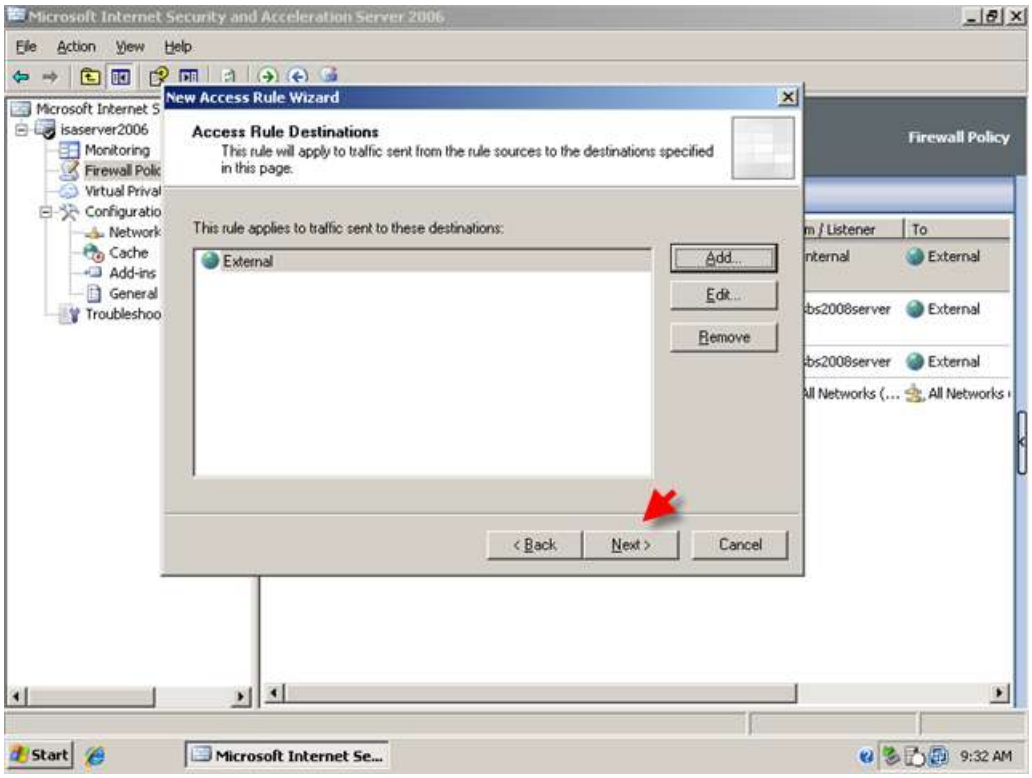
9. On the Access Rule Destinations page, click Add.



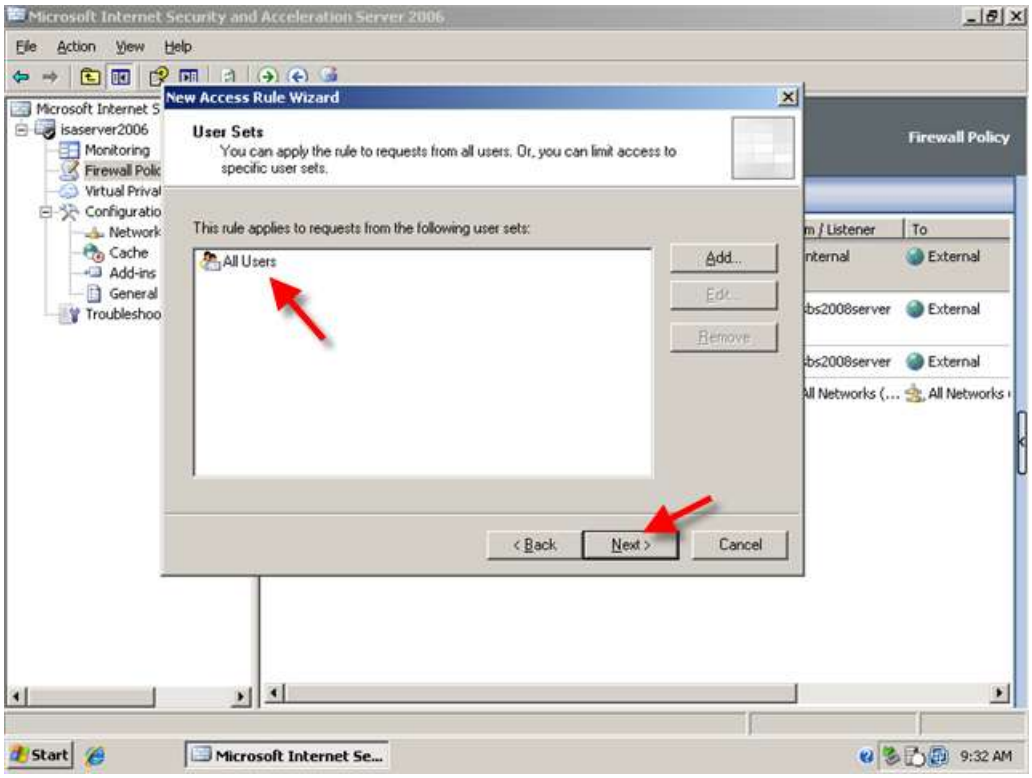
10. Expand Networks, Select the External Network. Click Add. Then click Close.



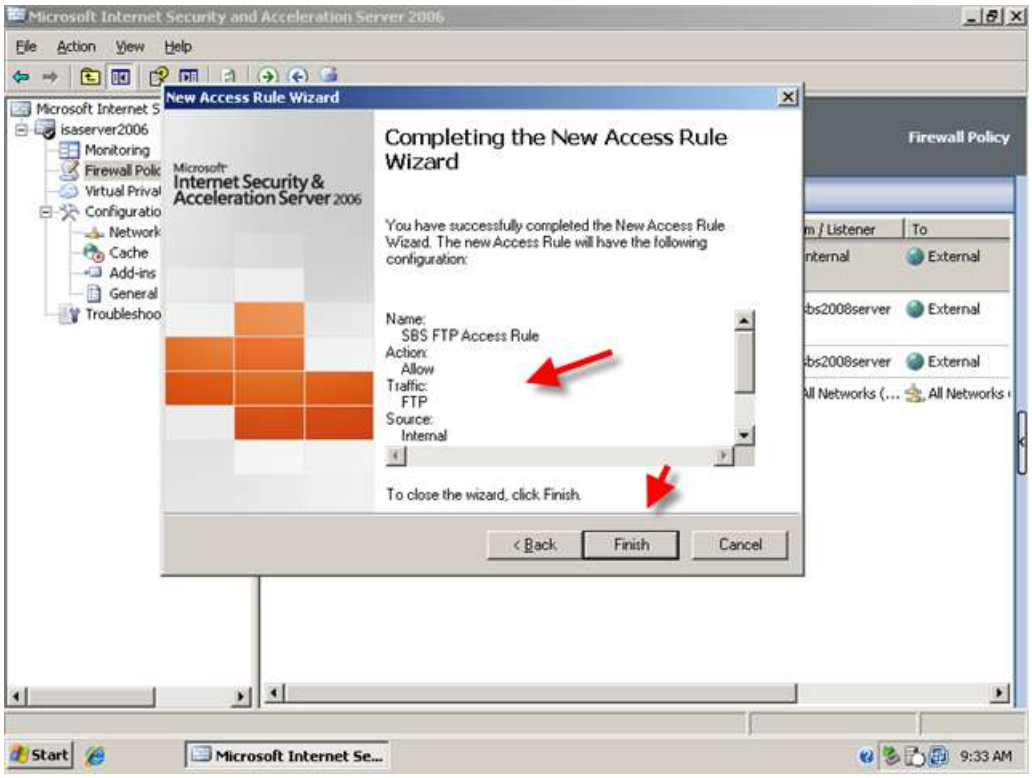
11. The External Network Object is displayed in the list, Click Next.



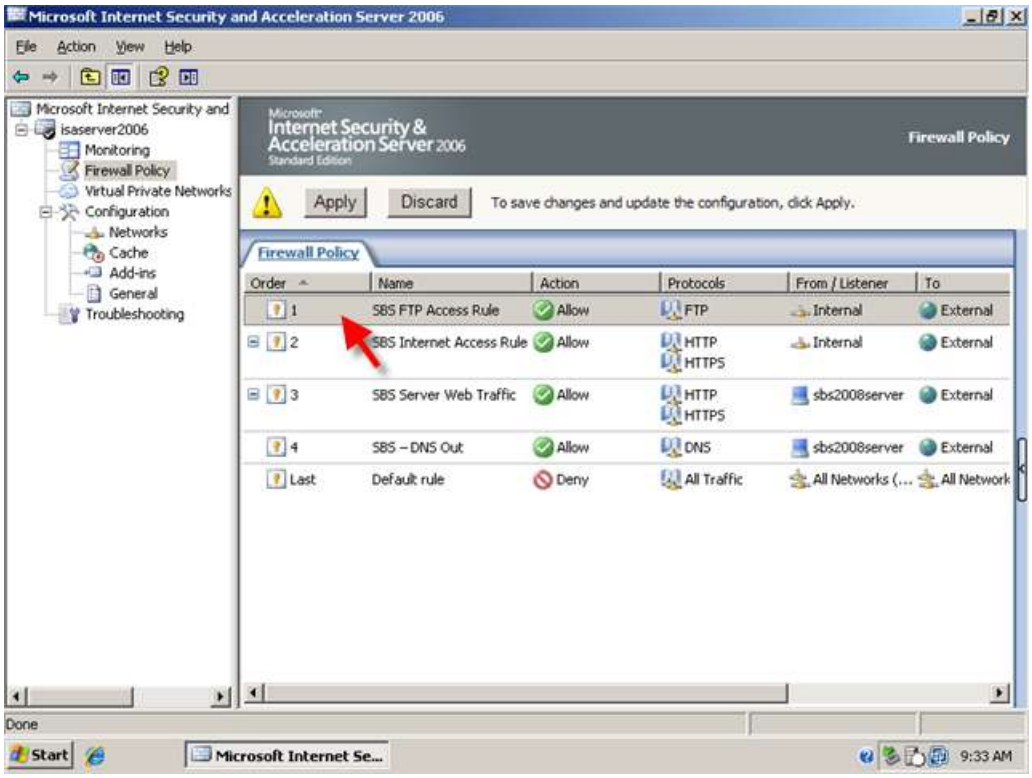
12. On the User Sets page, Leave the default 'All Users' and click Next.



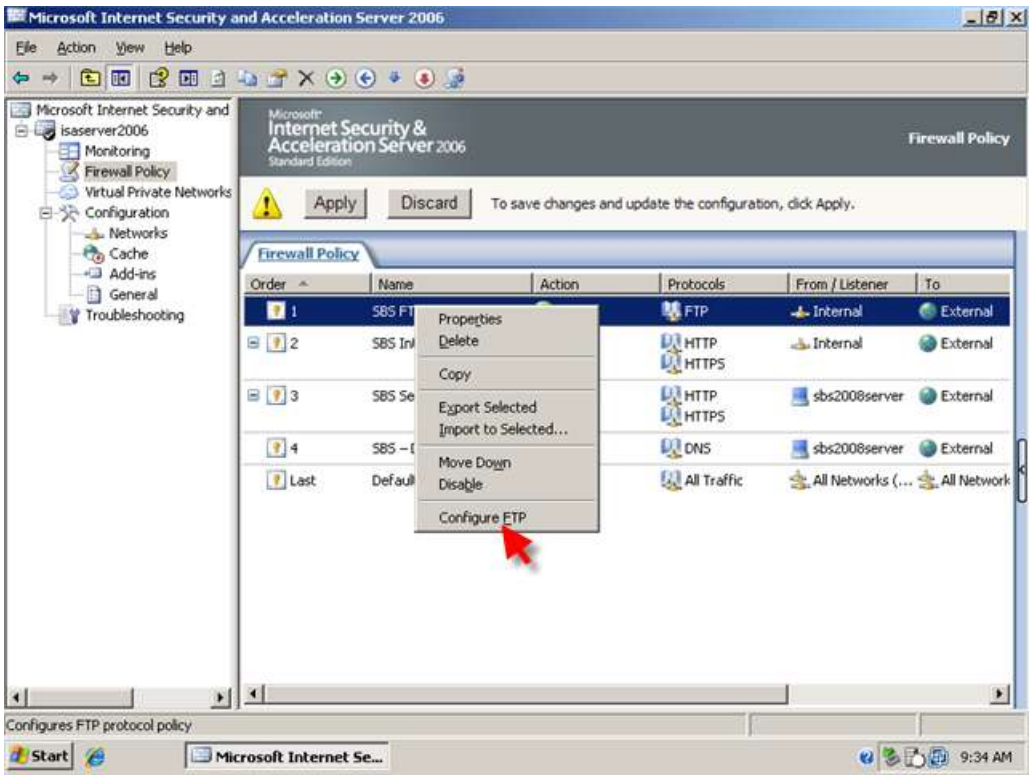
13. On the next page you can review your Access Rule settings, and click Finish to add them to the firewall policy.



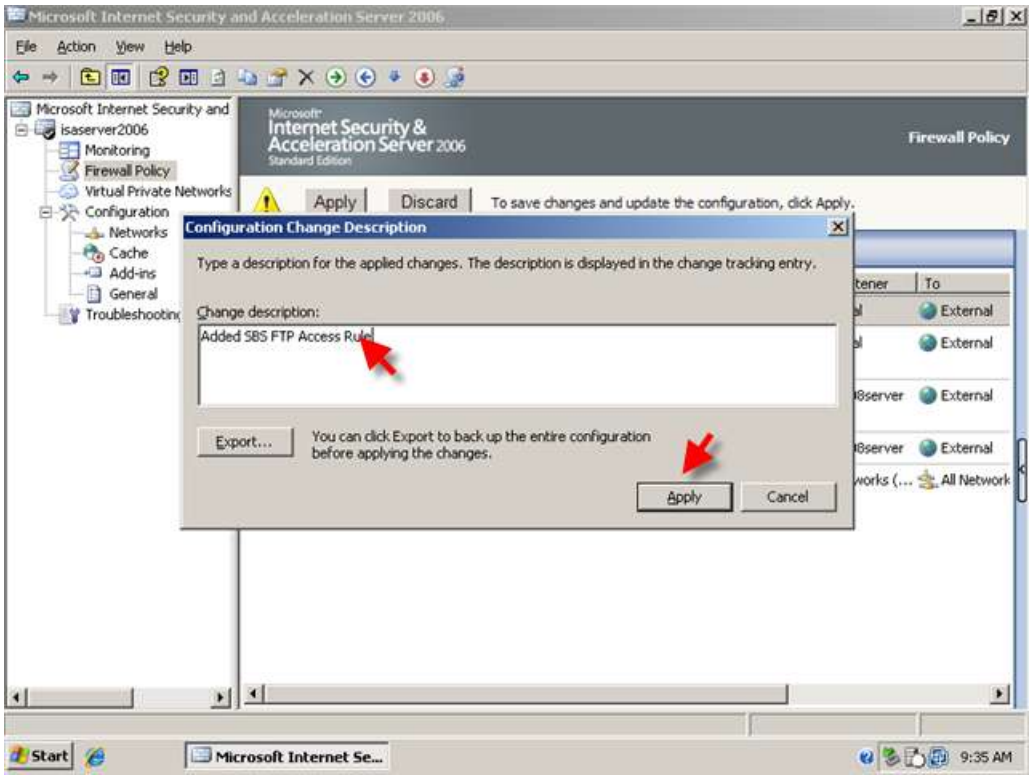
14. Switching to the Firewall Policy view, you can see your rule is added at the top of the list.



15. To allow FTP uploads, right click SBS FTP Access Rule, click 'Configure FTP' on the window that opens un-tick the box for read only FTP and click OK.

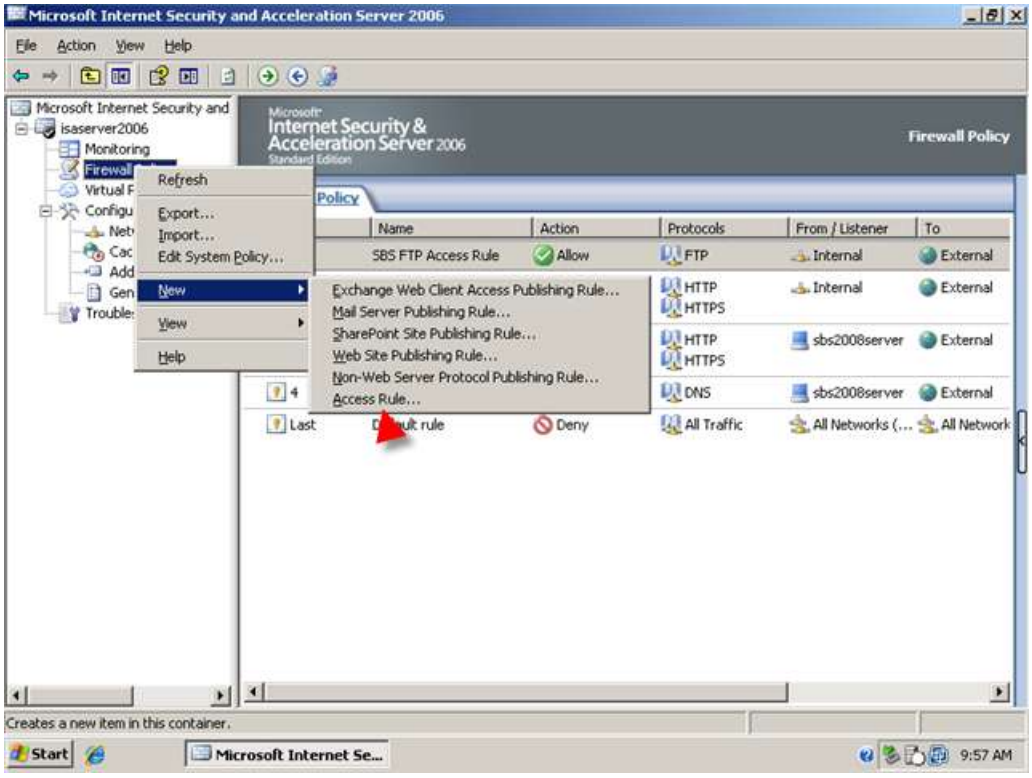


16. Click Apply to save your changes to the Firewall Policy. Enter a comment in the change tracking description box, and click Apply. When the changes are applied, Click OK.

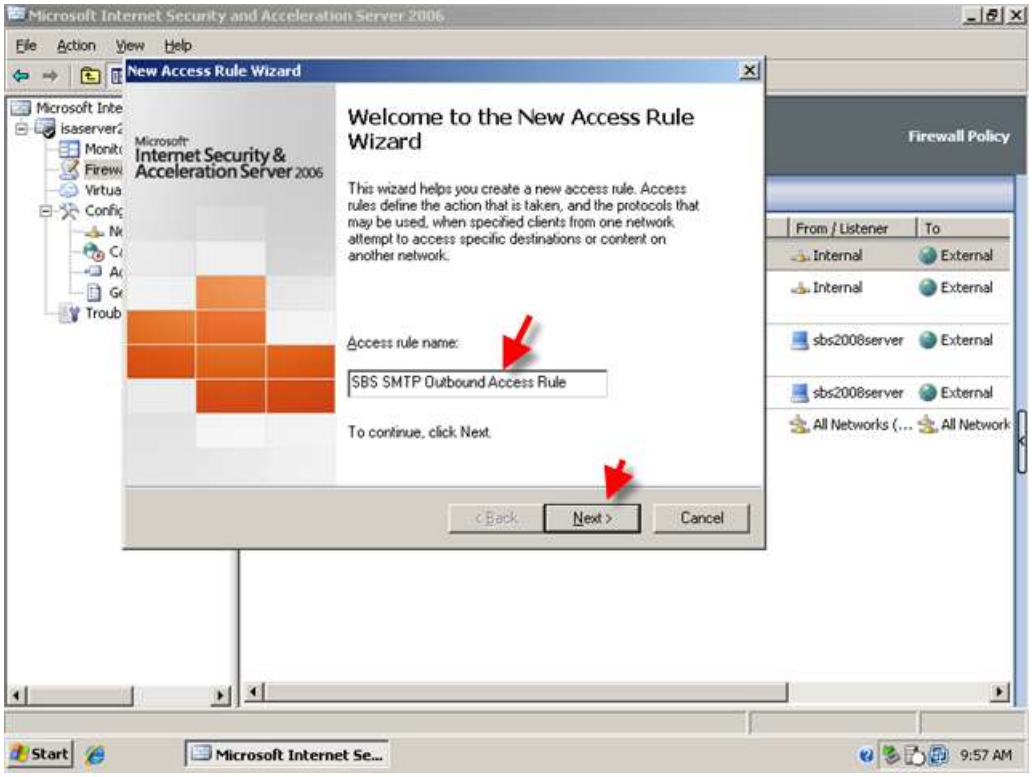


Allowing Sending SMTP Email & Publishing SMTP Server

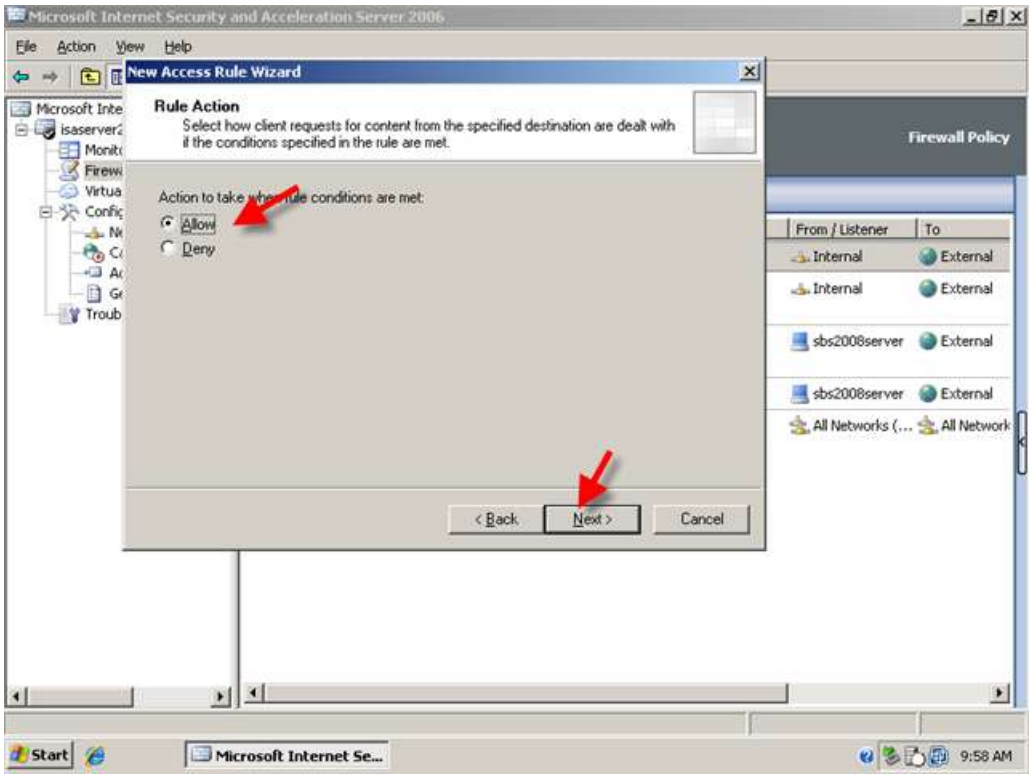
1. Right click the Firewall Policy and click New > Access Rule



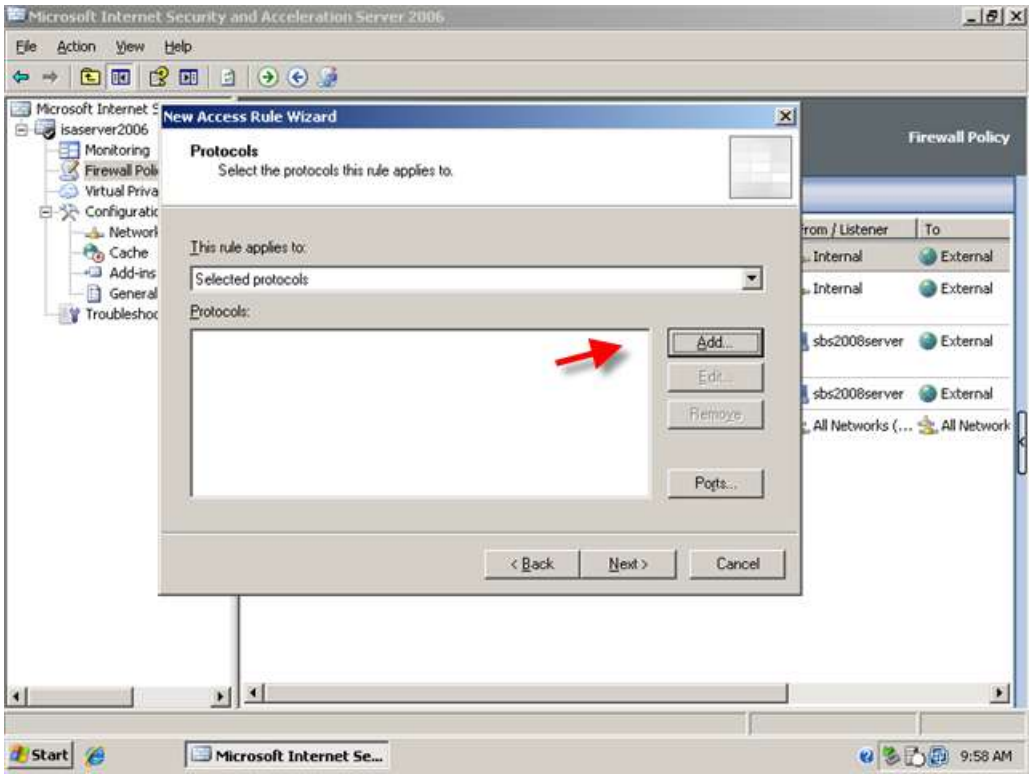
2. Name the rule SBS SMTP Outbound Access Rule, click Next.

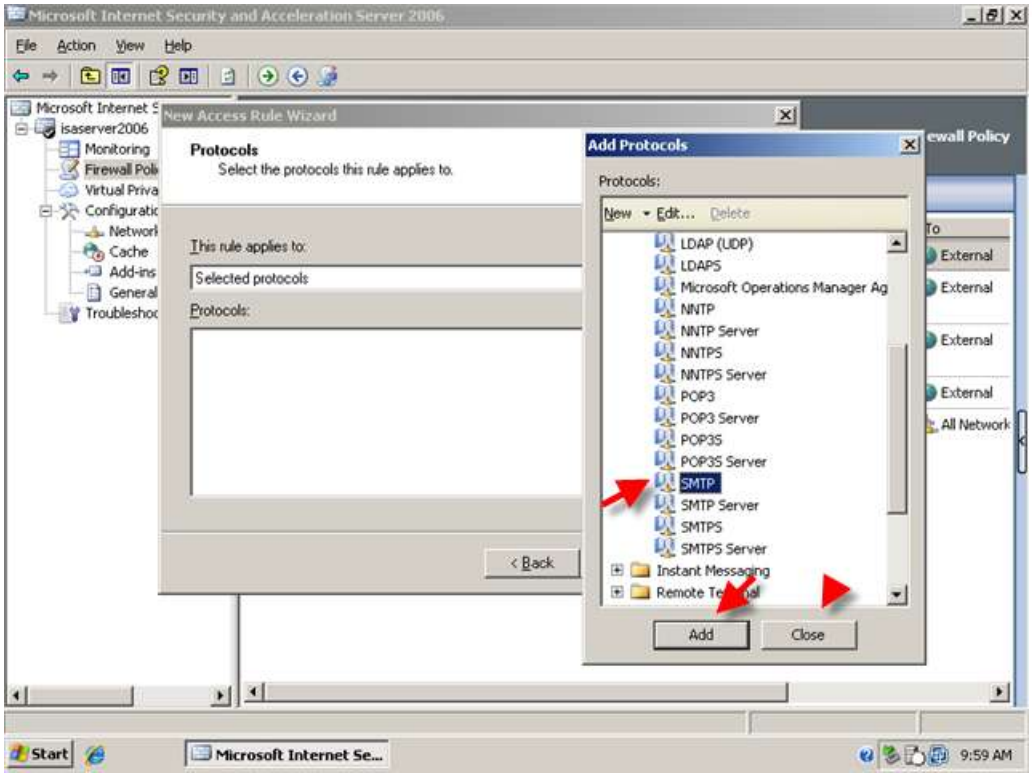


3. Set the rule to 'allow'

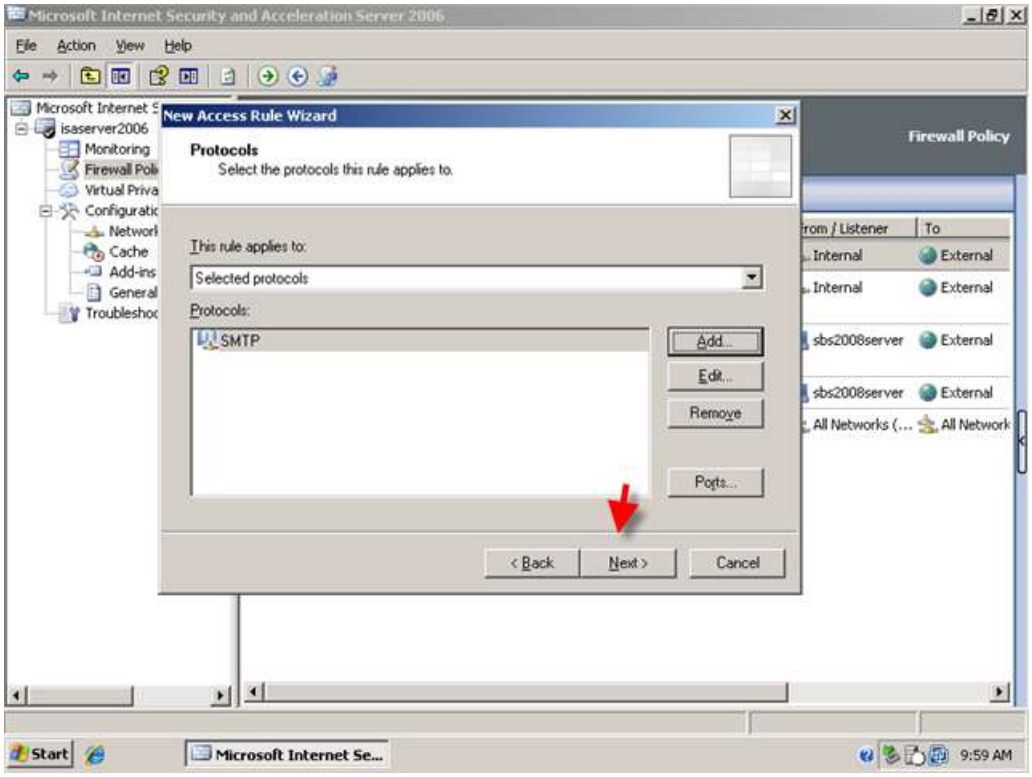


4. On the protocols page, click add, expand Mail, scroll down and select SMTP, click Add, then click Close.

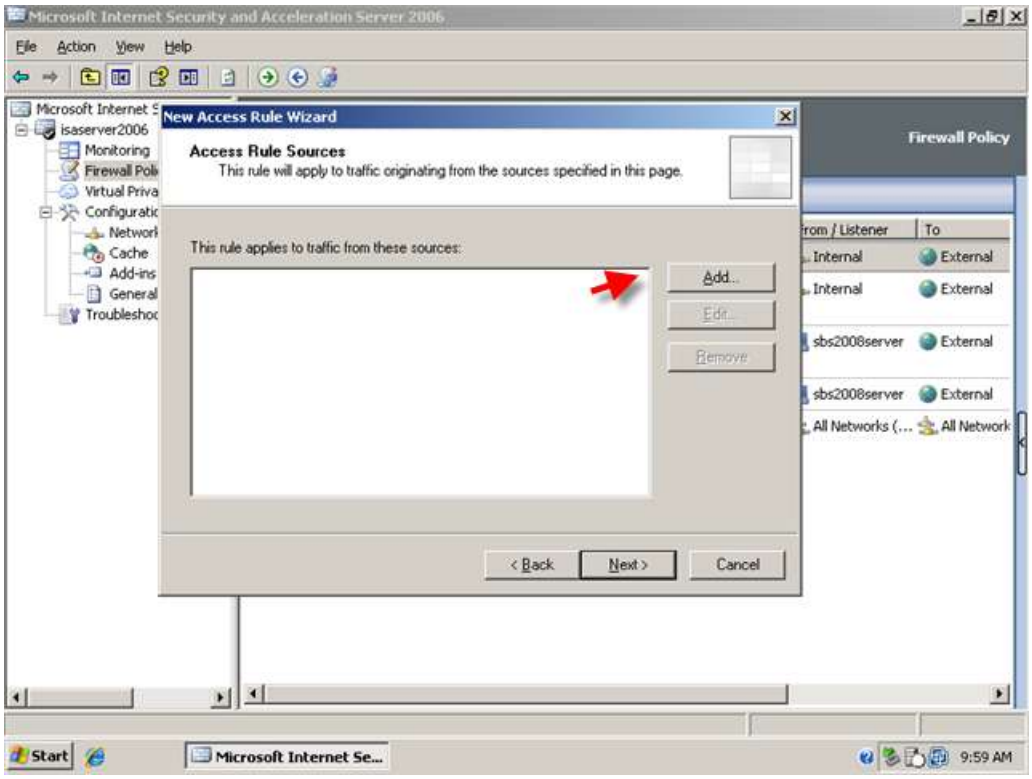


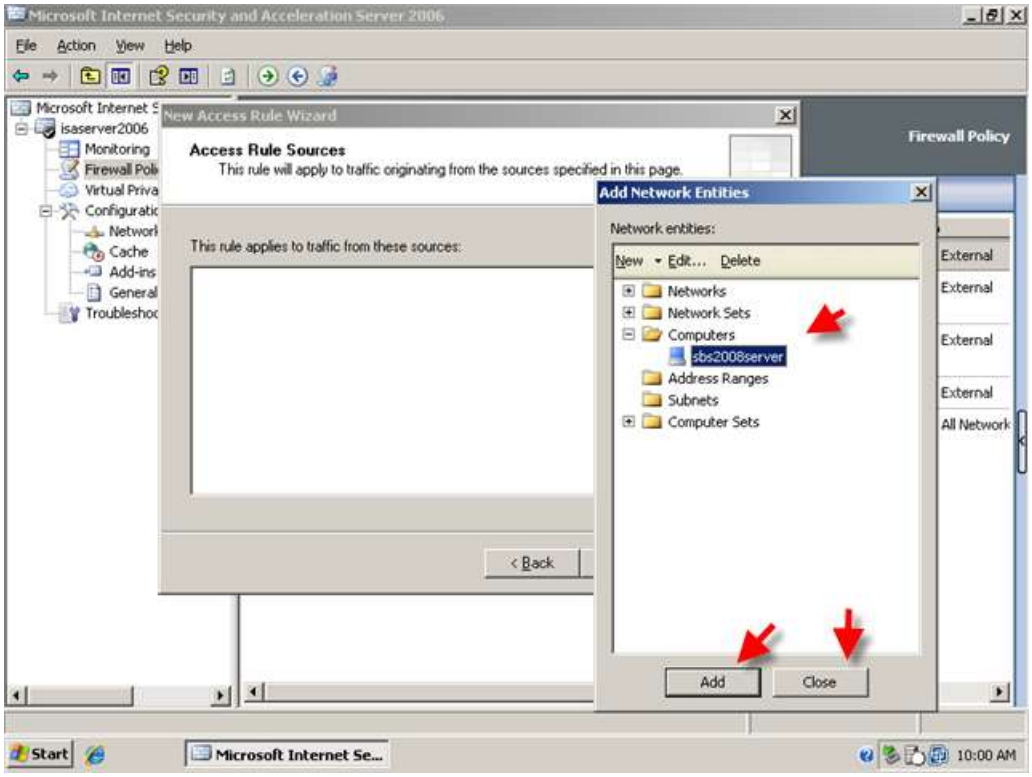


5. SMTP is now displayed in the list. Click Next.

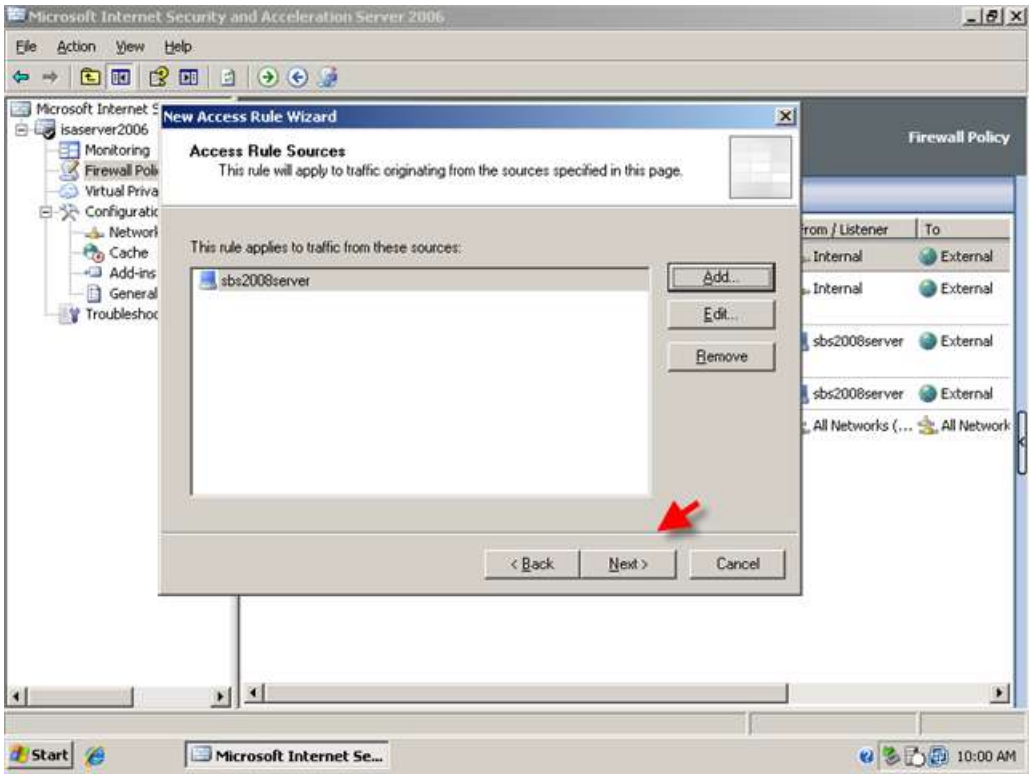


6. On the Source networks page Click Add, expand Computers, select the sbs2008server object, and click Add. Click Close.

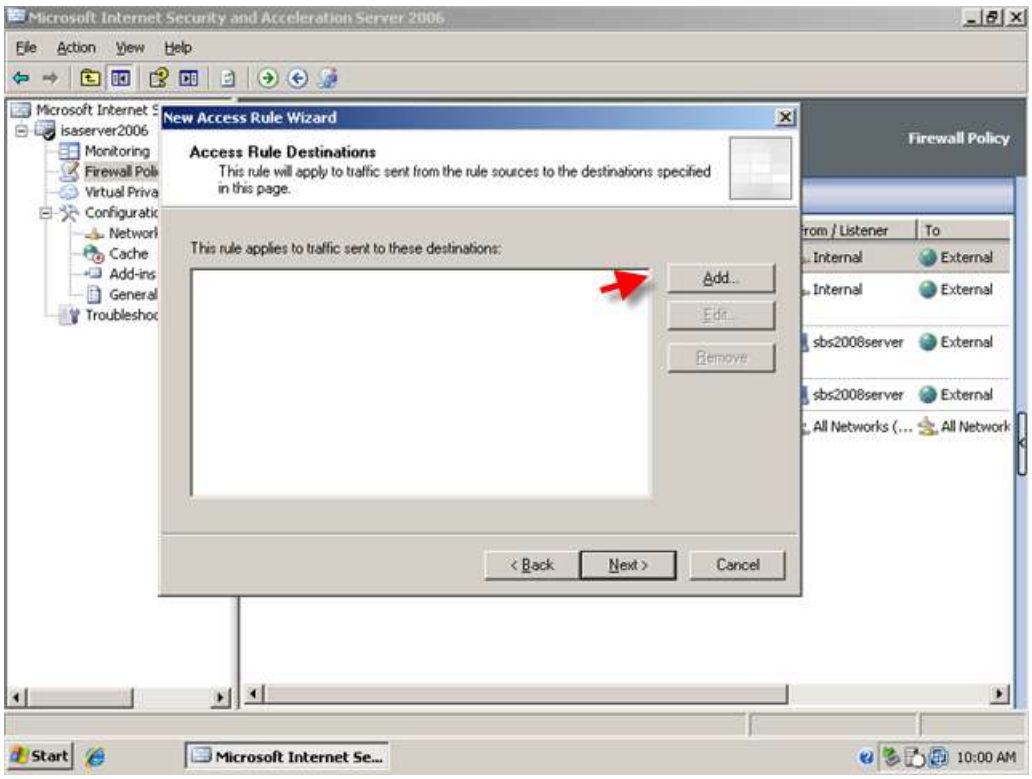


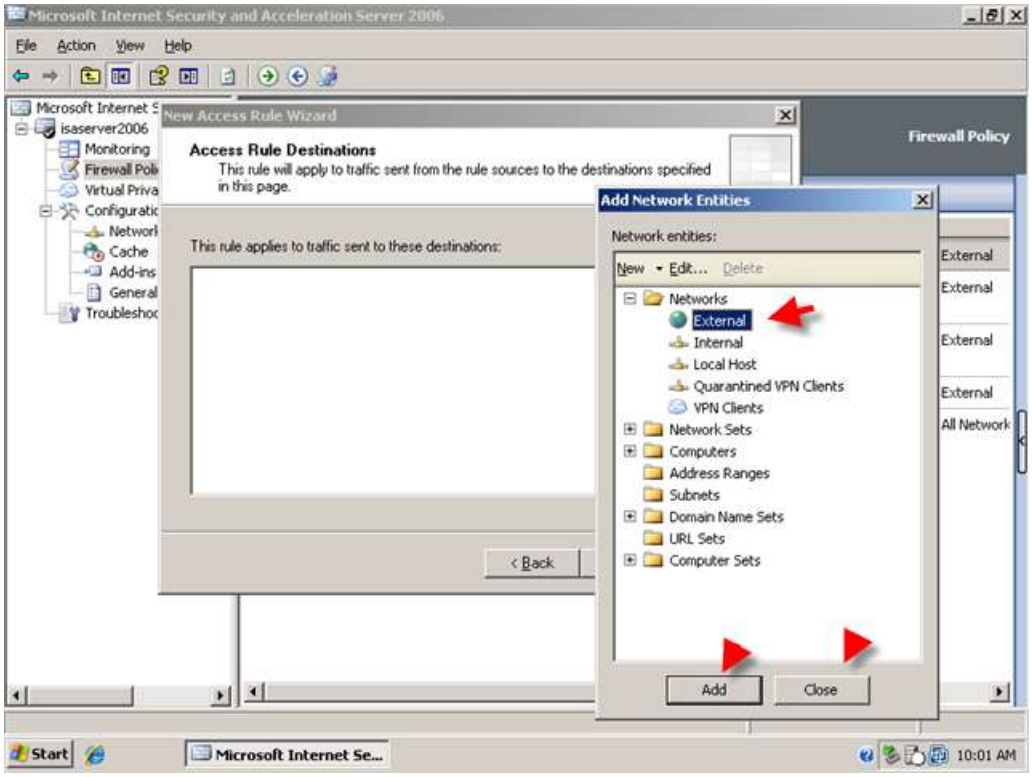


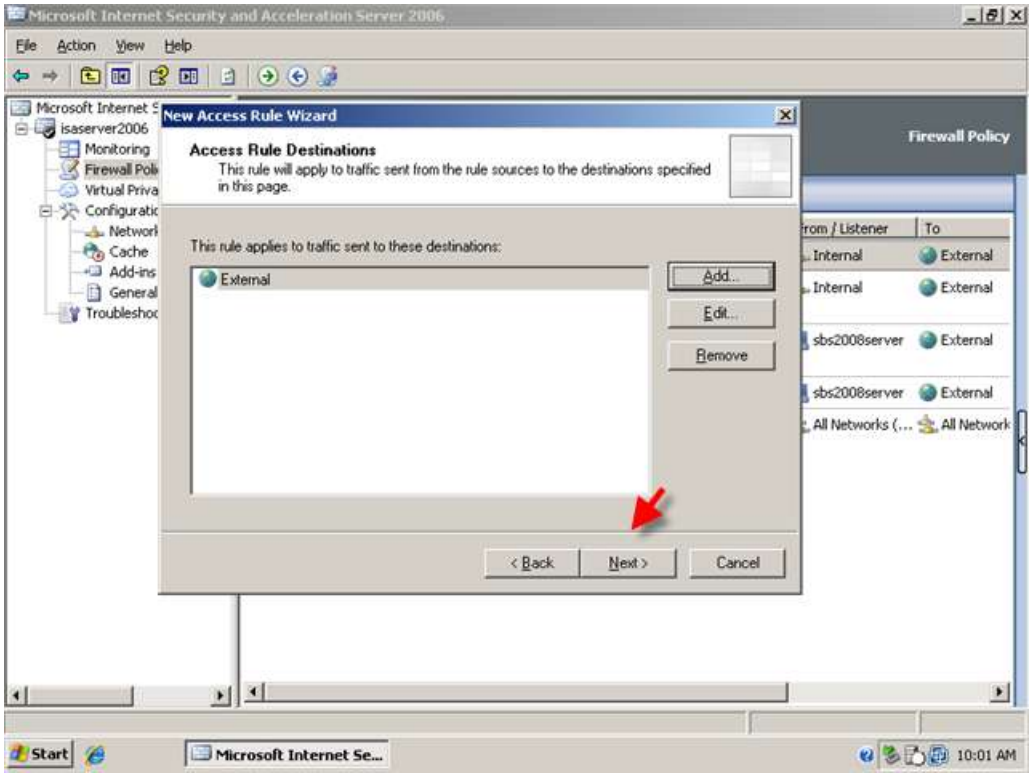
7. Sbs2008server is now displayed in the list, click Next.



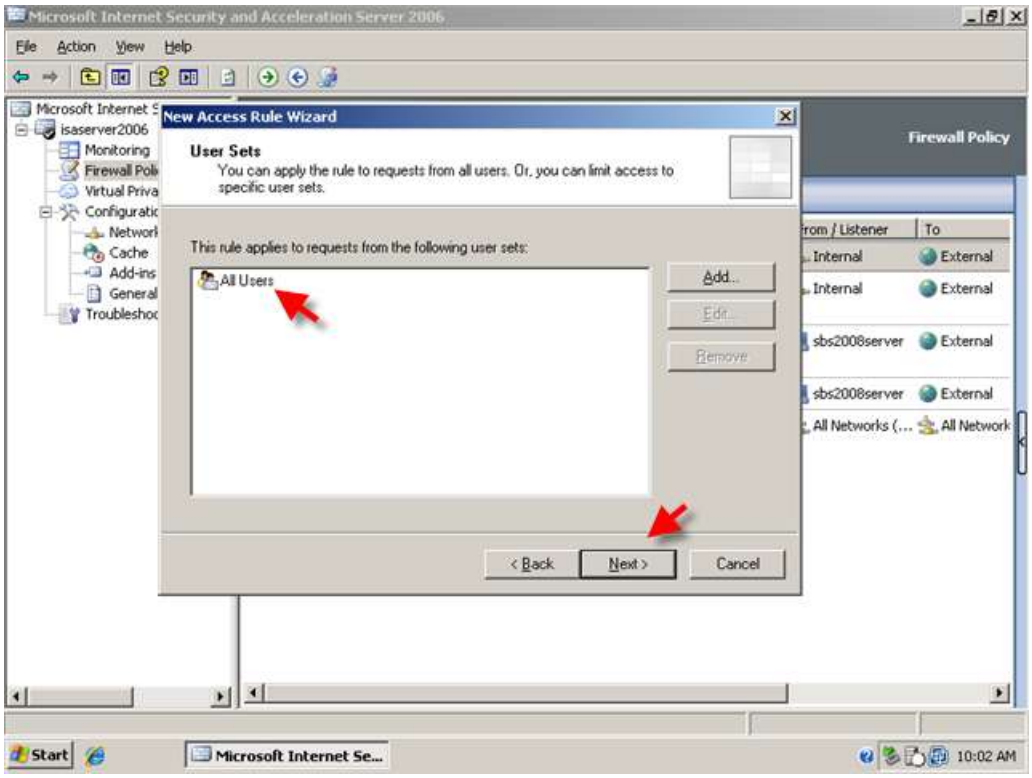
8. On the destinations page click Add, expand networks and click External. Click Add, then click Close. The external network object is now displayed in the list. Click Next.



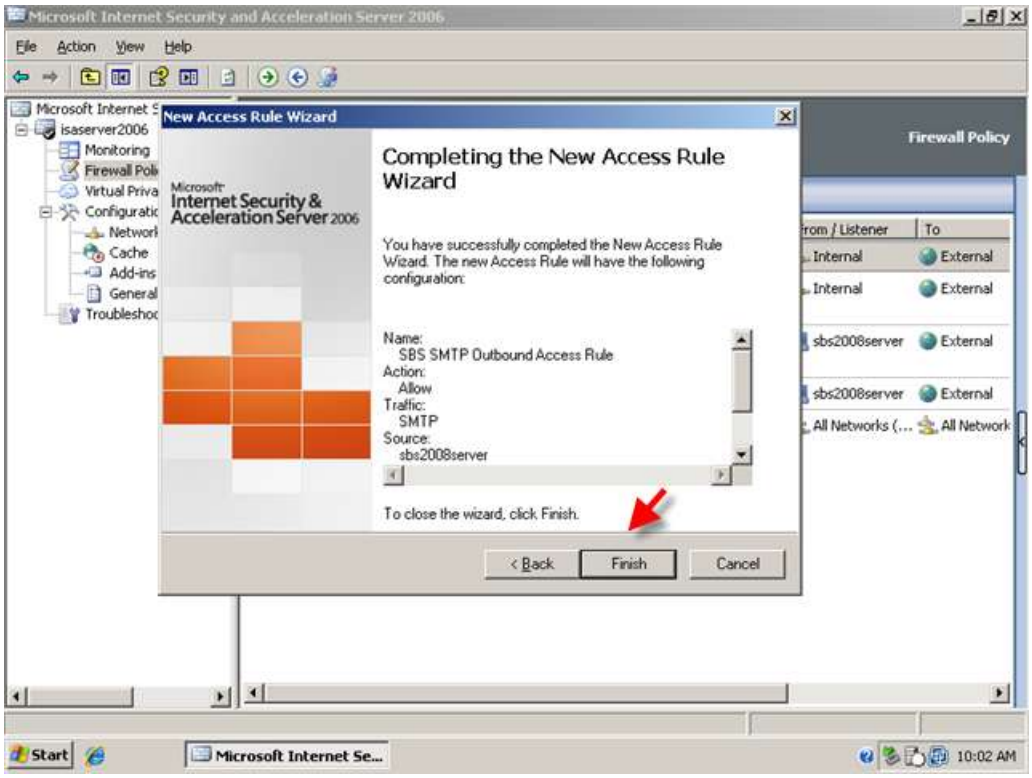

Microsoft Internet Security and Acceleration Server 2006
File Action View Help
New Access Rule Wizard
Access Rule Destinations
This rule will apply to traffic sent from the rule sources to the destinations specified in this page.
This rule applies to traffic sent to these destinations:
< Back
Add Network Entities
Network entities:
New Edit... Delete
Networks
External
Internal
Local Host
Quarantined VPN Clients
VPN Clients
Network Sets
Computers
Address Ranges
Subnets
Domain Name Sets
URL Sets
Computer Sets
Add
Close
Firewall Policy
Start
Microsoft Internet Se...
10:01 AM


Microsoft Internet Security and Acceleration Server 2006
File Action View Help
New Access Rule Wizard
Access Rule Destinations
This rule will apply to traffic sent from the rule sources to the destinations specified in this page.
This rule applies to traffic sent to these destinations:
External
Add...
Edit...
Remove
< Back
Next >
Cancel
Firewall Policy
Start
Microsoft Internet Se...
10:01 AM

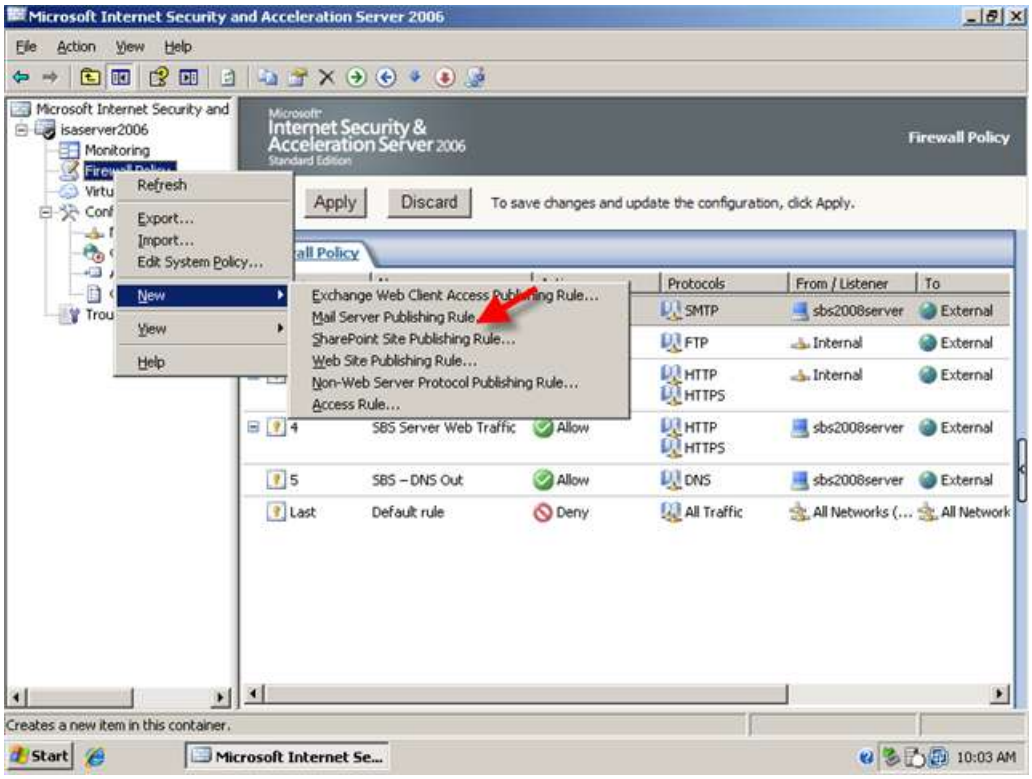
9. Accept the default 'All Users' on the user sets page, and click Next.



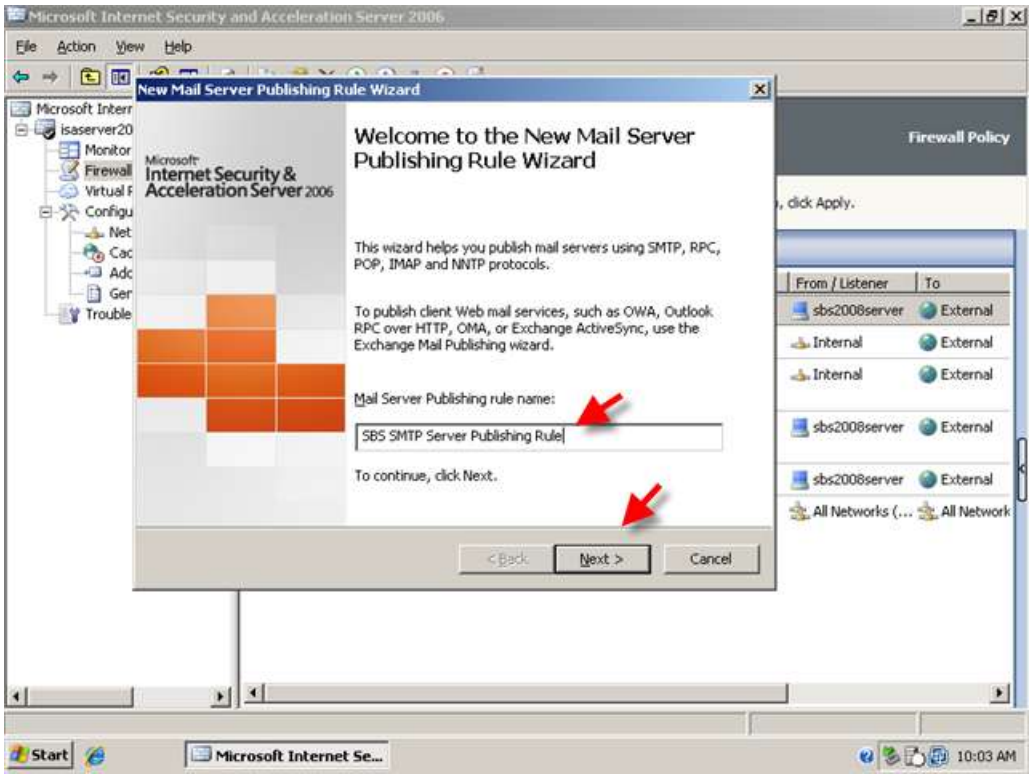
10. Review your rule settings and click Finish.



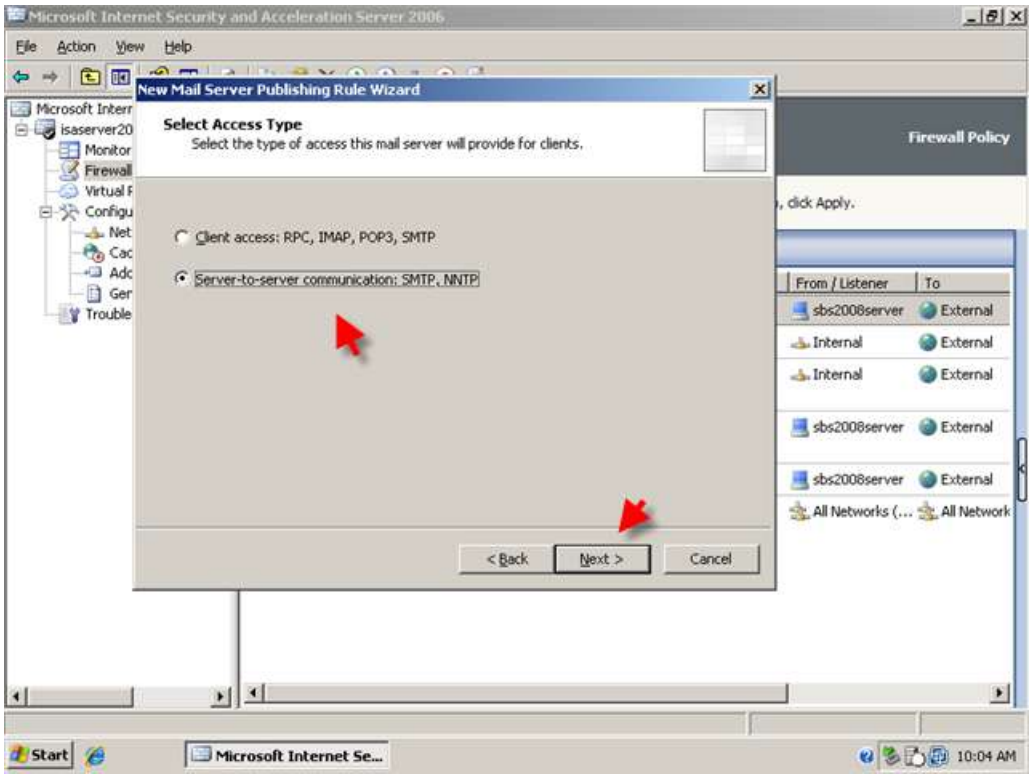
11. To allow your SBS Server to receive incoming email we need to create a Mail Server publishing rule. Right click the Firewall Policy and click New > Mail server publishing rule.



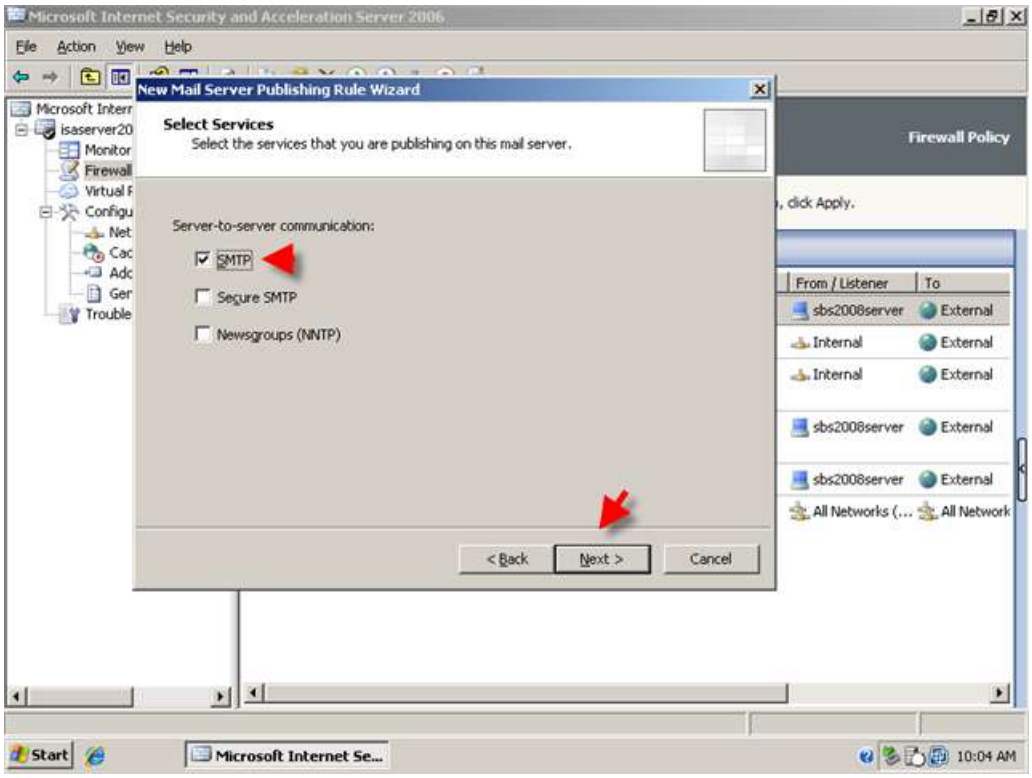
12. Name the rule SBS SMTP Server Publishing Rule and click Next.



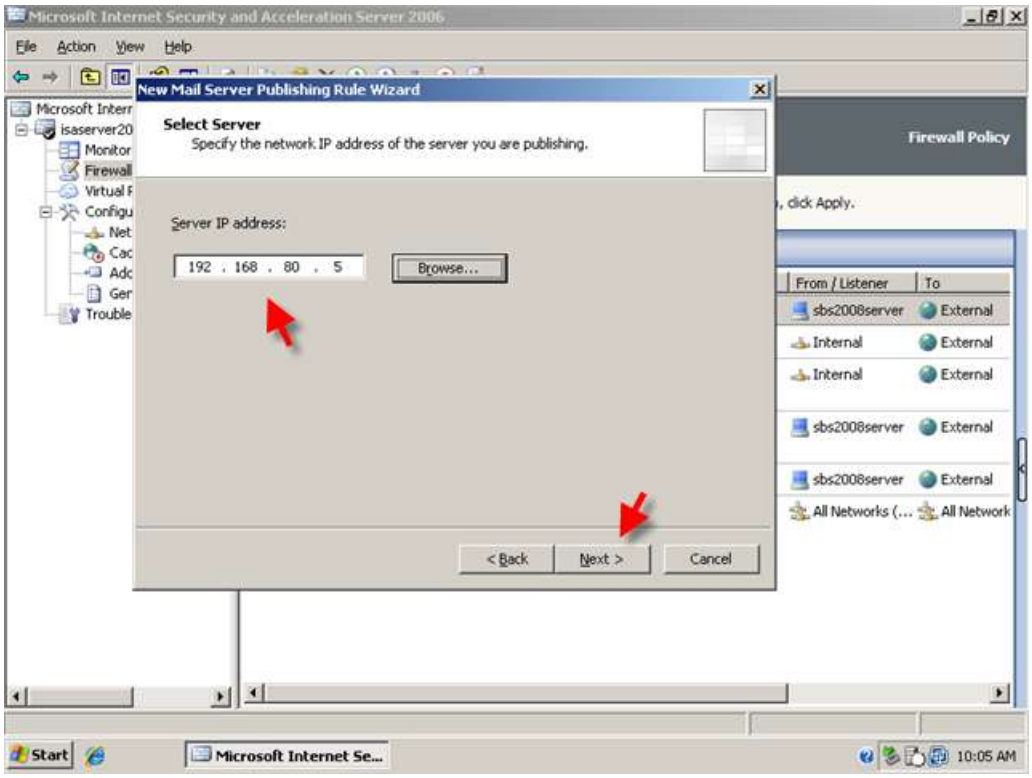
13. Choose server to server communication SMTP; NNTP and click Next.



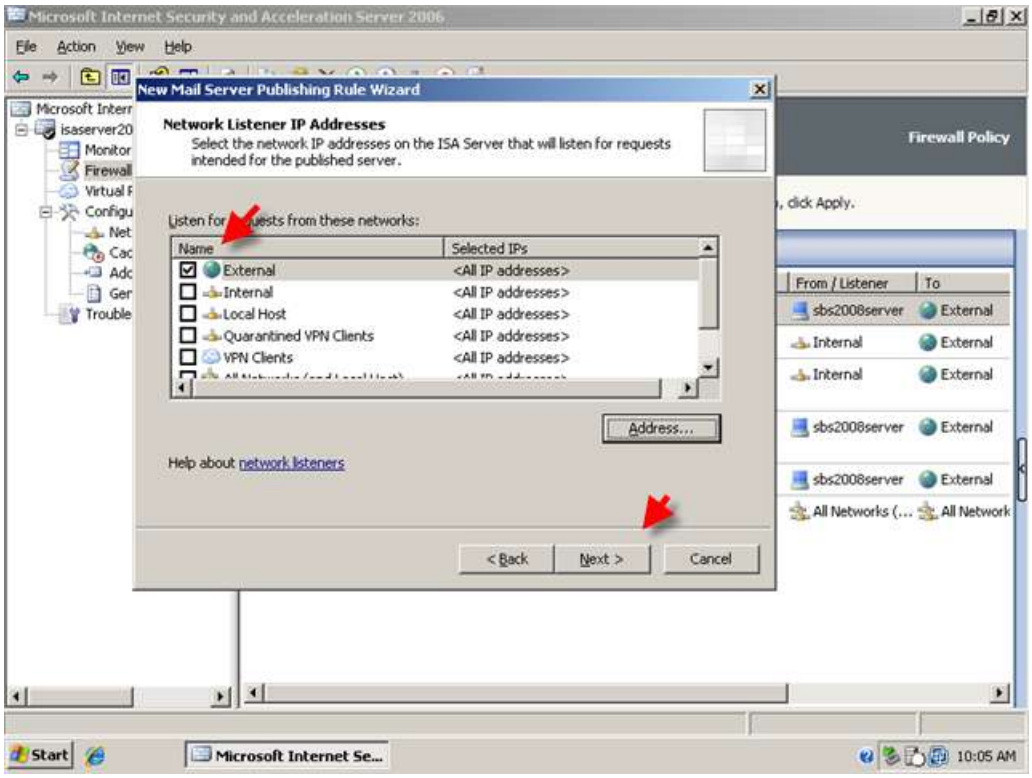
14. Tick the box for SMTP and click Next.



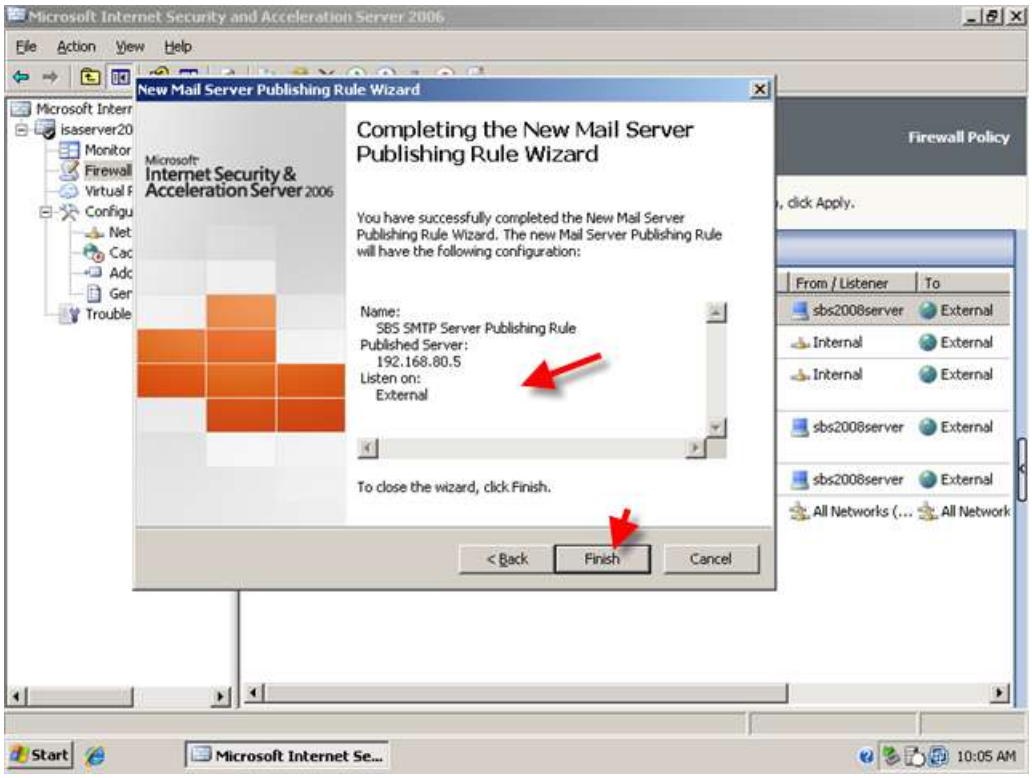
15. Enter the ip address of our SBS Server – 192.168.80.5 and click Next.



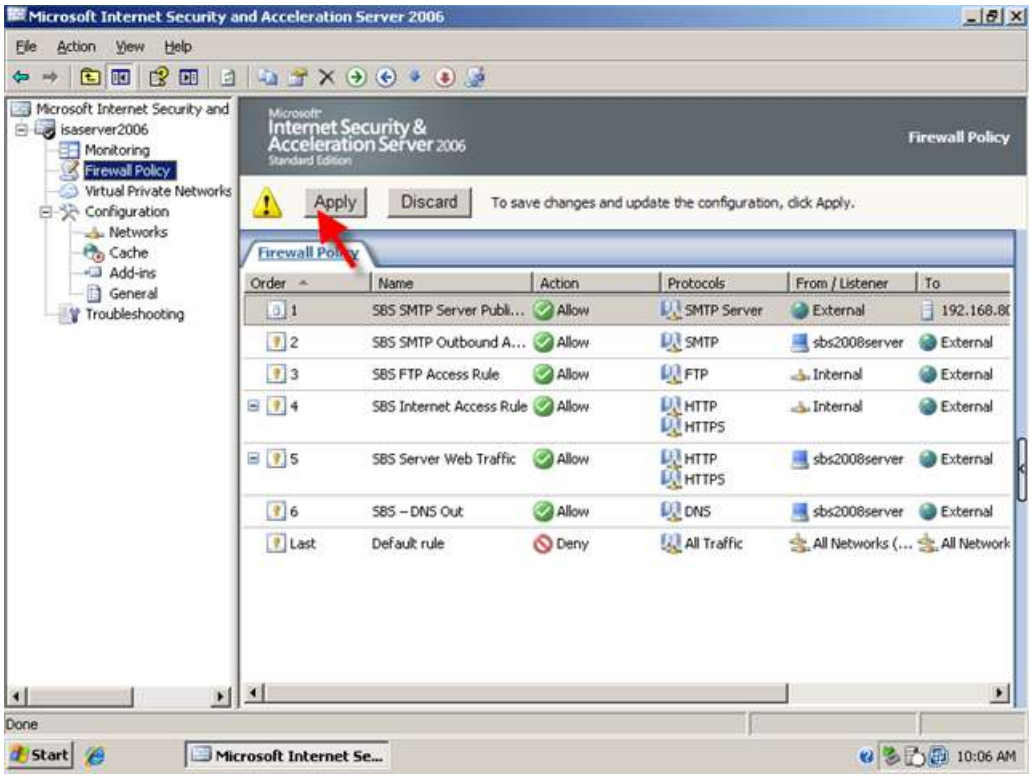
16. Put a tick in the box for External Network and click Next.

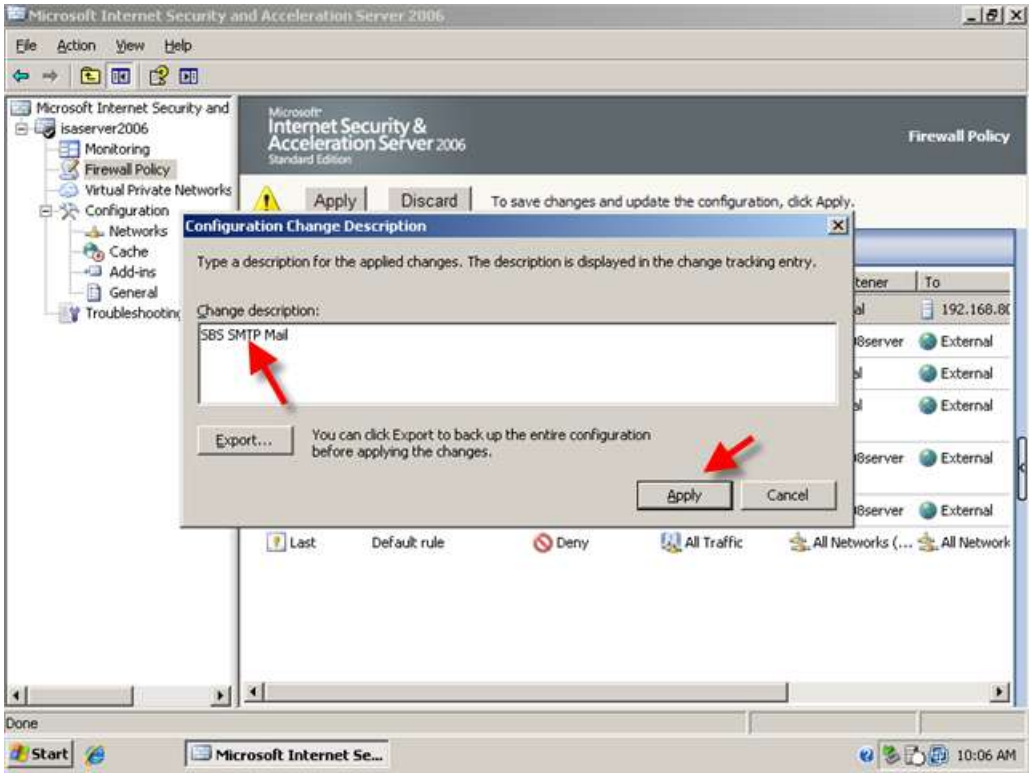


17. Review your rule settings and click Finish.



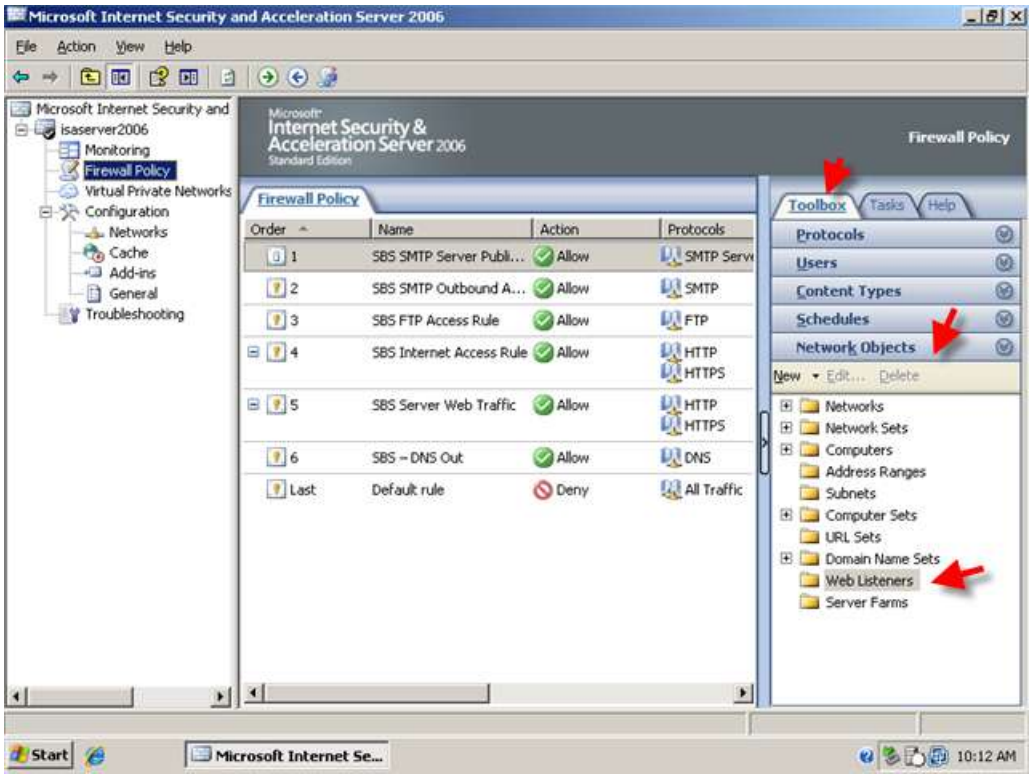
18. You can now apply the changes to save your firewall policy.



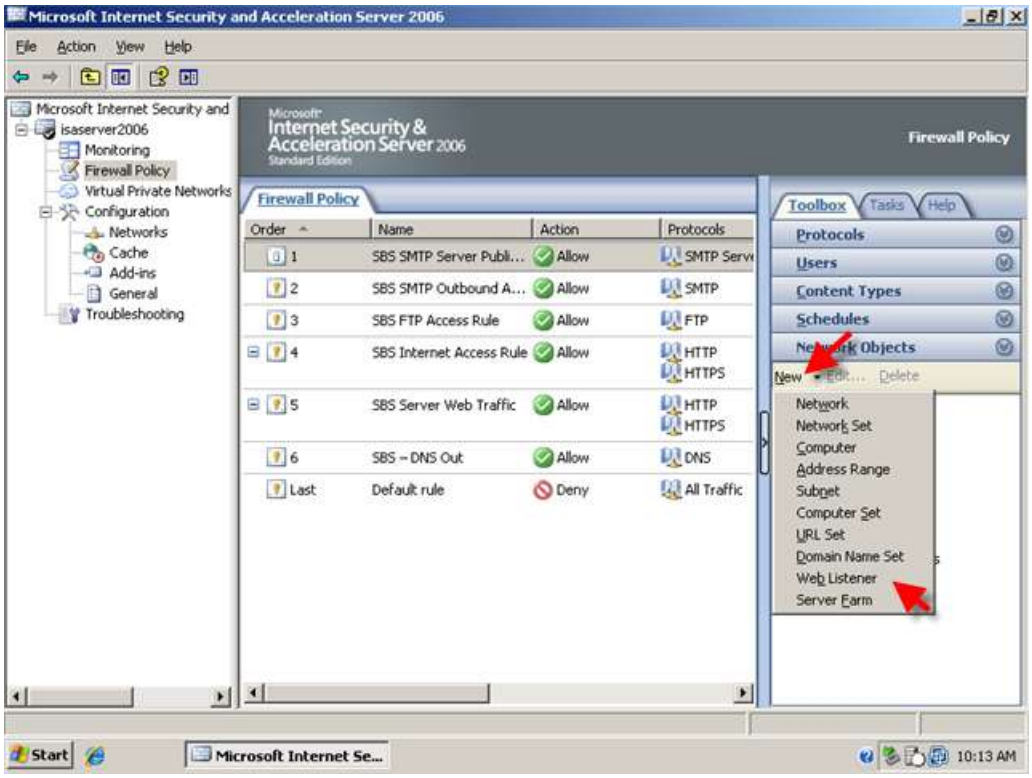

Microsoft Internet Security and Acceleration Server 2006
File Action View Help
Microsoft Internet Security and
isaserver2006
Monitoring
Firewall Policy
Virtual Private Networks
Configuration
Networks
Cache
Add-ins
General
Troubleshooting
Internet Security & Acceleration Server 2006
Standard Edition
Firewall Policy
Apply
Discard
To save changes and update the configuration, click Apply.
Configuration Change Description
Type a description for the applied changes. The description is displayed in the change tracking entry.
Change description:
SBS SMTP Mail
Export...
You can click Export to back up the entire configuration before applying the changes.
Apply
Cancel
Last
Default rule
Deny
All Traffic
All Networks (...
All Network
External
Done
Start
Microsoft Internet Se...
10:06 AM

Creating a Web Listener for Web Publishing

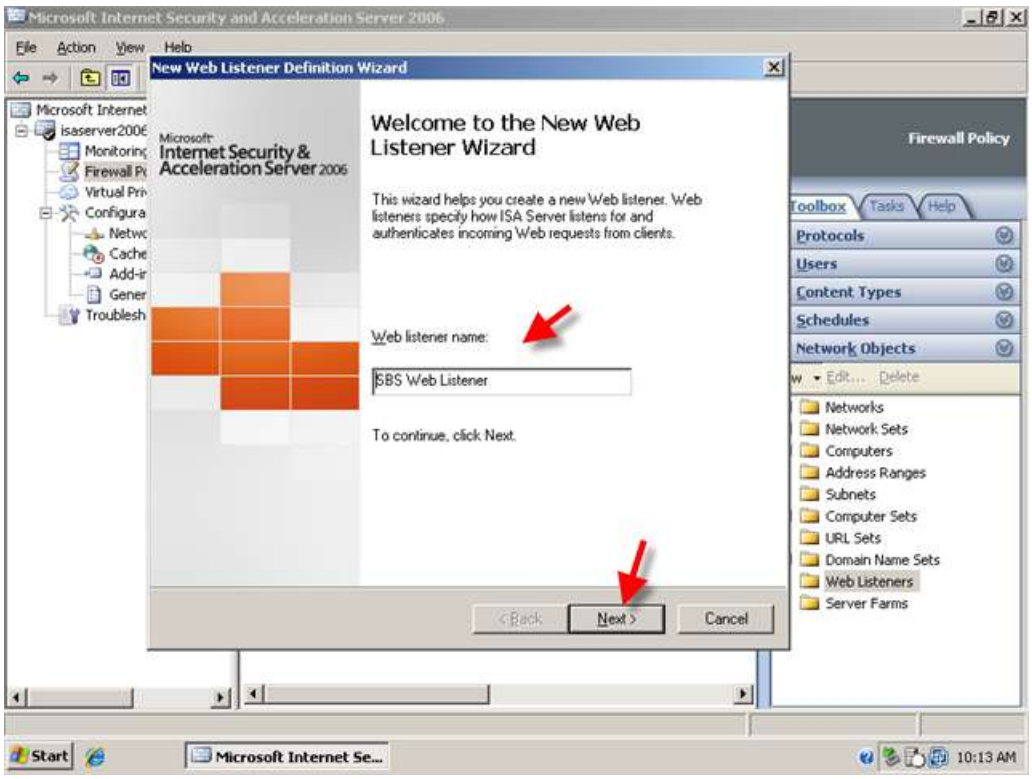
1. On the ISA Server we must create a new Web Listener – this will allow the ISA server to listen for requests from the internet. Open up ISA Server Management. In the far right hand column click on 'Toolbox' then click on 'Network Objects'.



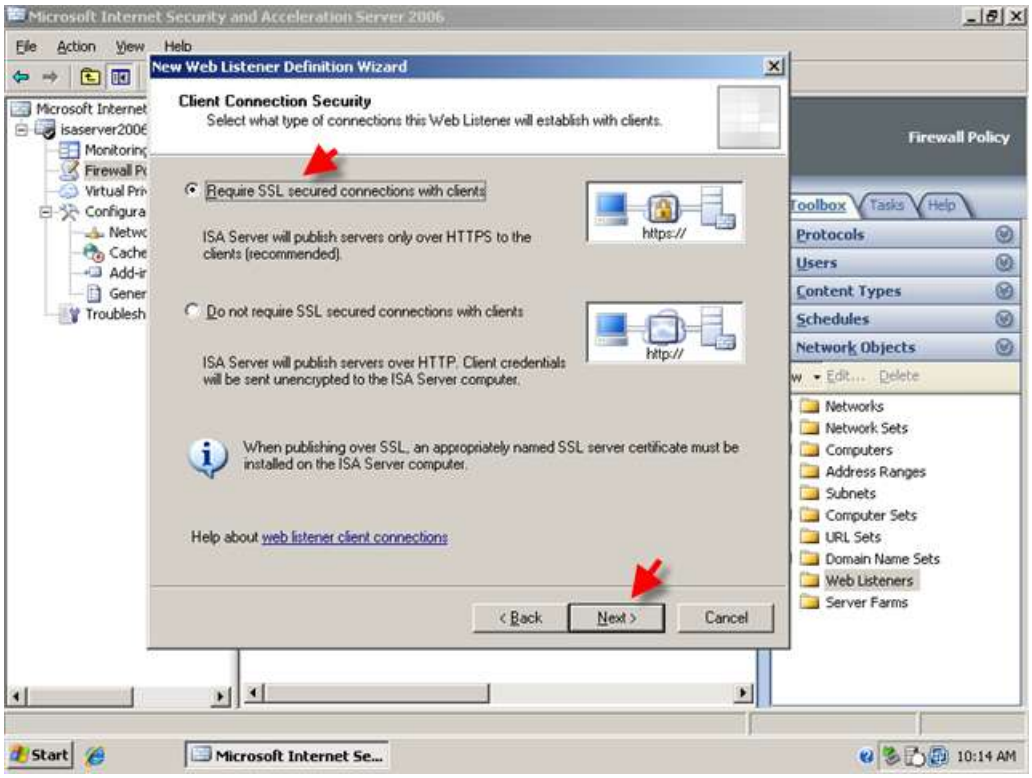
2. Click on 'New' and select 'Web Listener'



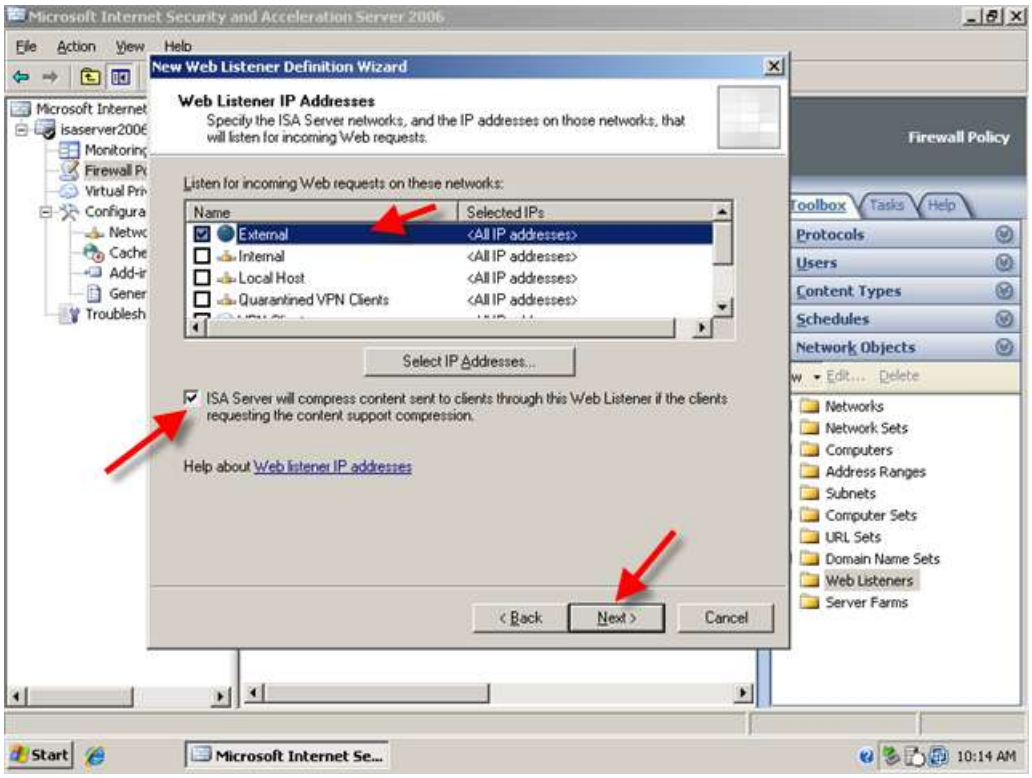
3. The new web listener wizard starts, enter a name for your web listener, I am choosing 'SBS Web Listener' click 'Next'



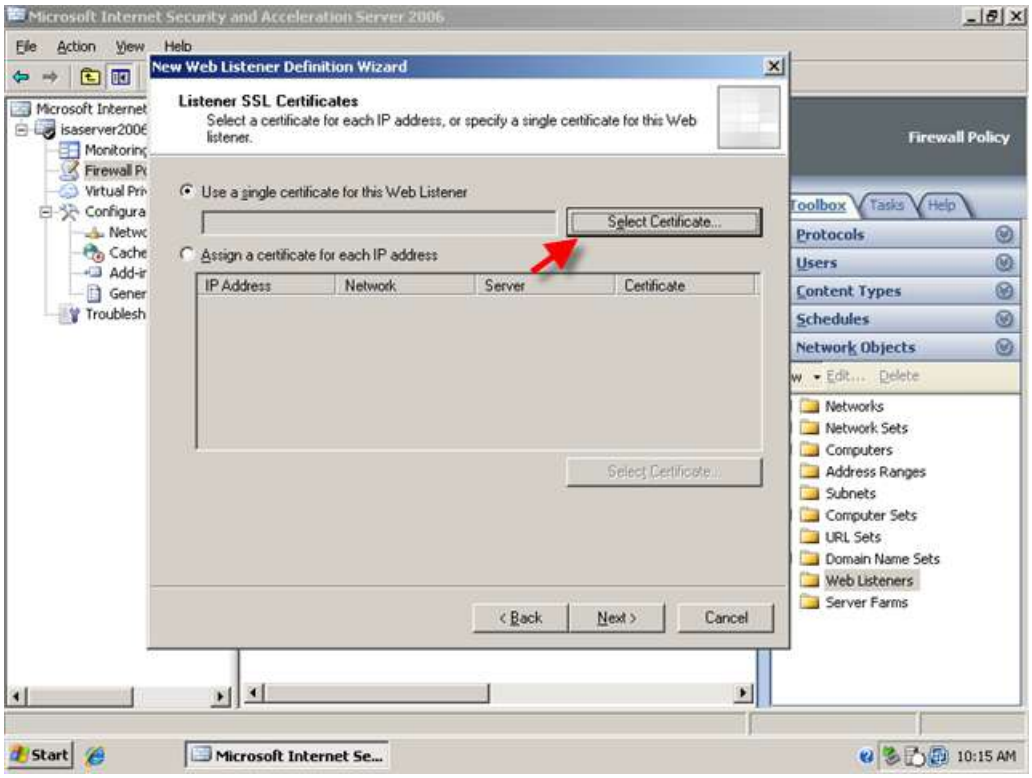
4. Accept the default 'Require SSL secured connections with clients' and click 'Next'

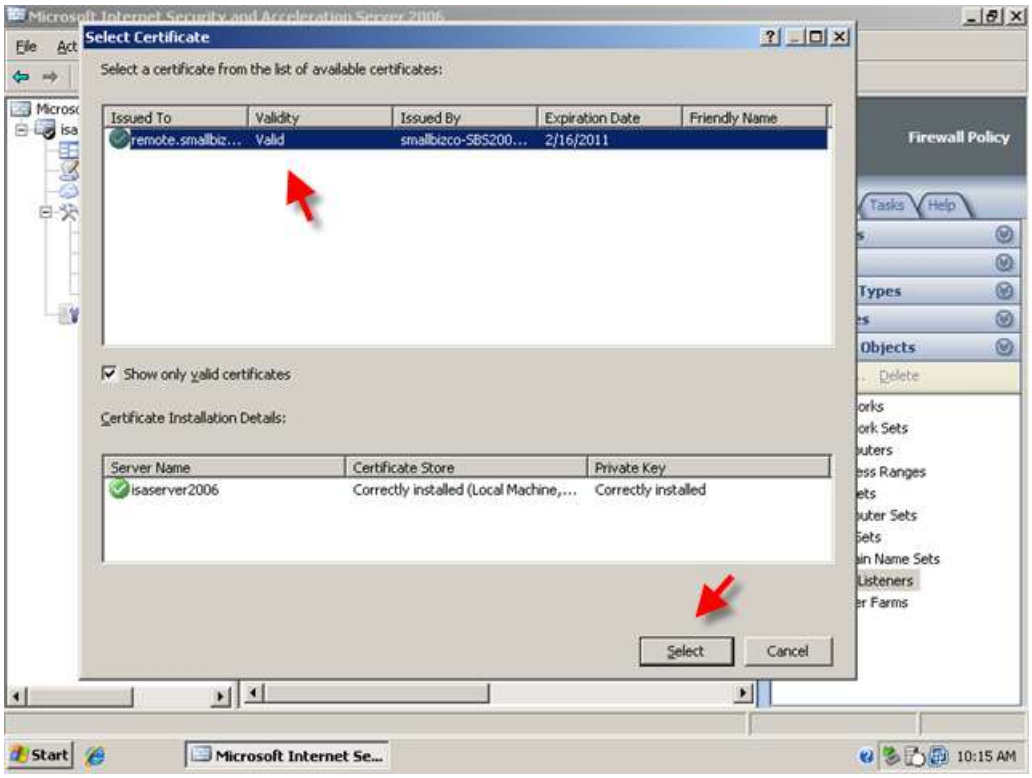


5. On the Web Listener IP Address page, Select the External Network and Click 'Next'

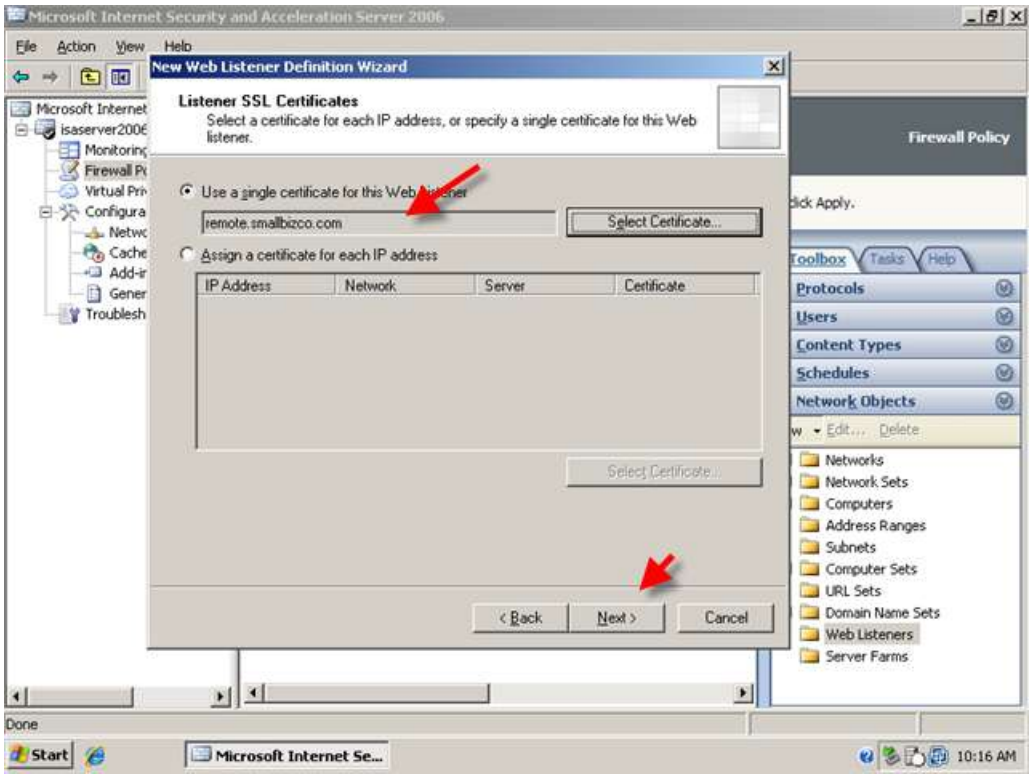


6. On the 'Listener SSL Certificate' click 'Select Certificate' there will only be one to choose from 'remote.domain.com' (this was installed into the local machine personal certificate store in Part 1 of this article, if you do not have any certificates installed please go back and review the steps to accomplish this)

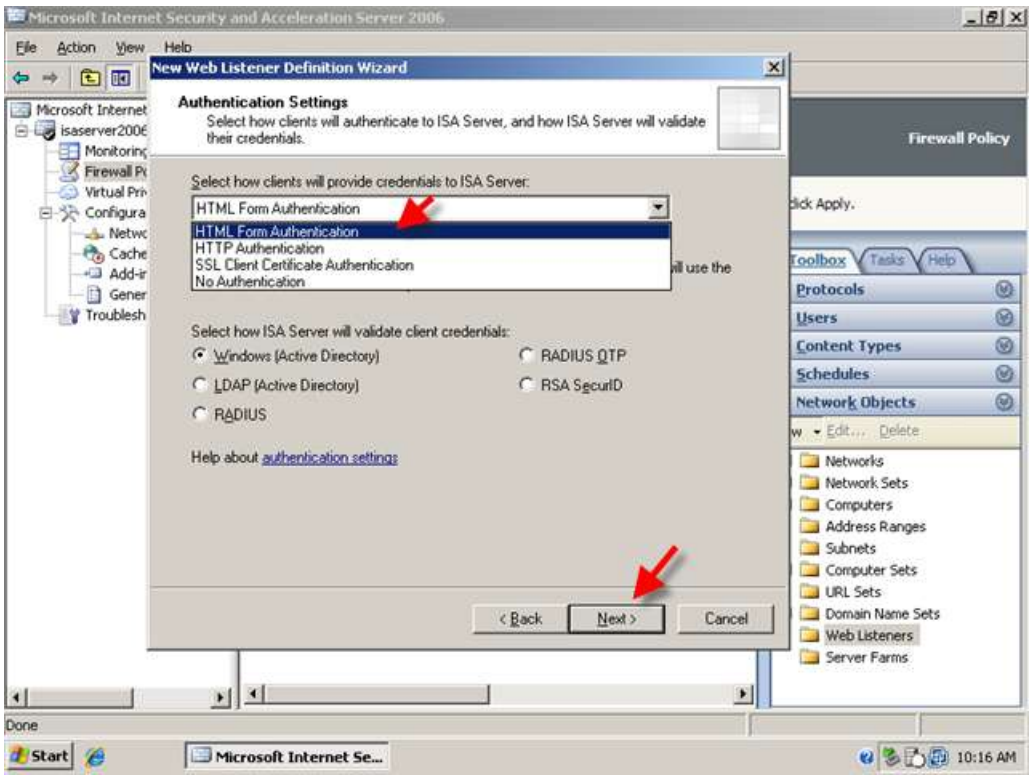




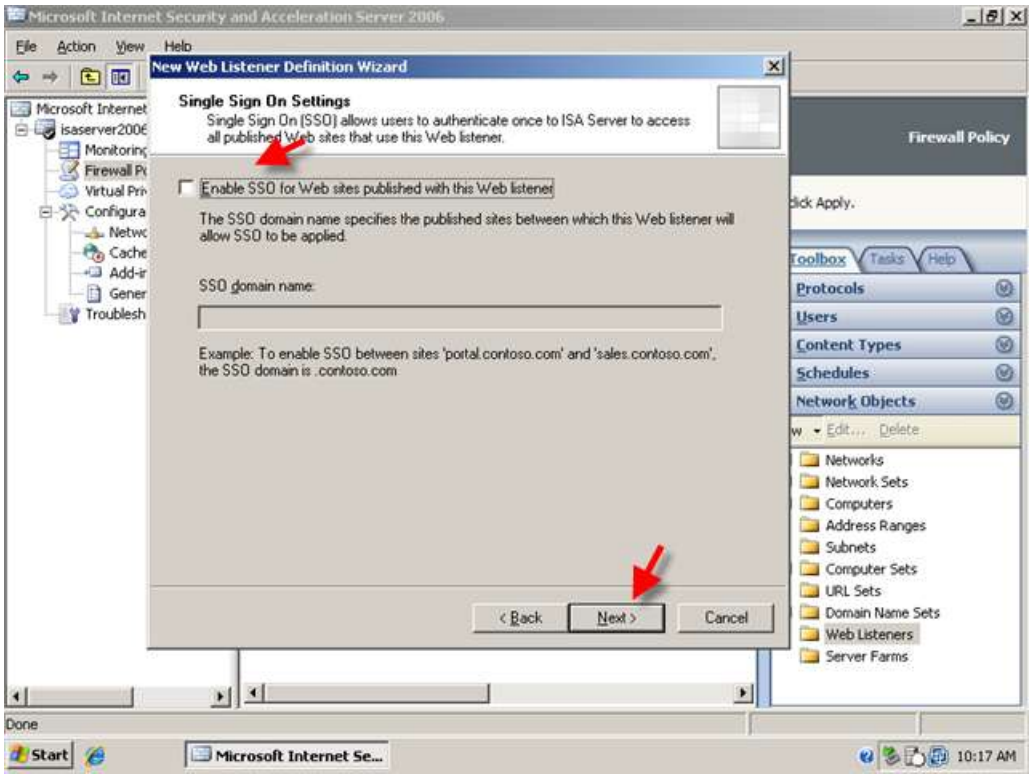
7. When you have selected your certificate, click 'Next'



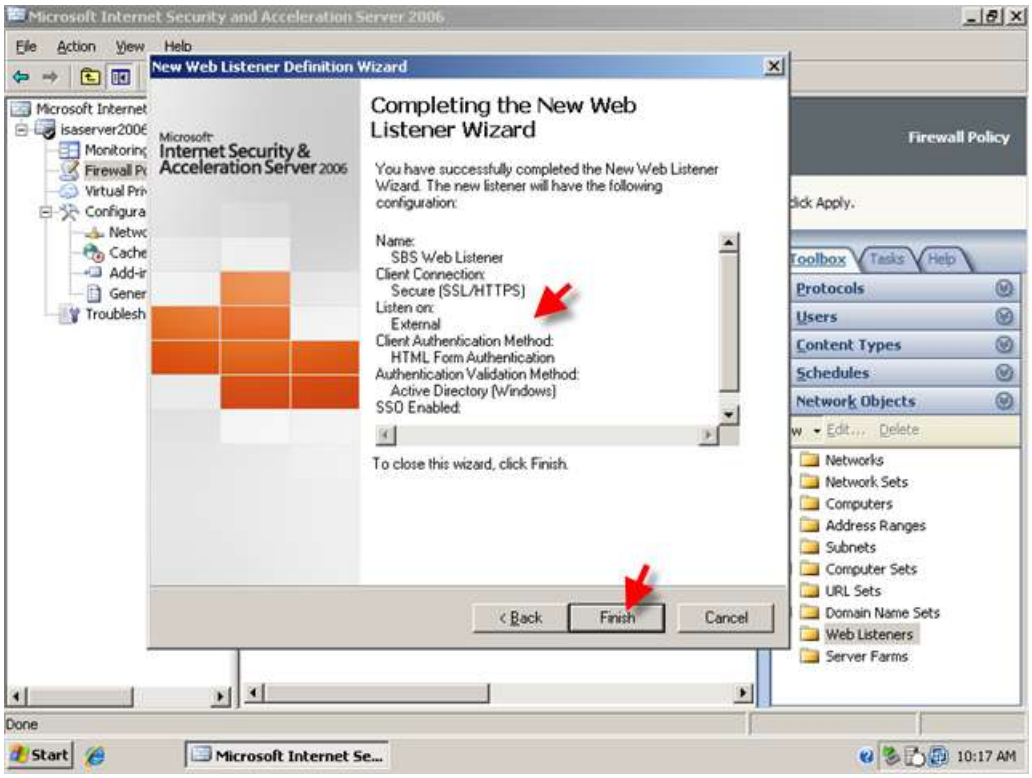
8. On the 'Authentication Settings' page choose HTML Form Authentication – leave the other settings untouched and click 'Next'



9. On the Single Sign On page – enter Un-tick the box for Single Sign on and Click Next.



10. Review your Web Listener Settings and click Finish to add them to the configuration.

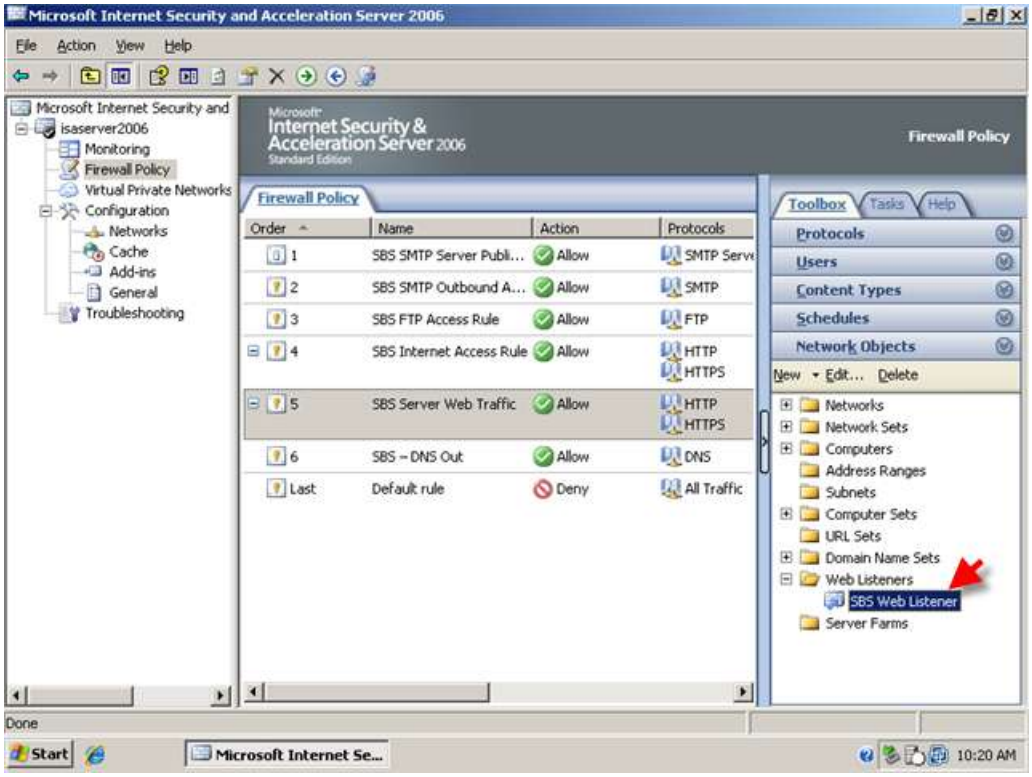


11. You can choose to apply your configuration now, or wait until after the next web listener has been created.

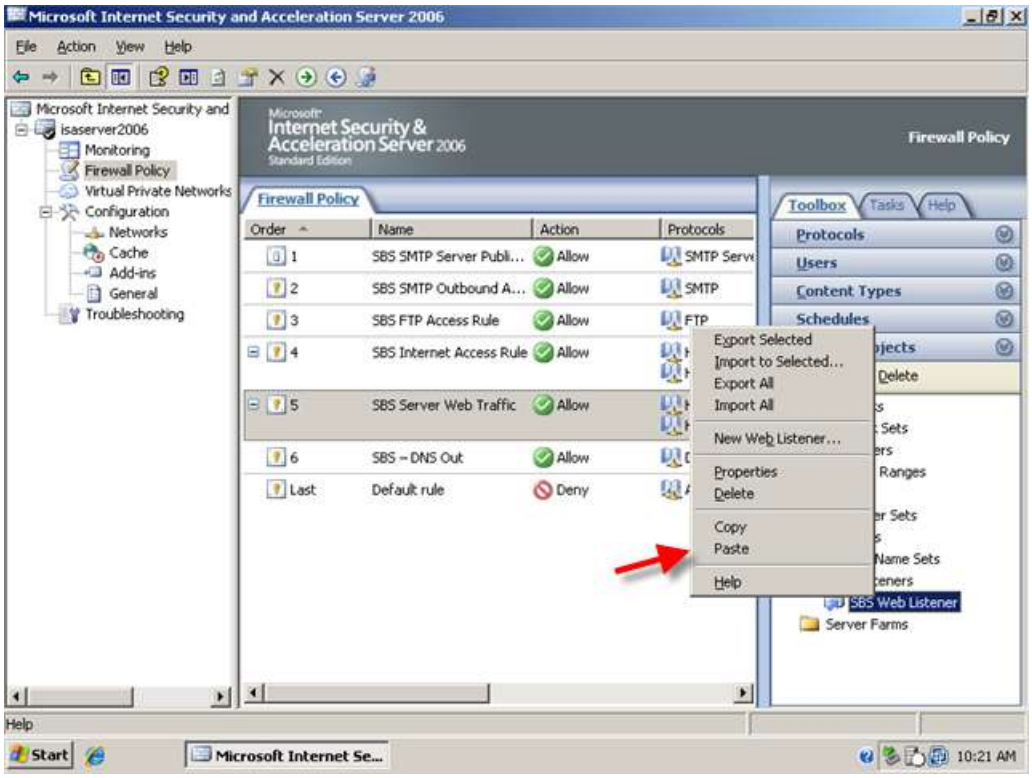
Creating a Web Listener for CompanyWeb Publishing

The settings for the CompanyWeb Web listener are nearly identical to that of the SBS Web Listener. The quickest way to create this is to use copy and paste.

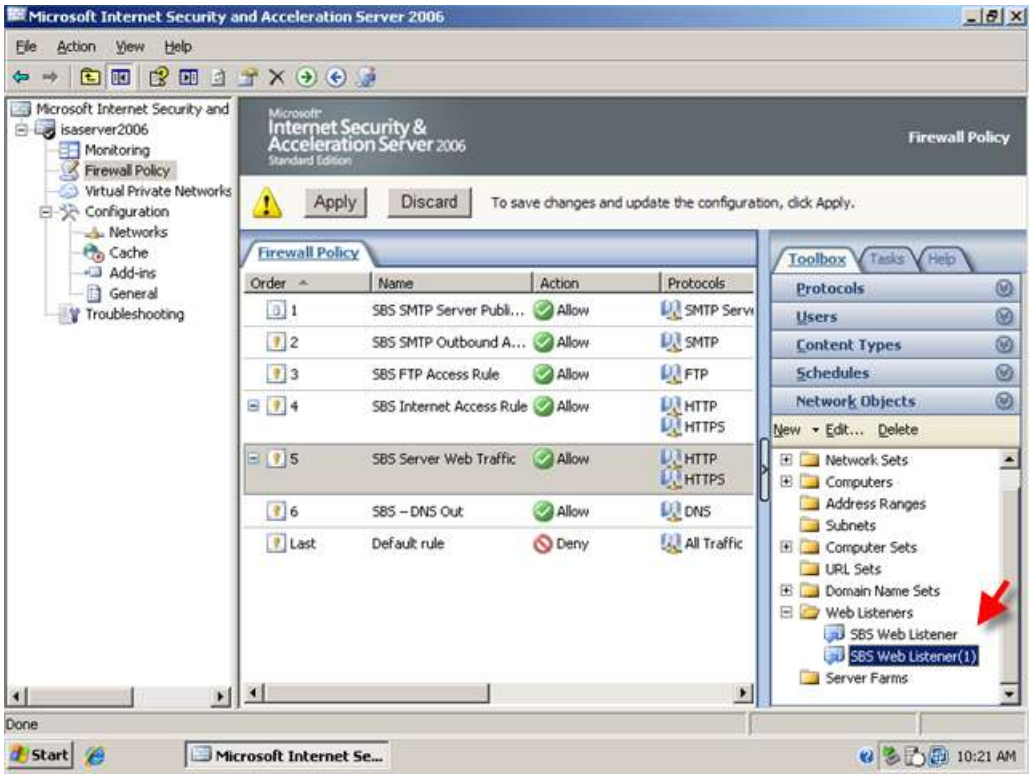
1. Right click the SBS Web Listener, and Click Copy.

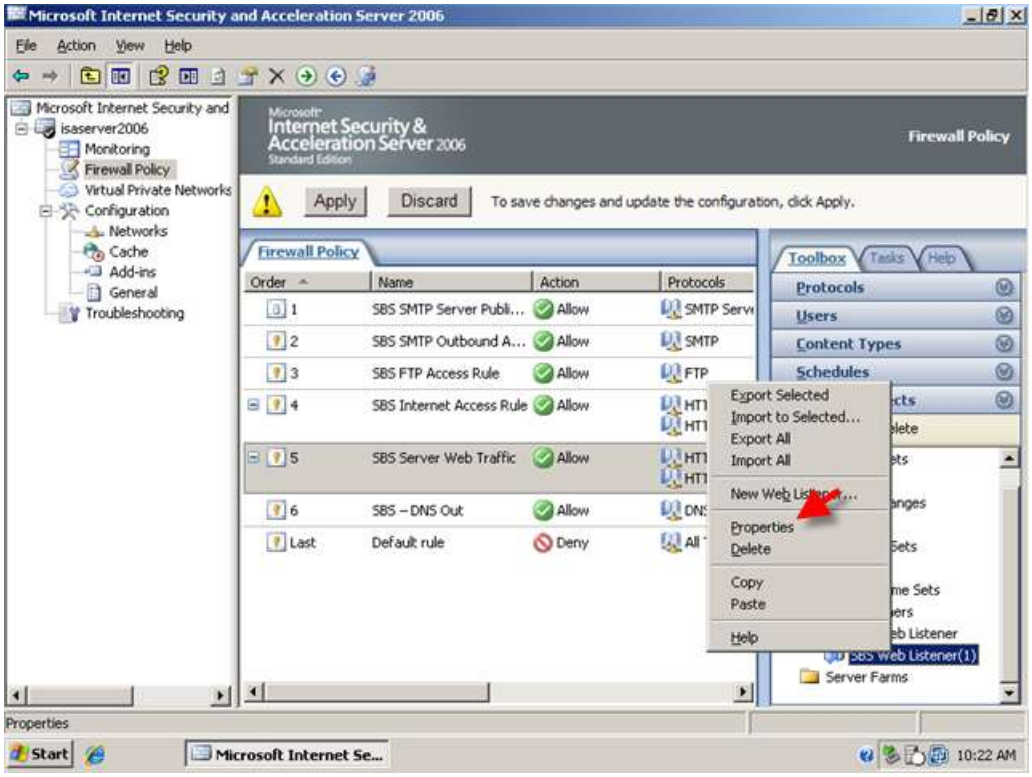


2. Right click it again, and click Paste.

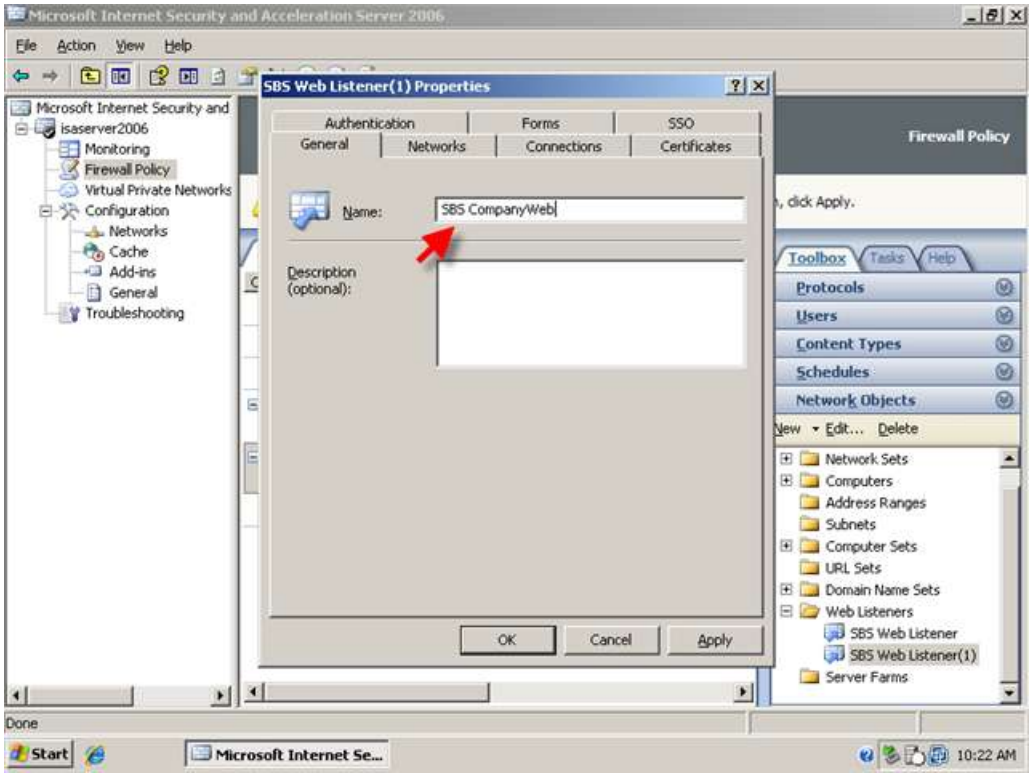


3. Notice your new web listener named SBS Web Listener(1) Right click this Web Listener and click Properties.

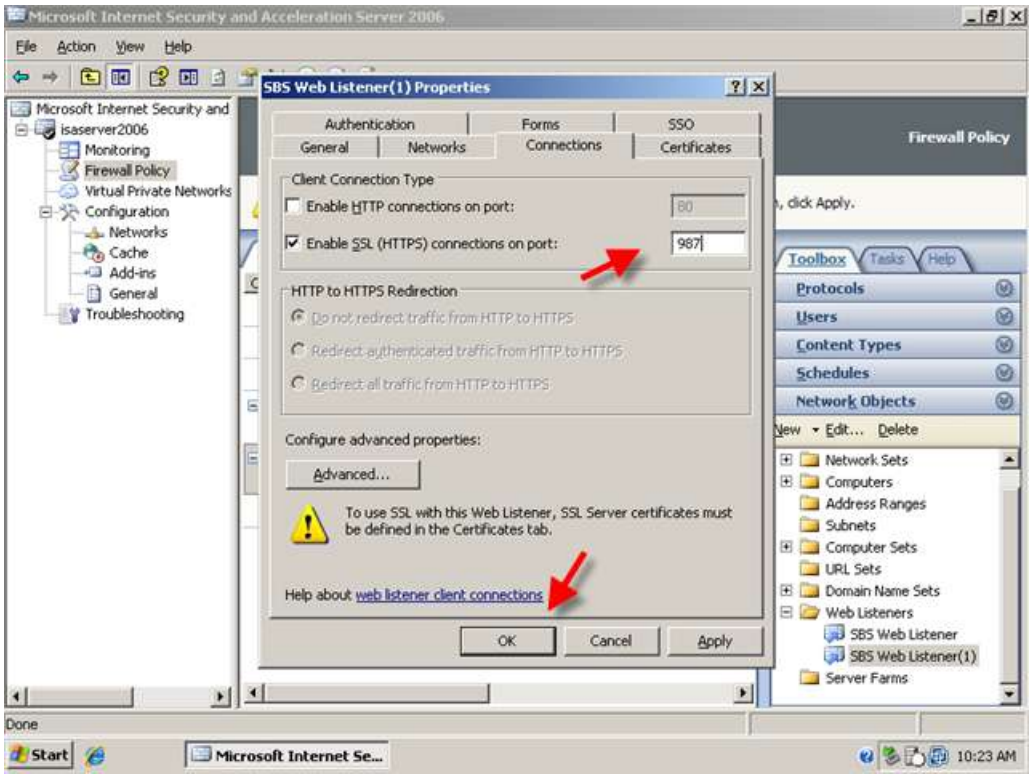




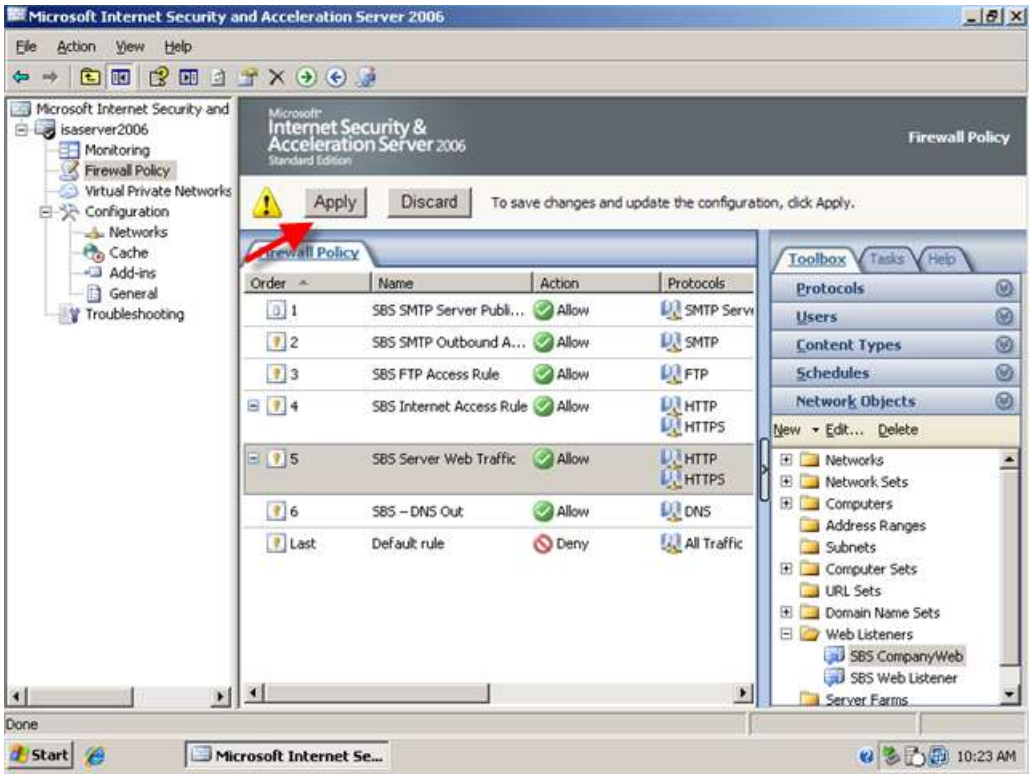
4. On the General Tab, you can rename this Web Listener – I am naming my listener SBS CompanyWeb Listener.



5. Switch to the Connections Tab. Change the Value 443 to 987. Click OK to accept these changes.



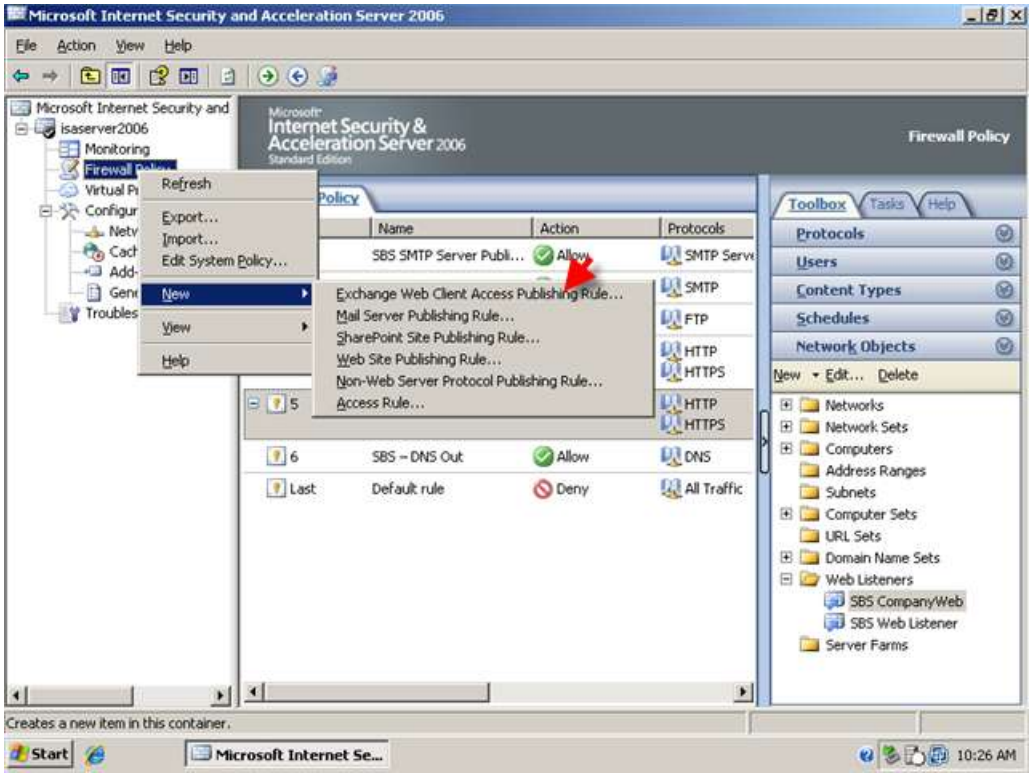
6. You will see your new web listener in the toolbox. Click Apply to save these changes to your Firewall Policy.



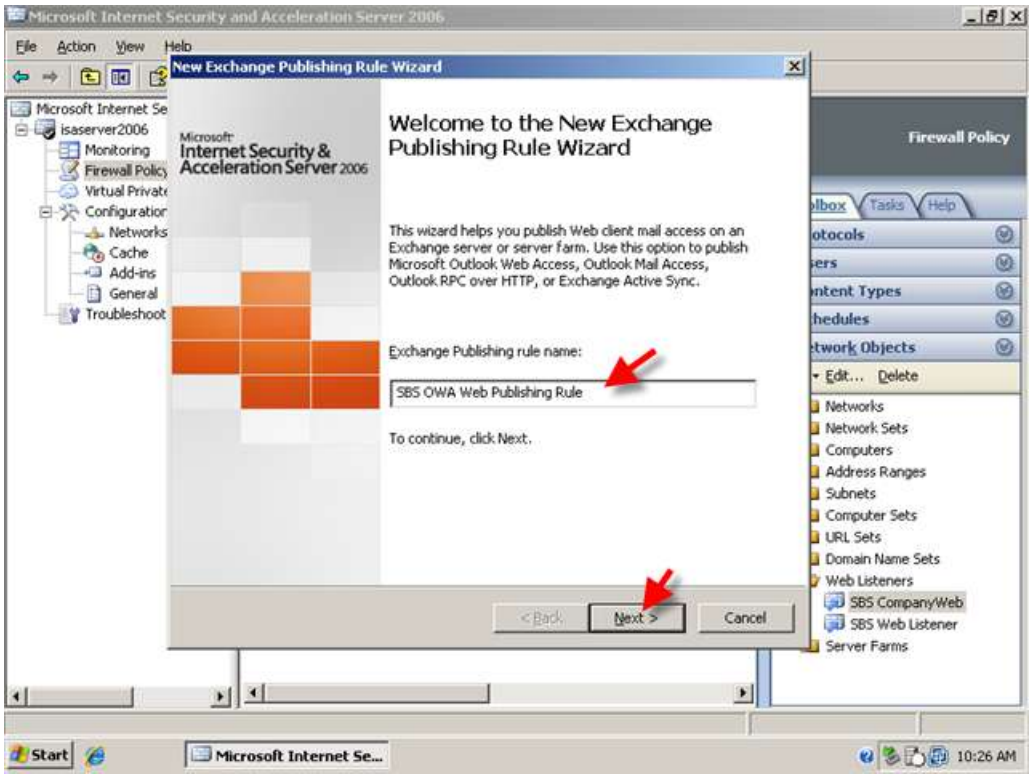
Creating a Web Publishing Rule For Microsoft Exchange Server 2007 Outlook Web Access

We can now create our first publishing rule.

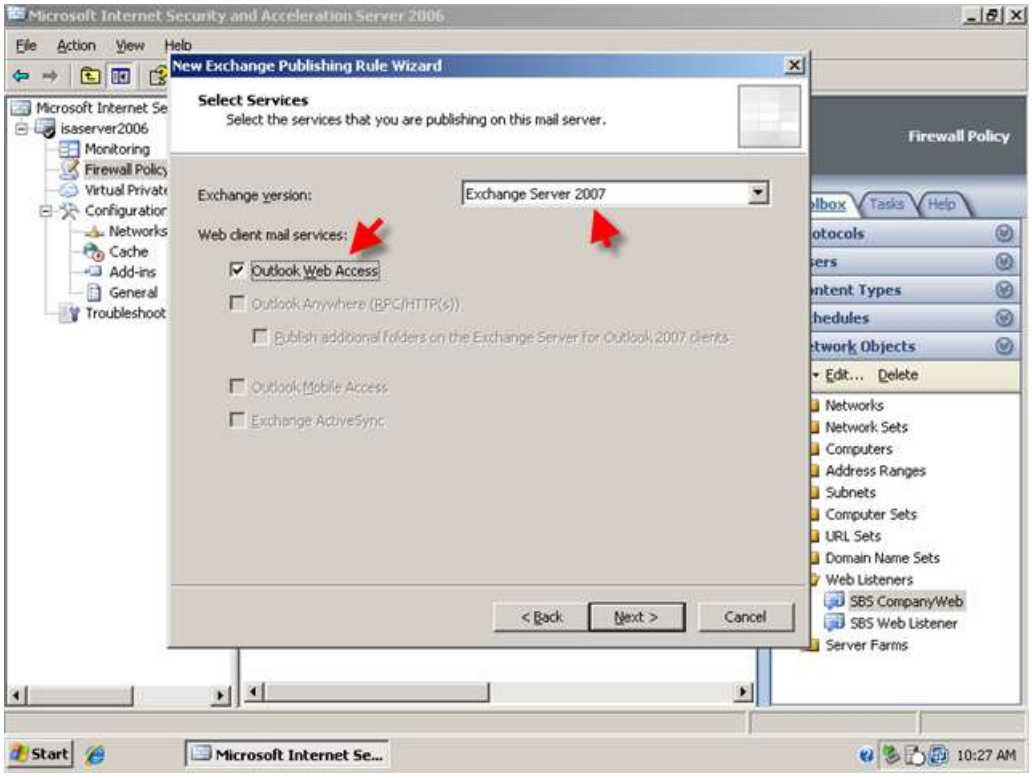
1. In ISA Server Management, right click 'Firewall Policy' click 'New' and then Click 'Exchange Web Client Access Publishing Rule'



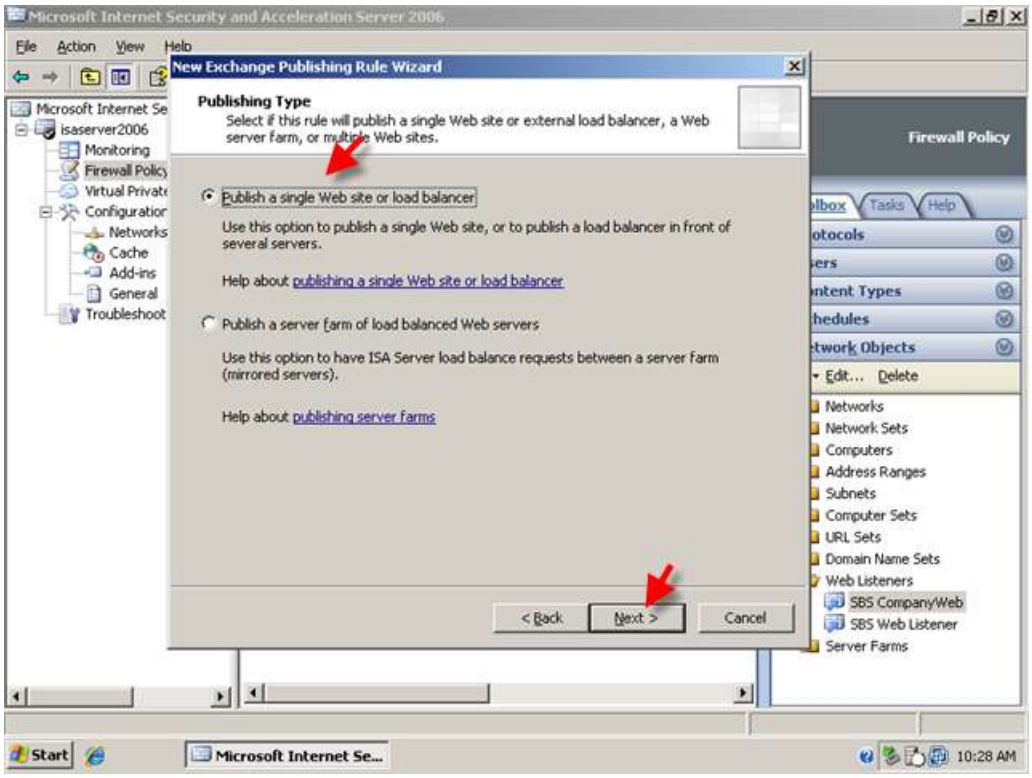
2. Name your rule, I am naming my rule – 'SBS OWA Web Publishing Rule' I am using the name OWA because each different type of Web Access now requires a separate publishing rule, With Exchange 2003 you could use one single rule.



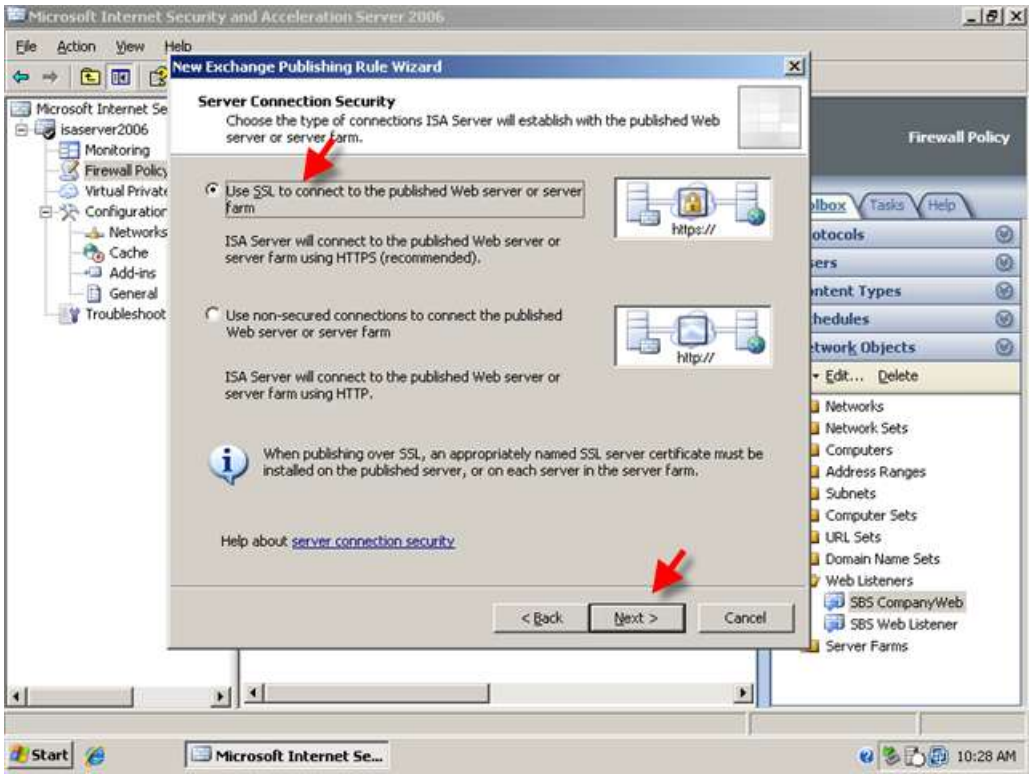
3. On the next page, choose Exchange 2007 from the drop down menu – then put a tick in the box for Outlook Web Access – you will see all the other options are now grayed out.



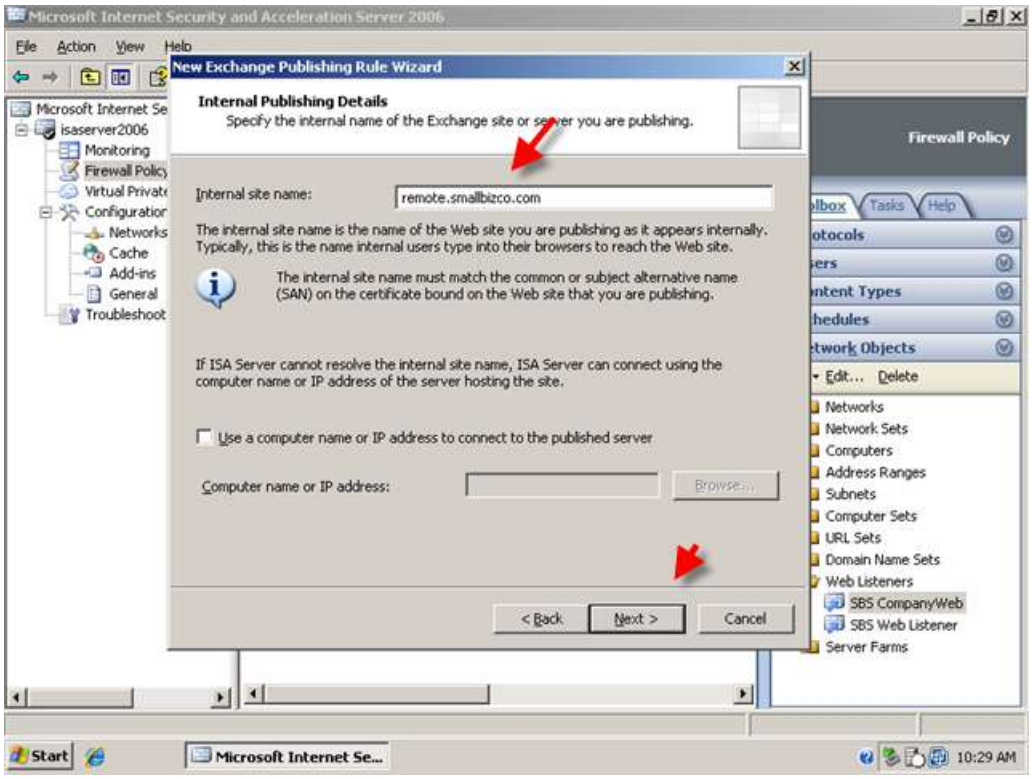
4. Click next and accept the default 'Single Web Site' Click Next

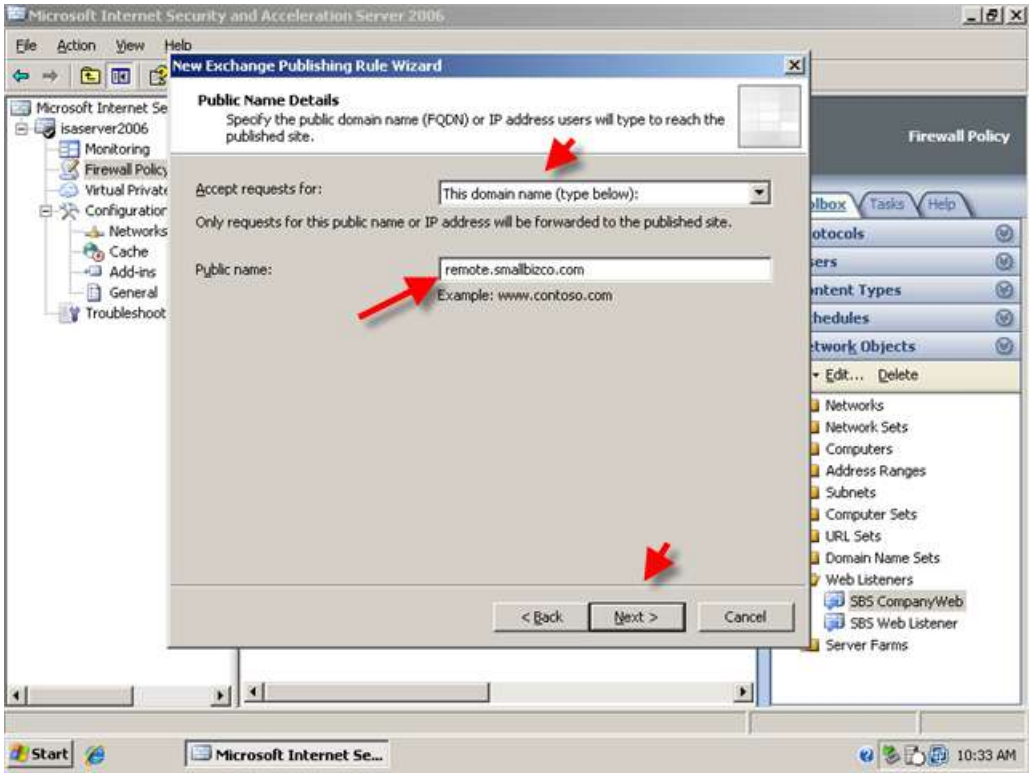


5. Accept the default for SSL to connect to the published web server or server farm

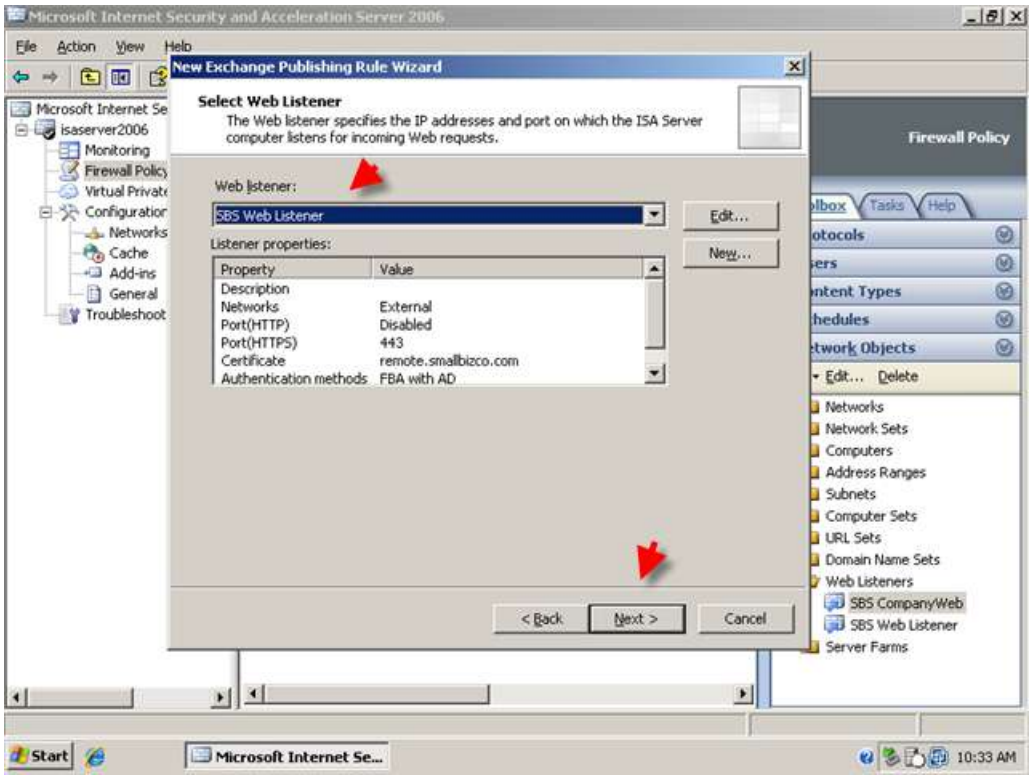


6. On the internal publishing details page, Enter 'remote.smallbizco.com' (where remote.smallbizco.com is your public domain name)

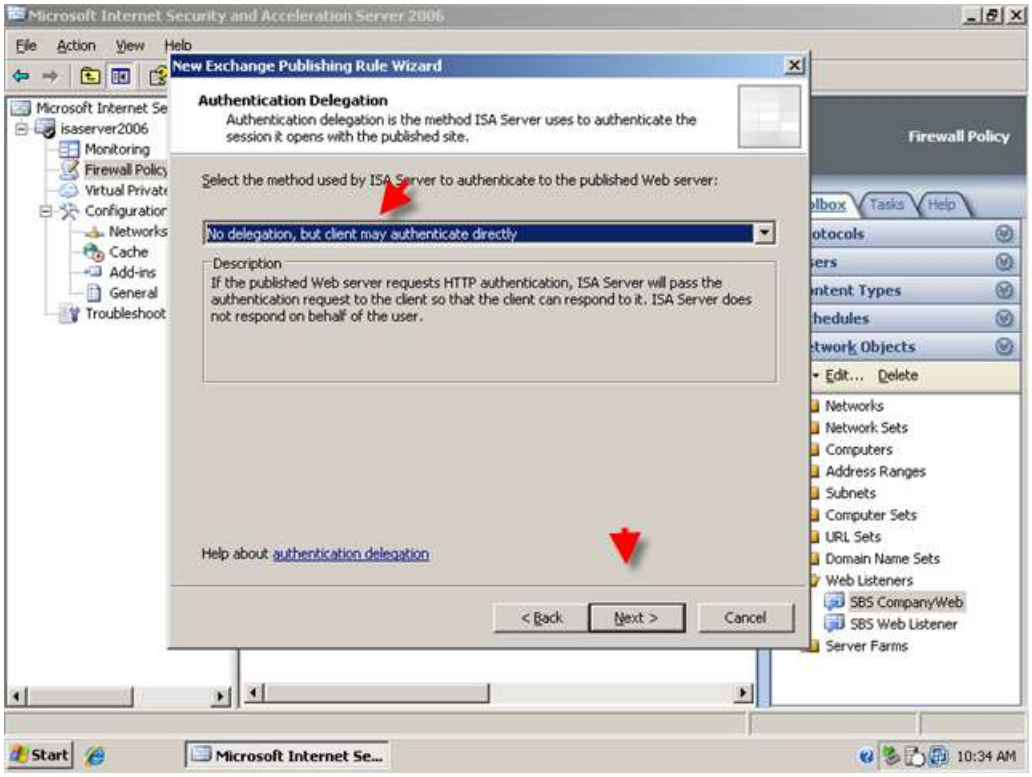




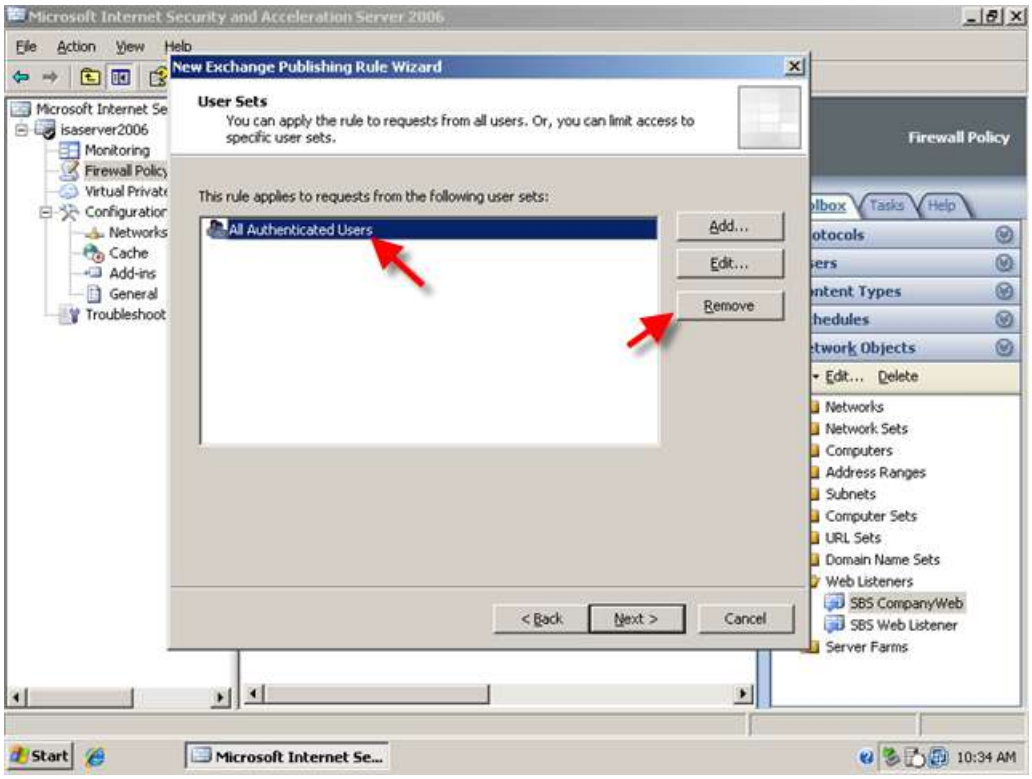
7. On the 'select web listener' page use the drop down menu to select the web listener we created earlier, and click next.

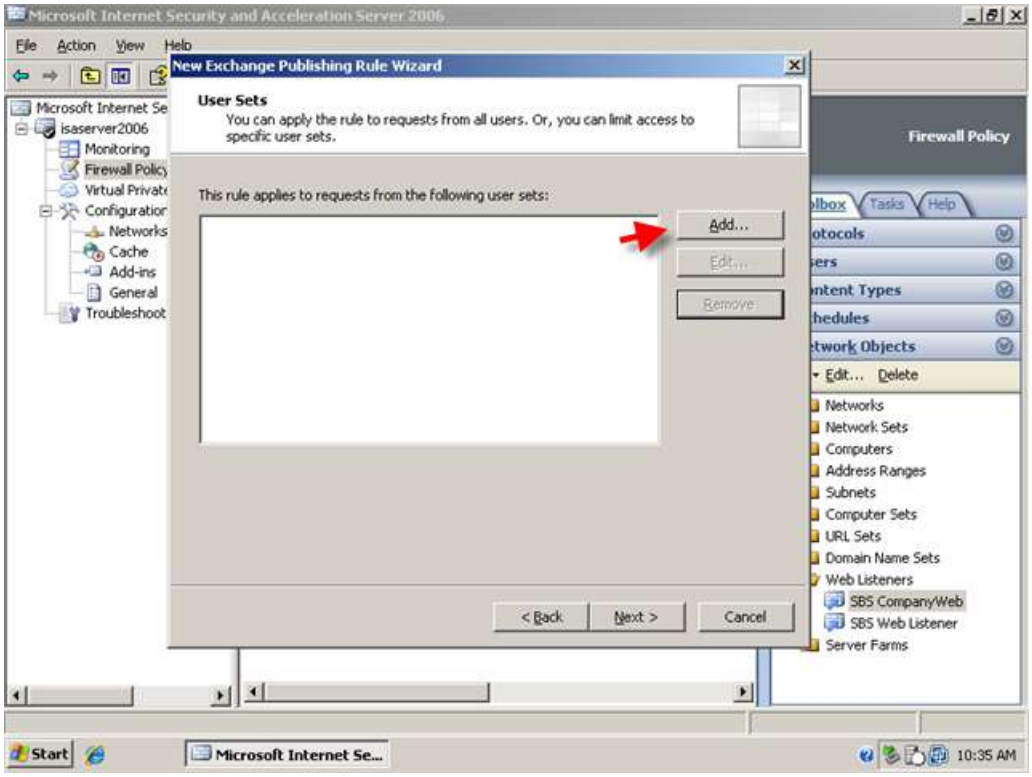


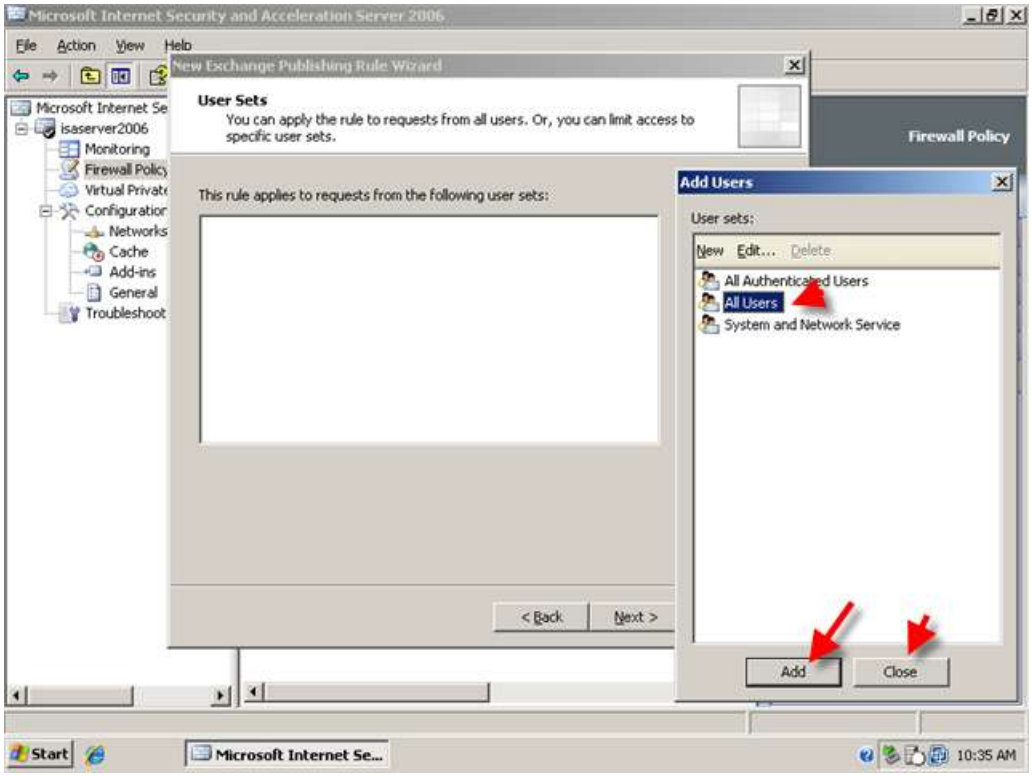
8. On the Authentication Delegation page – change the authentication method to 'no authentication delegation but client may authenticate directly' and click next

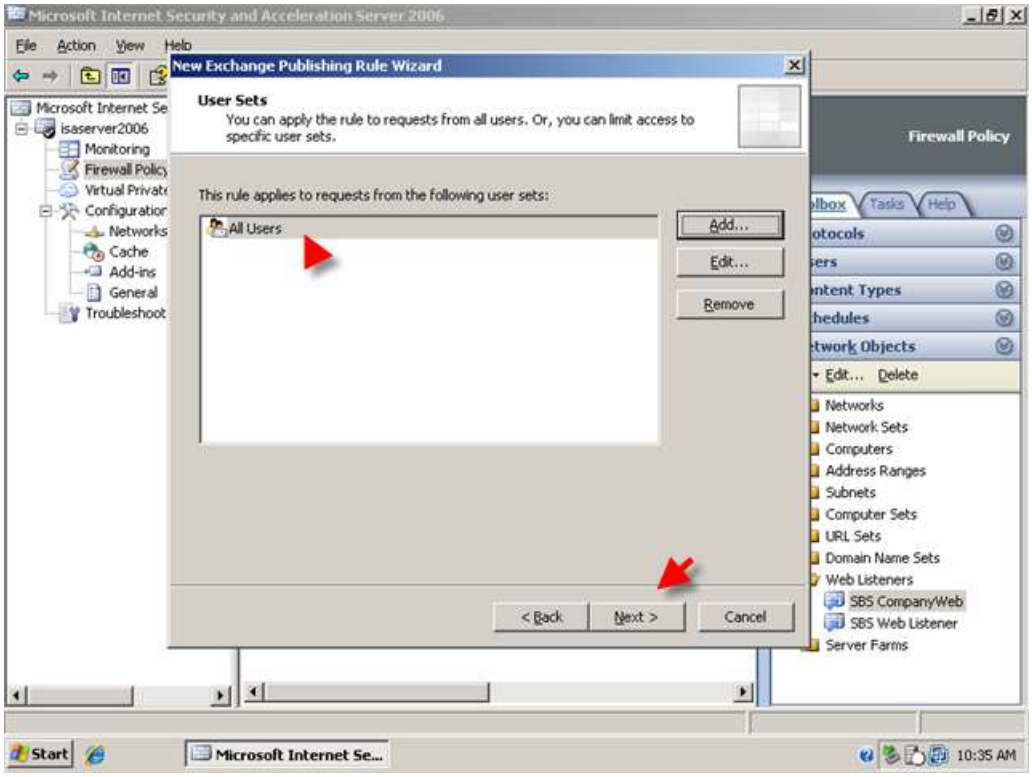


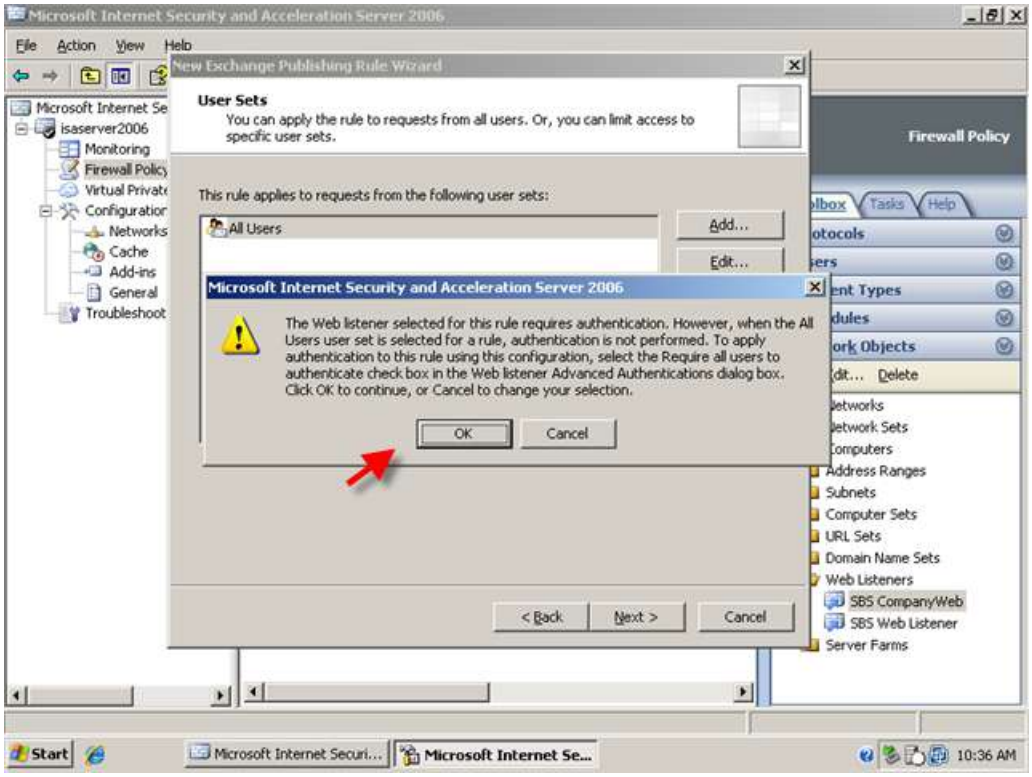
9. On the User select 'All Authenticated users, and click Remove. Click Add and select All Users, Click Add then click Close.



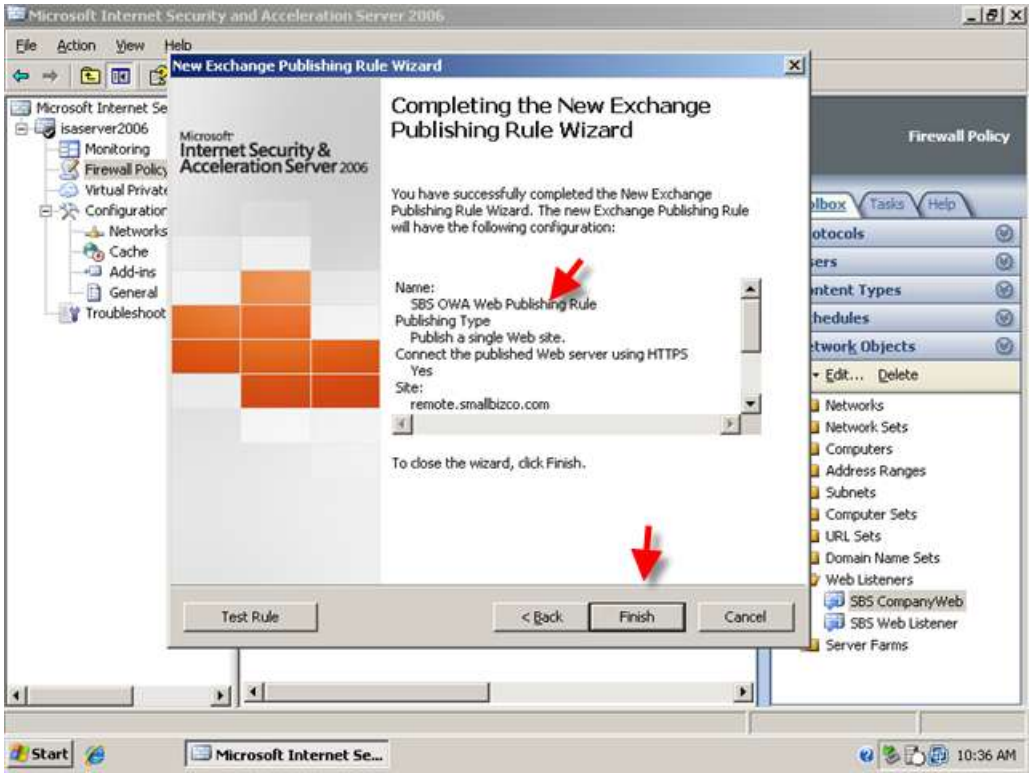


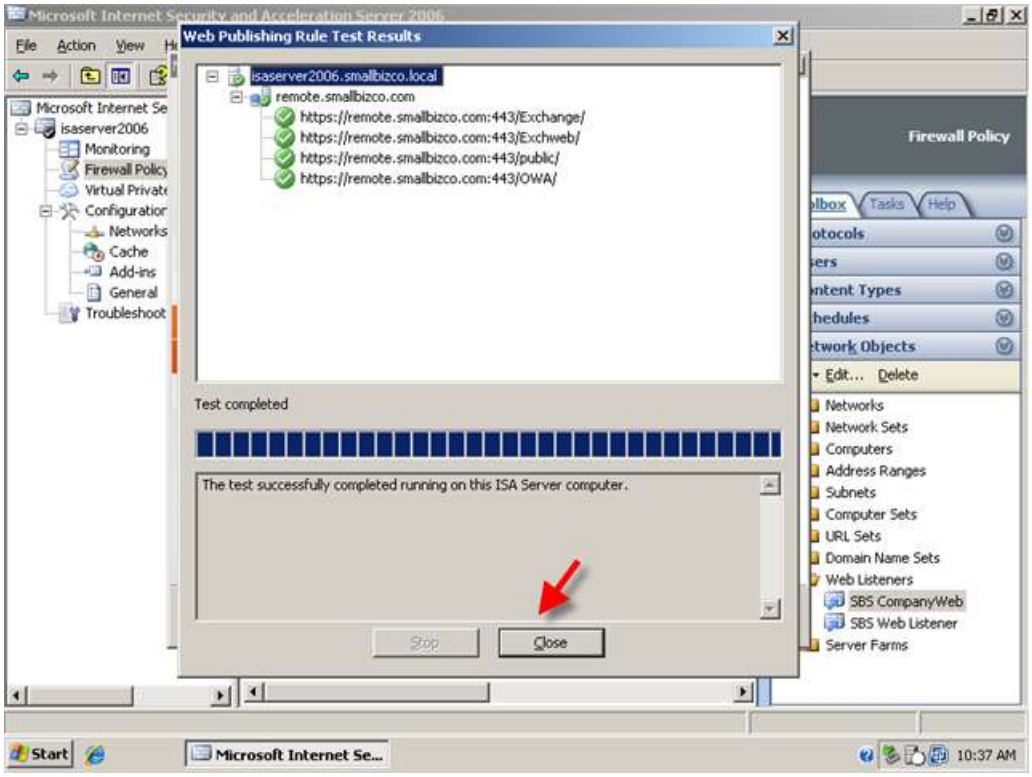

Microsoft Internet Security and Acceleration Server 2006
File Action View Help
New Exchange Publishing Rule Wizard
User Sets
You can apply the rule to requests from all users. Or, you can limit access to specific user sets.
This rule applies to requests from the following user sets:
< Back
Next >
Add Users
User sets:
New Edit... Delete
All Authenticated Users
All Users
System and Network Service
Add
Close
Firewall Policy
Start
Microsoft Internet Se...
10:35 AM


Microsoft Internet Security and Acceleration Server 2006
File Action View Help
New Exchange Publishing Rule Wizard
User Sets
You can apply the rule to requests from all users. Or, you can limit access to specific user sets.
This rule applies to requests from the following user sets:
All Users
Add...
Edit...
Remove
< Back
Next >
Cancel
Firewall Policy
Tasks
Help
Edit... Delete
Networks
Network Sets
Computers
Address Ranges
Subnets
Computer Sets
URL Sets
Domain Name Sets
Web Listeners
SBS CompanyWeb
SBS Web Listener
Server Farms
Start
Microsoft Internet Se...
10:35 AM

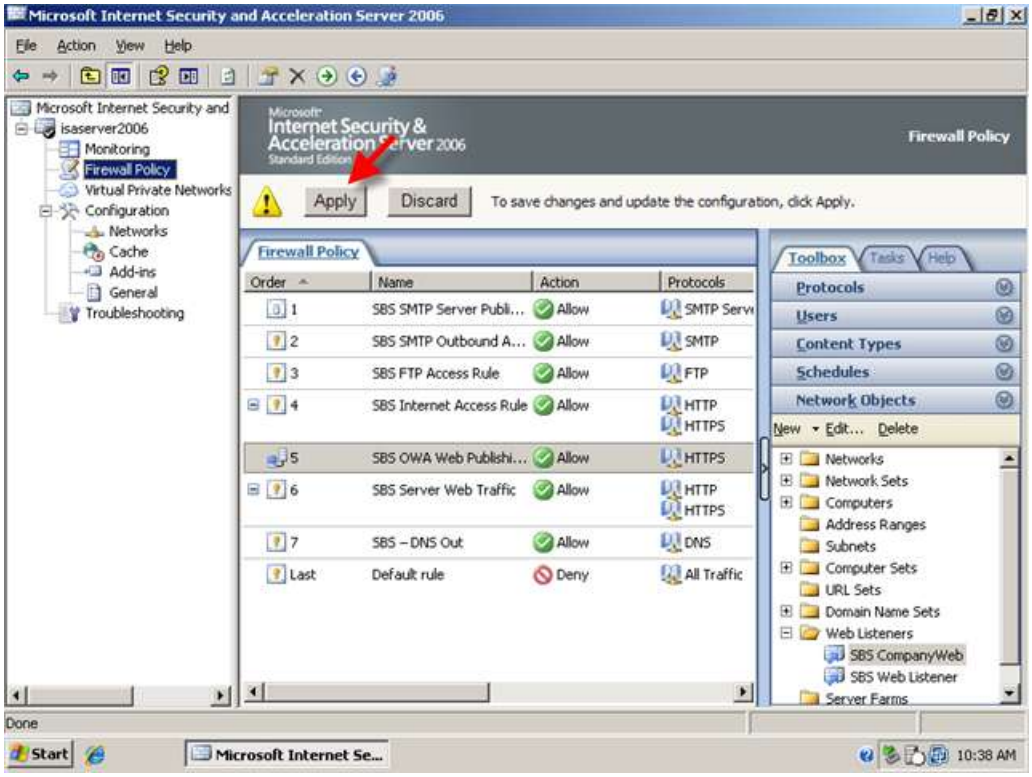


10. Click Next to review your rule settings, you can also click to 'Test Rule' the rule at this point. Click Finish when you are happy with your rule.





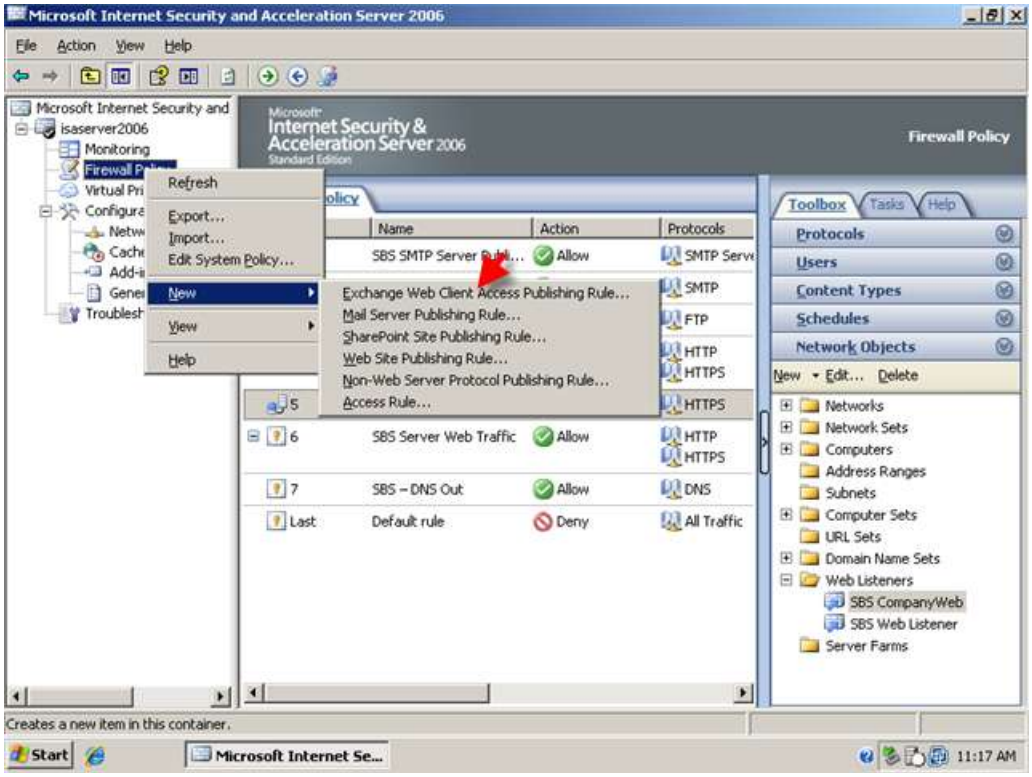
11. Click Apply to accept these configuration changes.



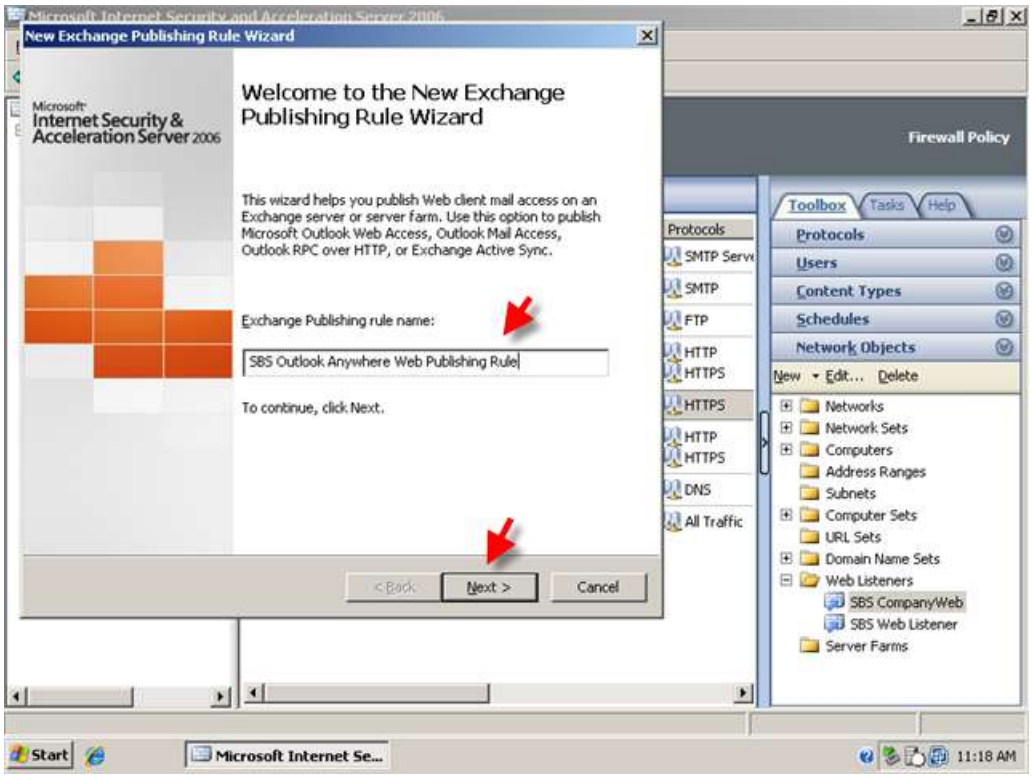
Now we must open up a port on your internet router to allow traffic to reach your ISA Server. The port required is TCP 443 and this should go to the external IP of your ISA Server. From an external source you can now navigate to https://remote.domain.com/owa to get to the OWA Site. If you are using a non domain workstation you will be prompted by a Certificate Warning which you will need to acknowledge before continuing on to the site. You will then be shown the OWA Login page. You can now login using your email address and password to access your Mail Box.

Creating a Web Publishing Rule For Microsoft Exchange Server 2007 Outlook Anywhere (Outlook RPC /HTTPS)

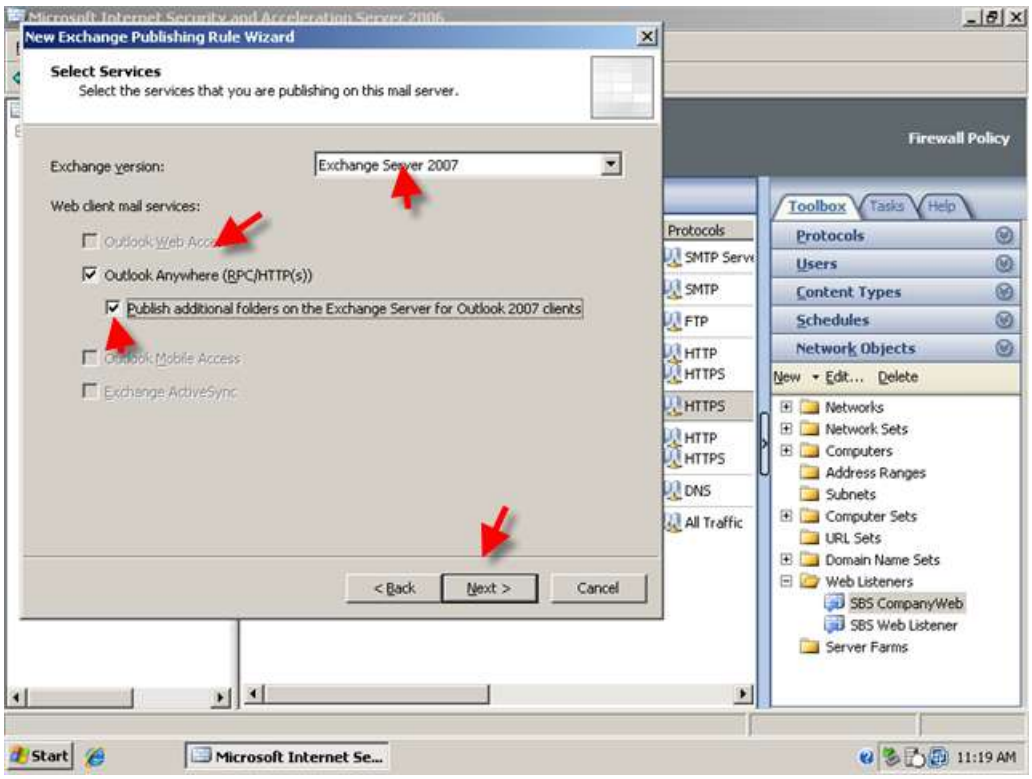
1. To create a rule for Outlook Anywhere (Outlook RPC/HTTPS) Right click Firewall Policy click New . Exchange Web Client Publishing Rule.



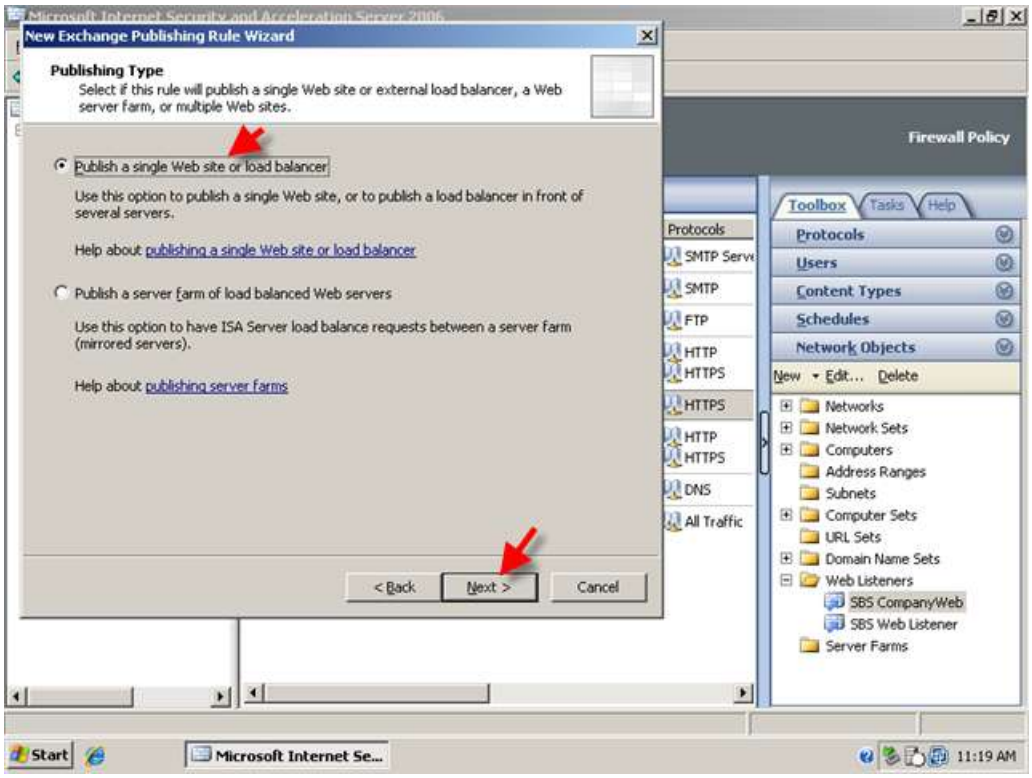
2. Name your rule, I am using the name SBS Outlook Anywhere Web Publishing Rule, click Next.



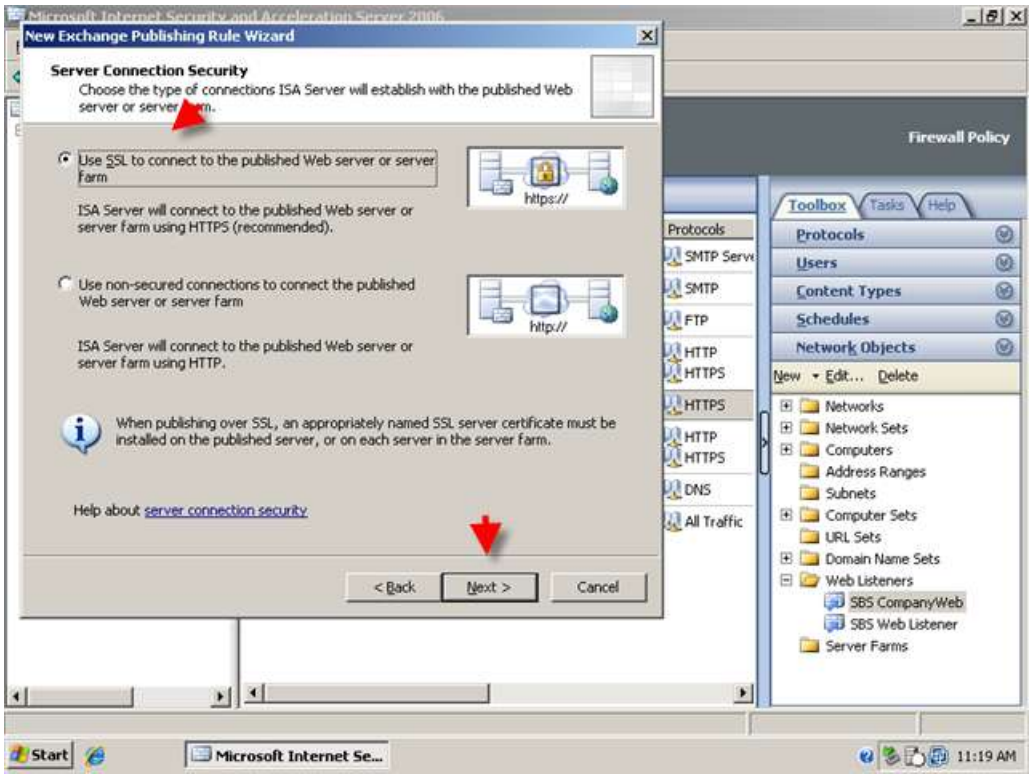
3. Choose Exchange 2007 from the dropdown list. Select the Outlook Anywhere check box and also tick the box to publish additional folders. Click Next.



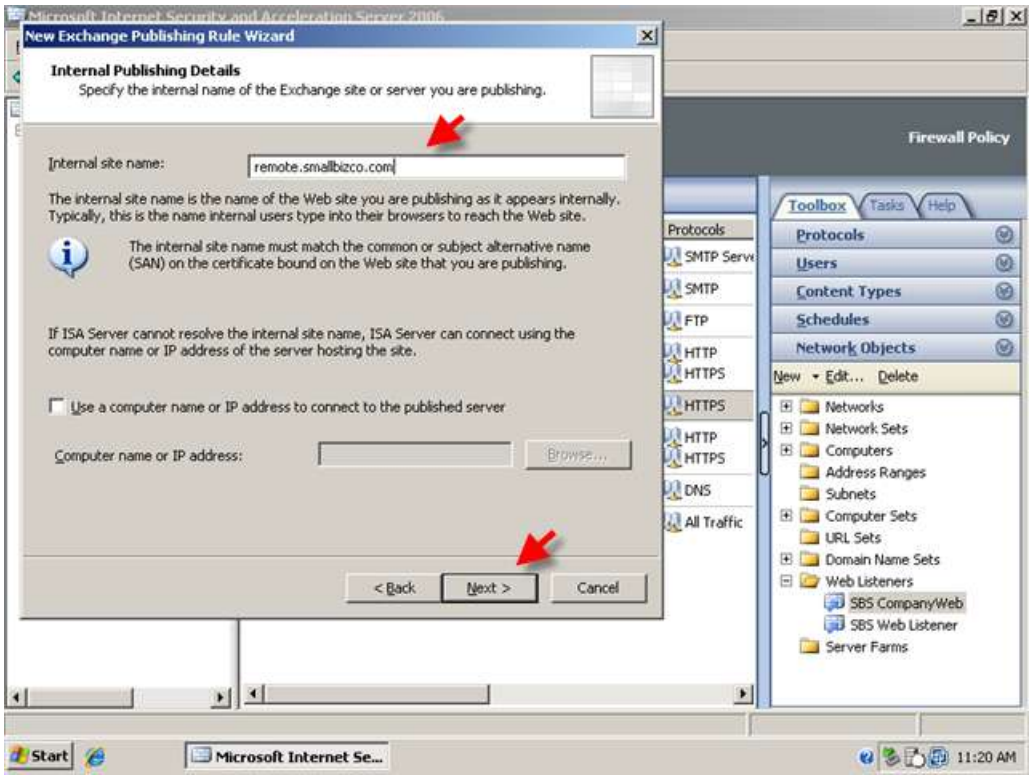
4. Click Next to accept the default 'Publish Single Website or Load Balancer'



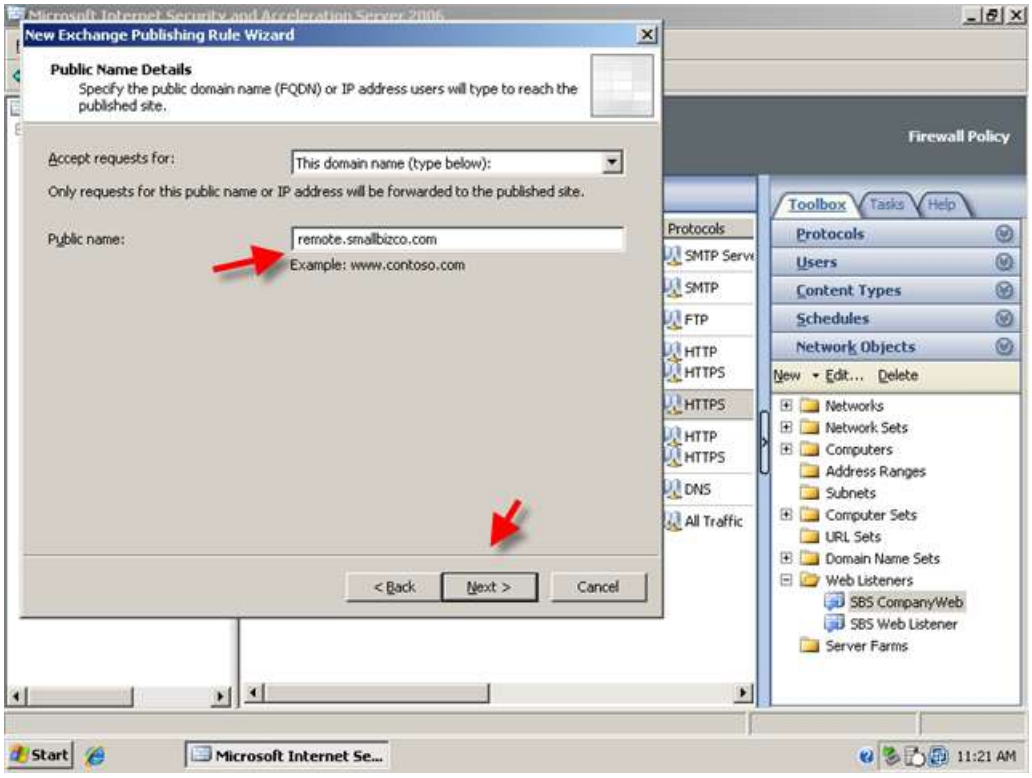
5. Click Next to accept the default 'Use SSL to connect to the published web Server'



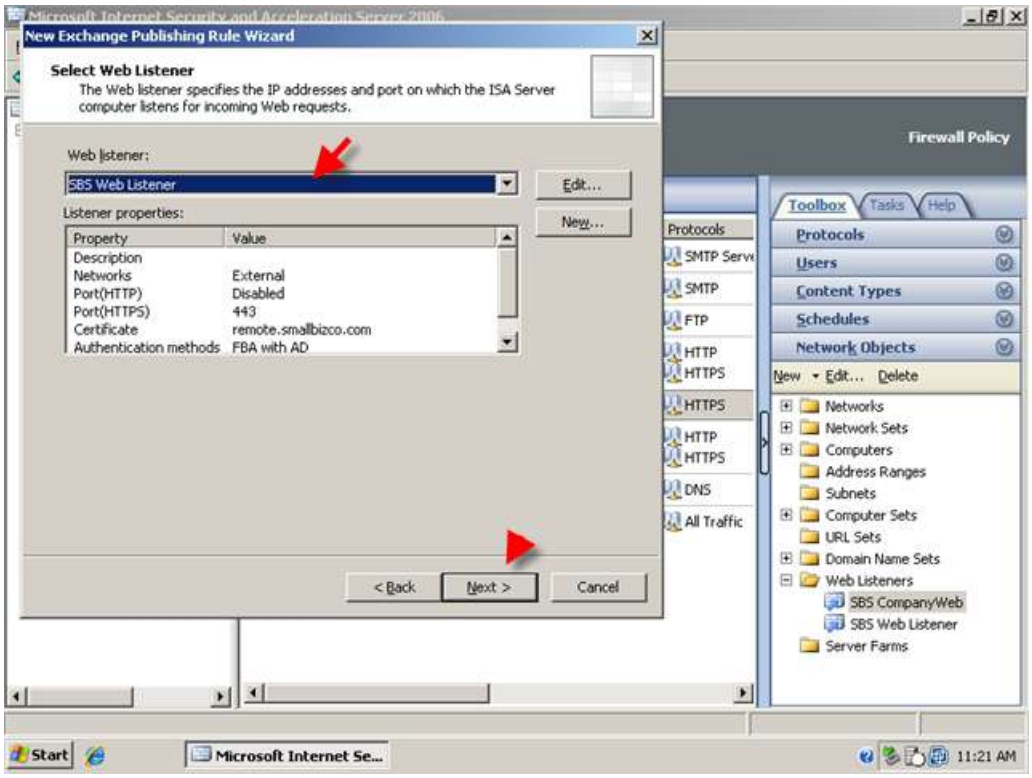
6. On the internal site name page enter 'remote.smallbizco.com' (where remote.smallbizco.com is your public DNS name) Click Next.



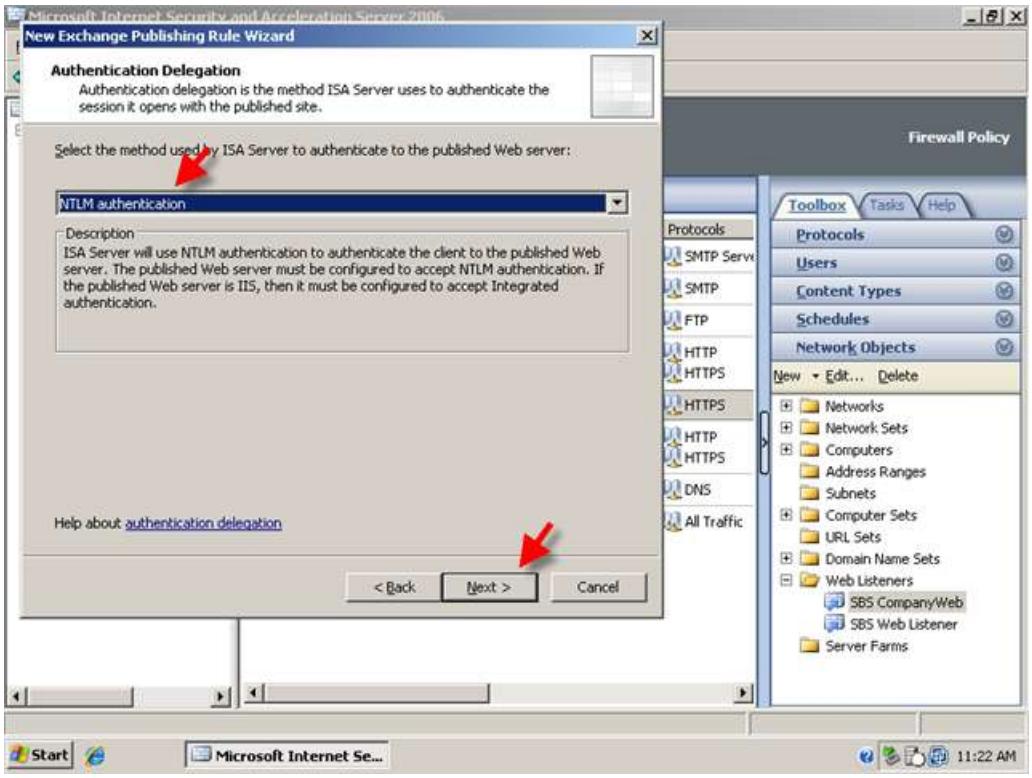
7. On the public name details page enter 'remote.smallbizco.com' (where remote.smallbizco.com is your public DNS name) Click Next.



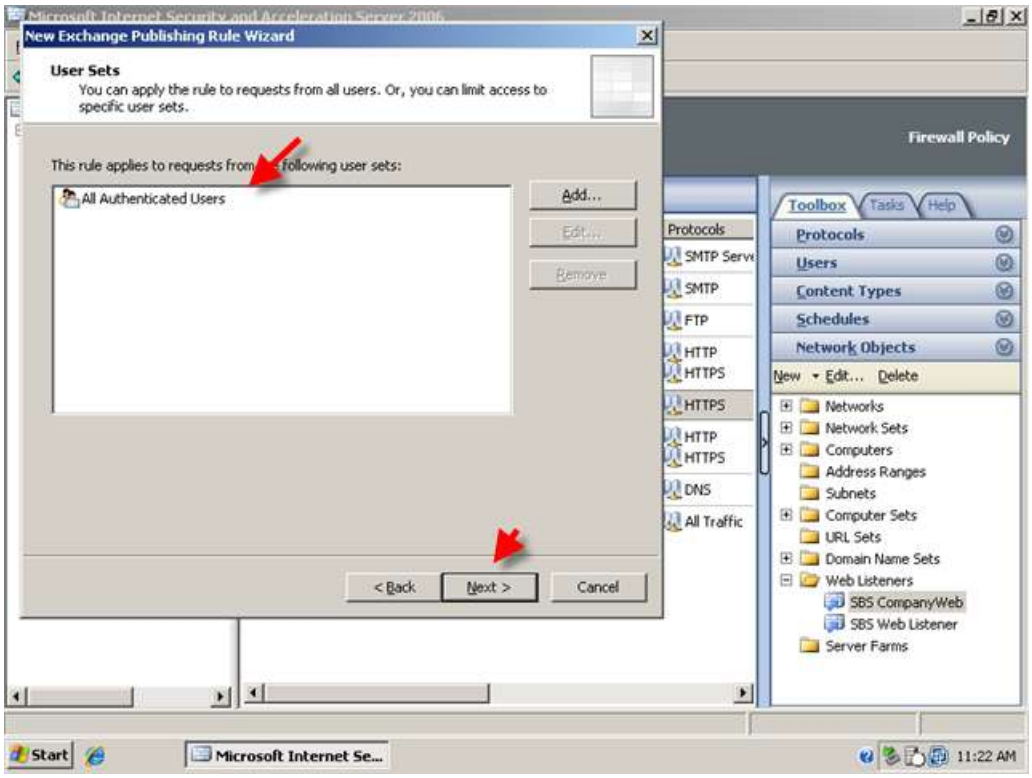
8. On the Web Listener page, select your SBS Web Listener from the drop down menu and click Next.



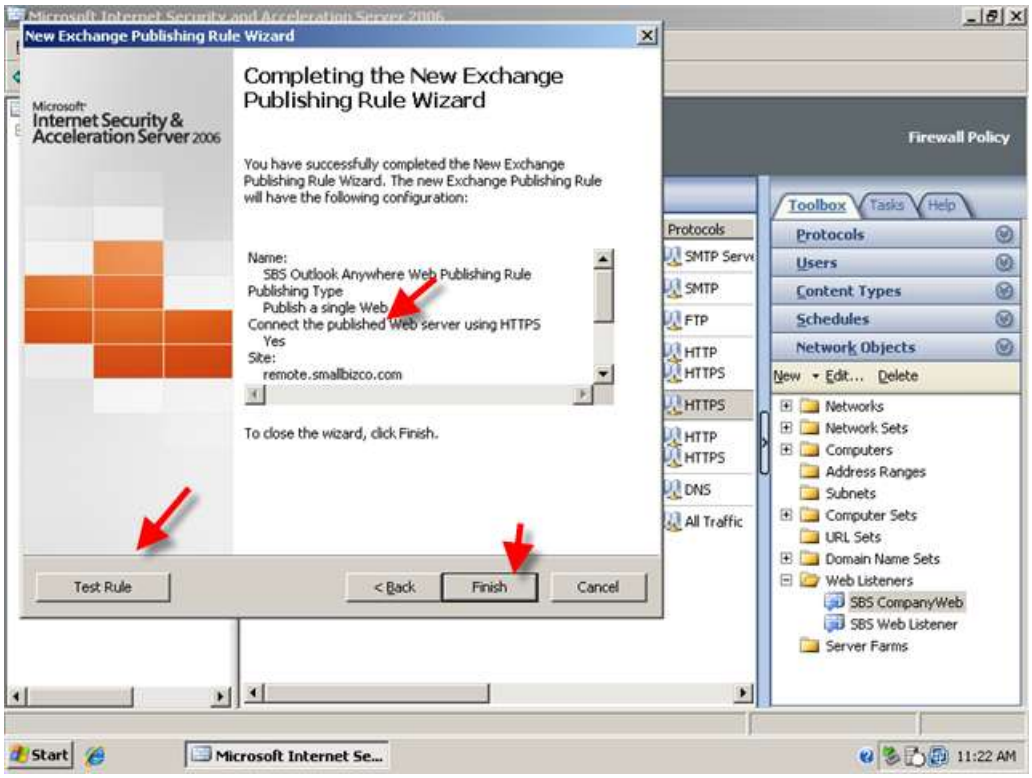
9. On the authentication delegation page, select NTLM from the drop down menu. Click Next.



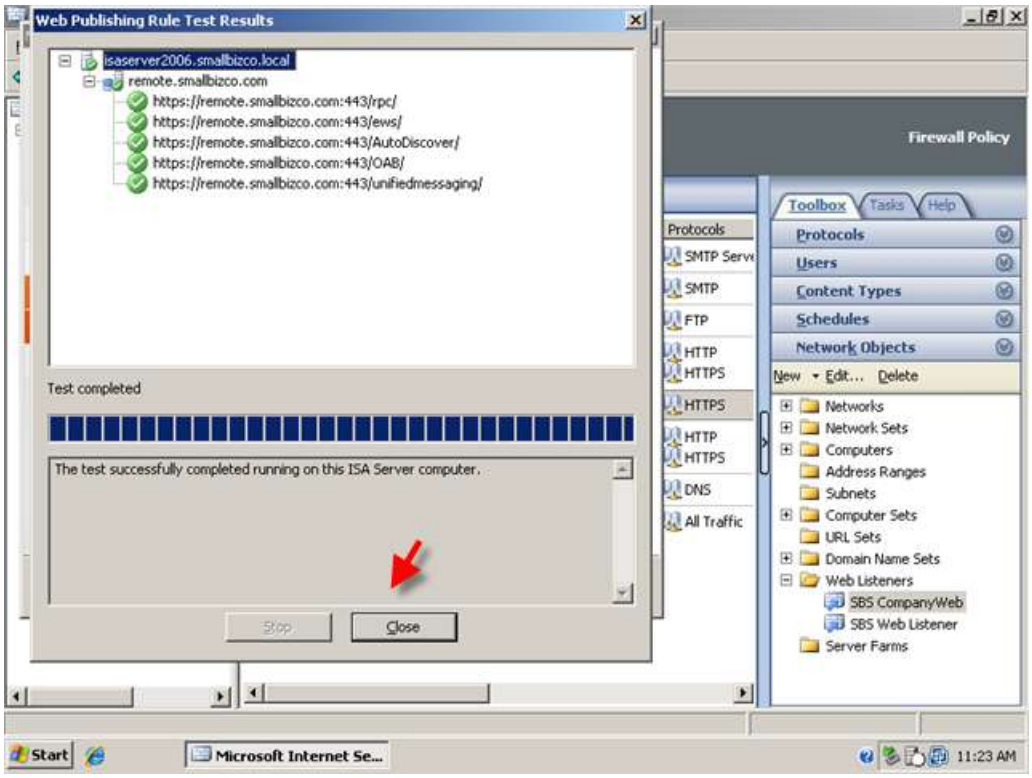
10. Leave the default 'All Authenticated Users' and click Next.



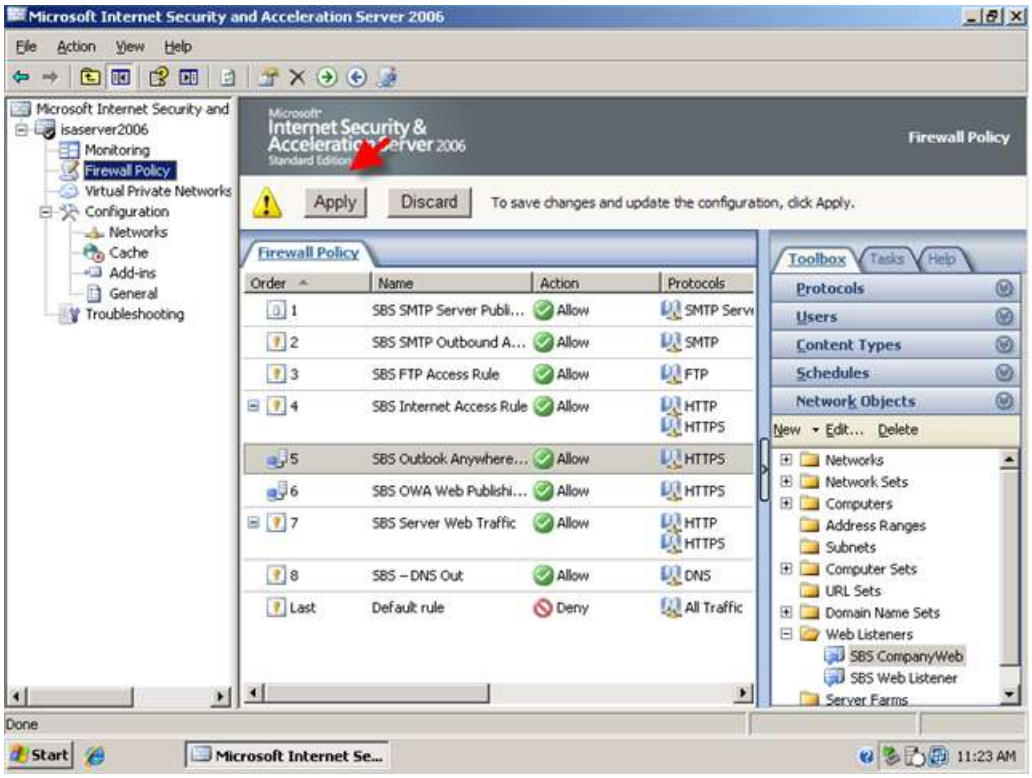
11. Click Test Rule, to check your rule settings. Click Close when the test has finished.



12. Click Finish when you are happy with your rule.

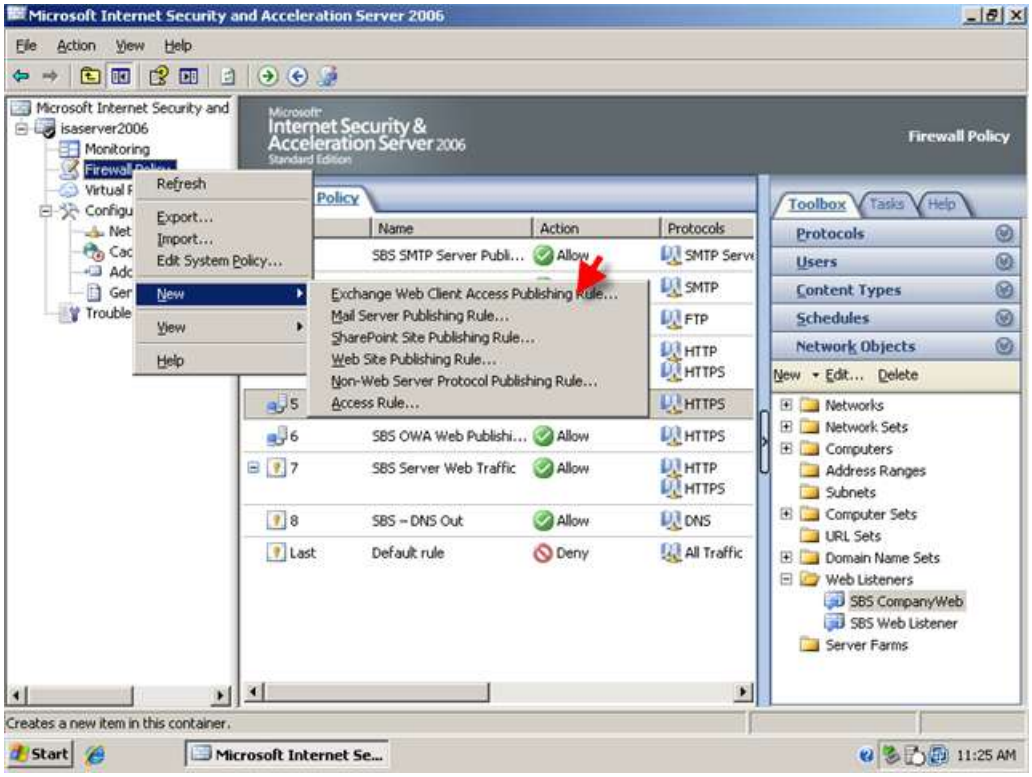


13. Click Apply to accept these configuration changes.

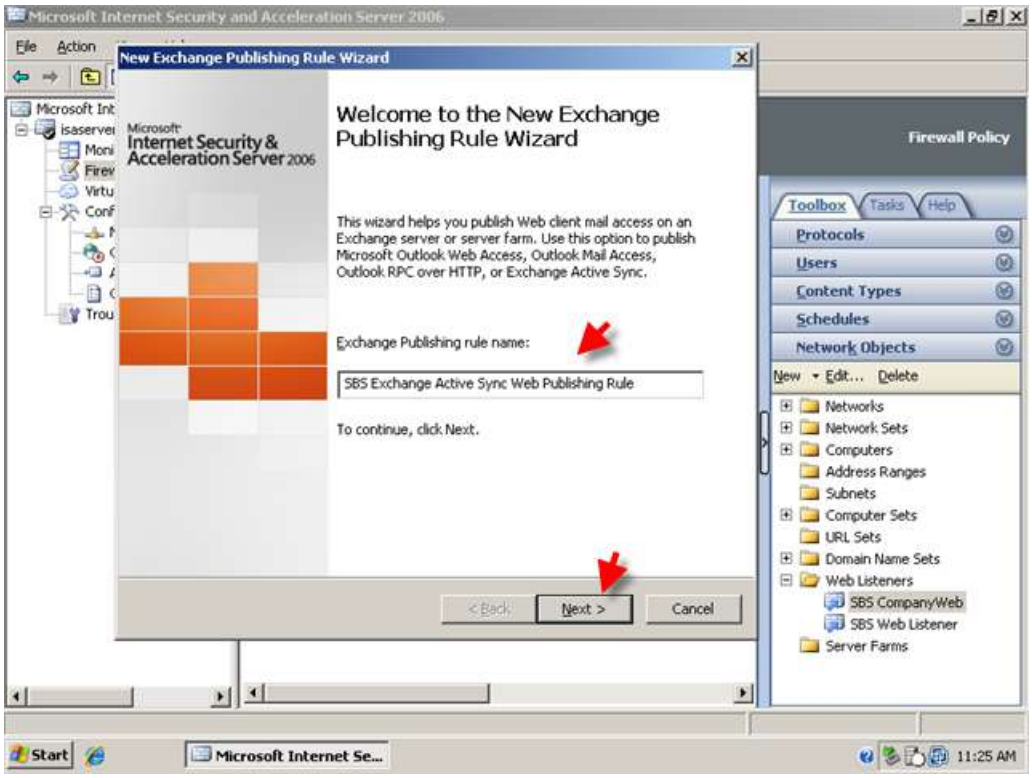


Creating a Web Publishing Rule For Microsoft Exchange Server 2007 Active sync

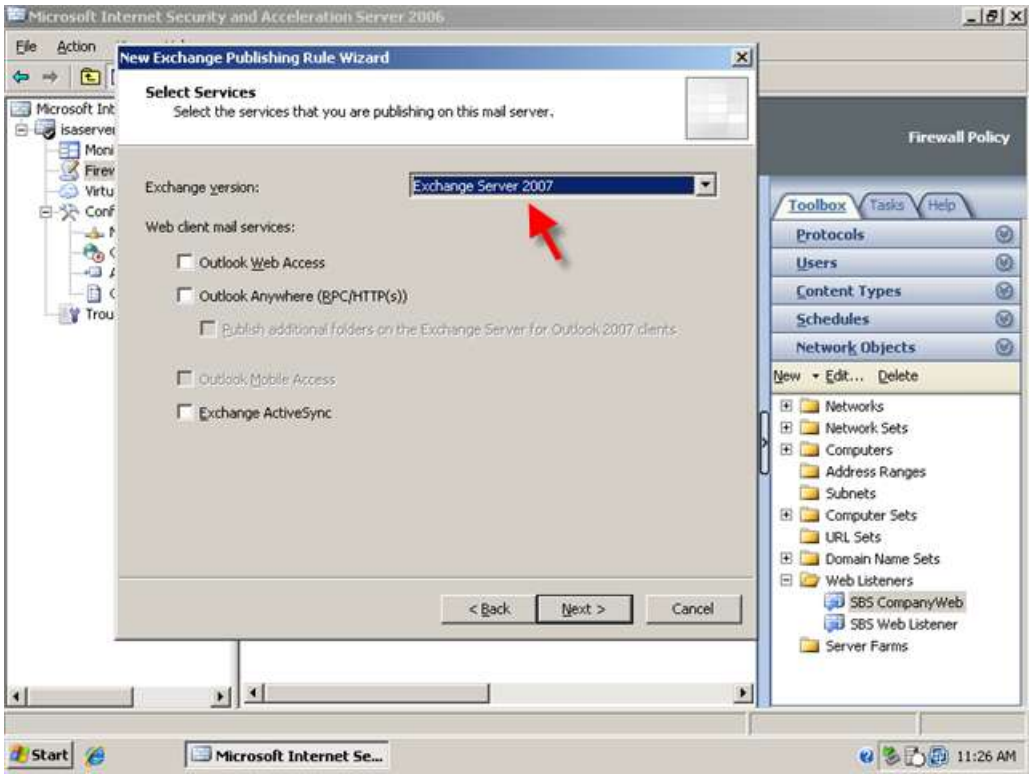
1. To create a rule for Exchange Active Sync Right click Firewall Policy click New . Exchange Web Client Publishing Rule.



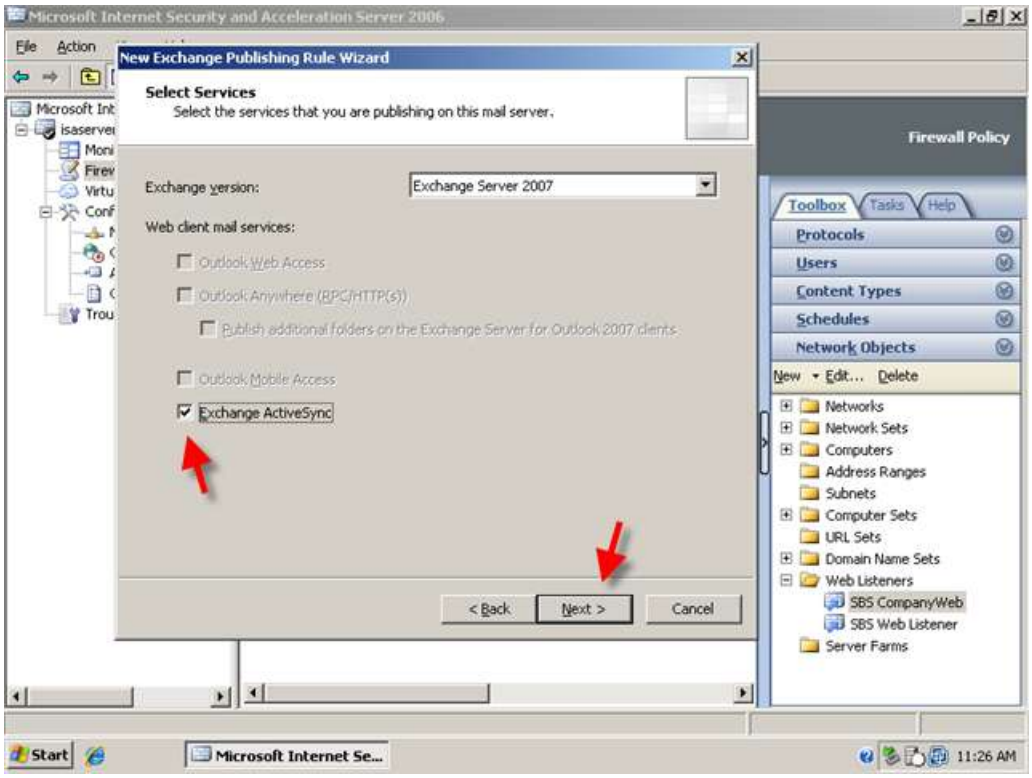
2. Name your rule, I am using the name SBS Exchange Active Sync Web Publishing Rule, click Next.



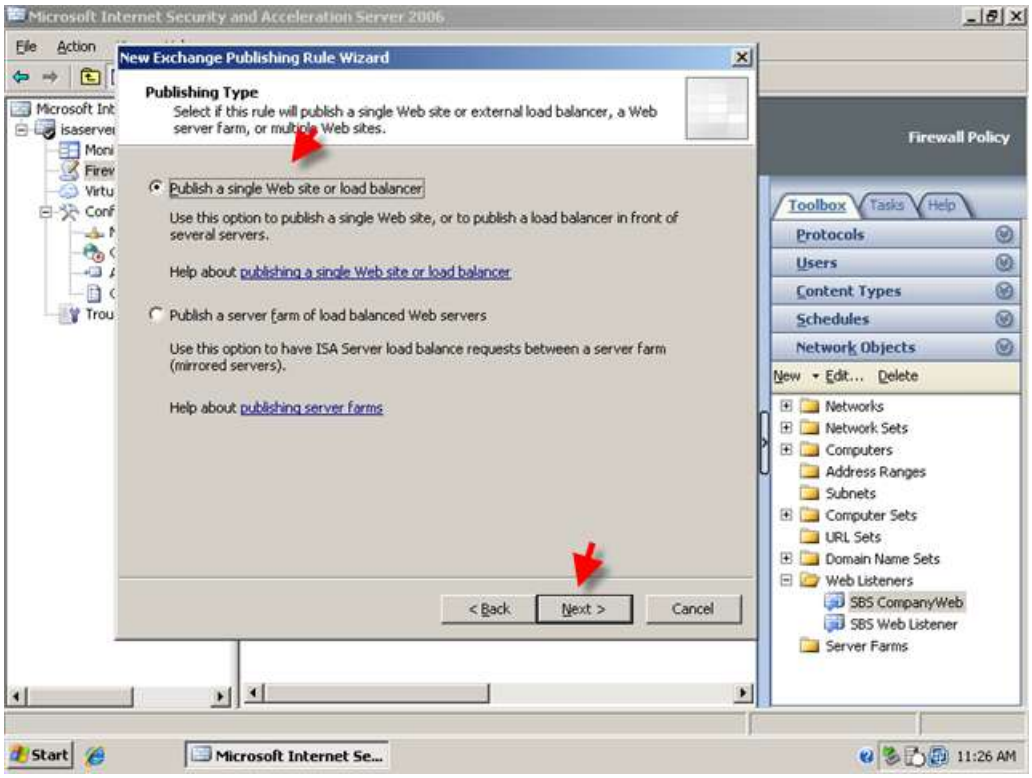
3. Choose Exchange 2007 from the dropdown list.



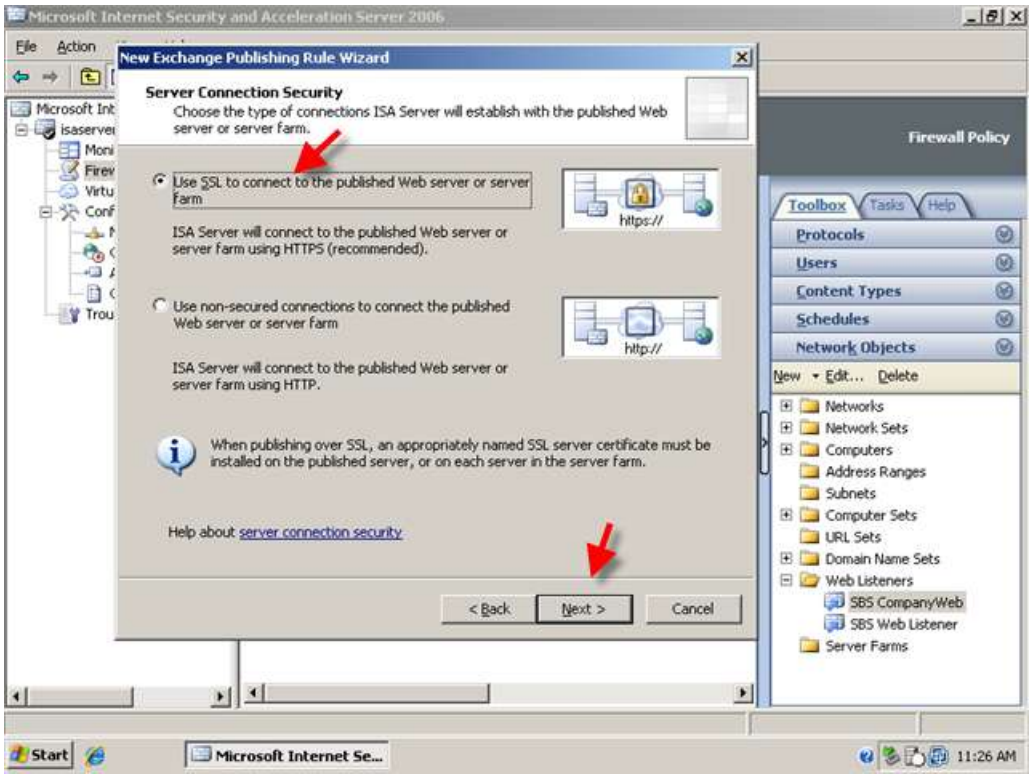
4. Select the Exchange Active Sync check box. Click Next.



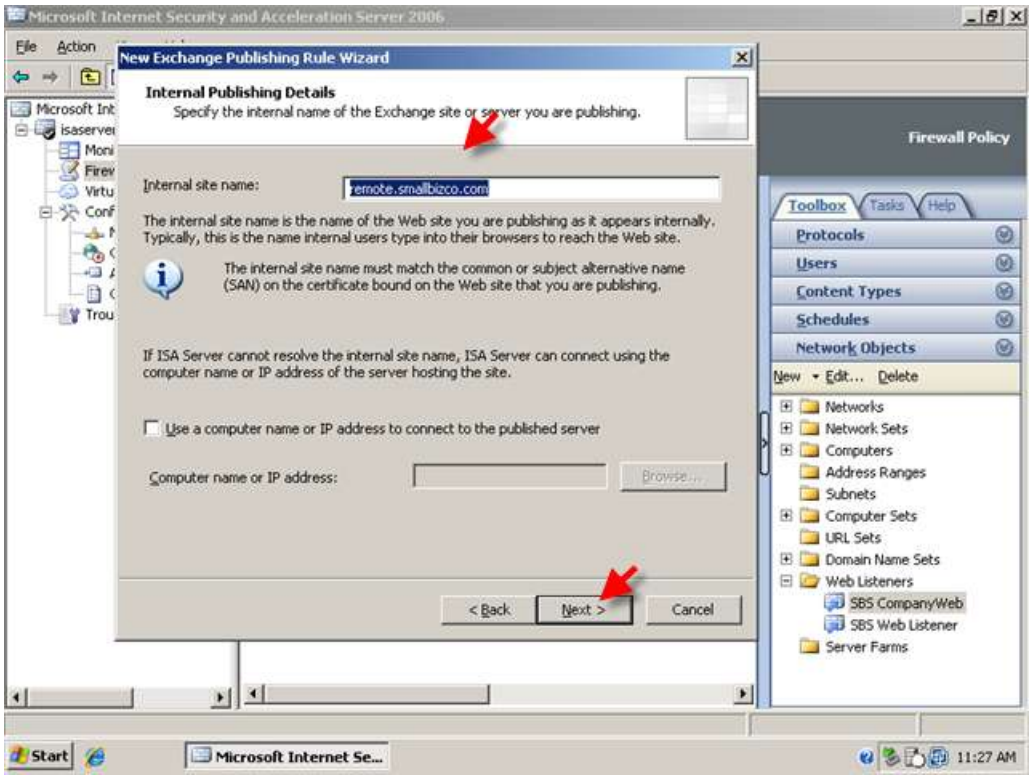
5. Click Next to accept the default 'Publish Single Website or Load Balancer'



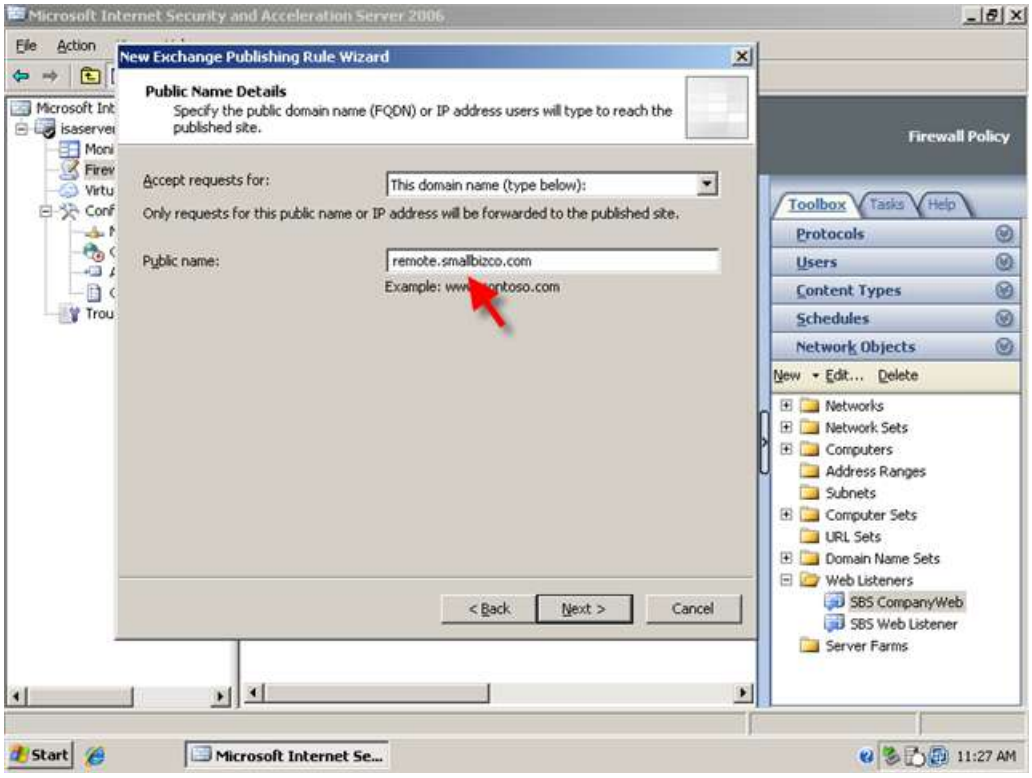
6. Click Next to accept the default 'Use SSL to connect ot he published web Server'



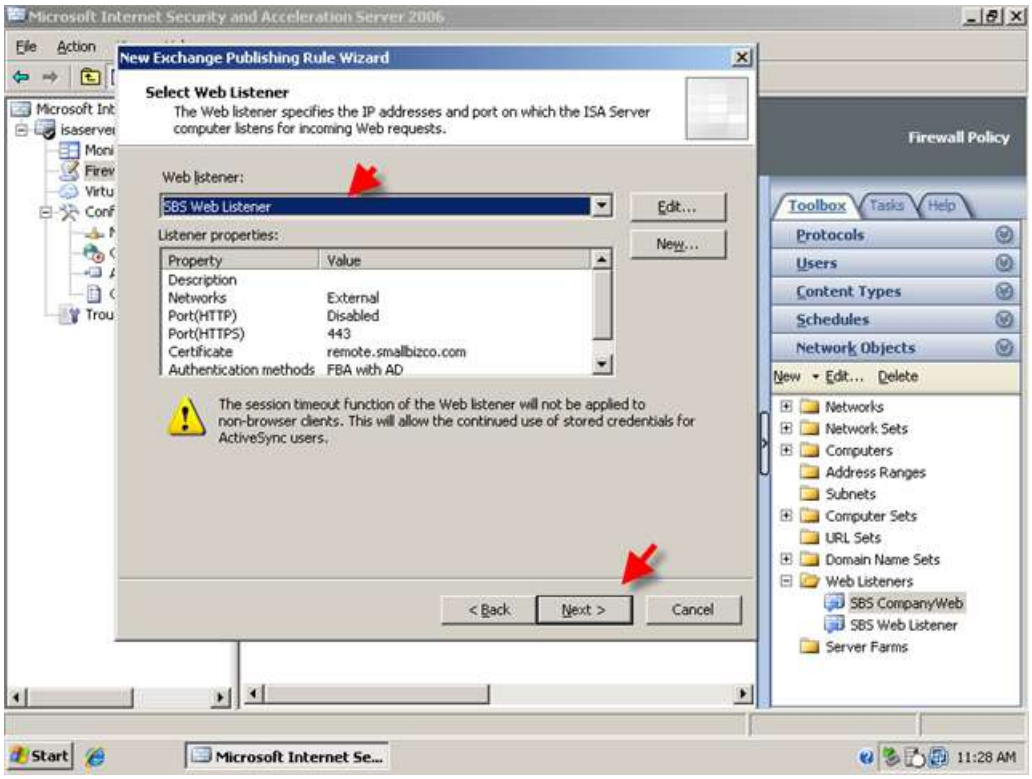
7. On the internal site name page enter 'remote.domain.com' (where remote.domain.com is your public DNS name) Click Next.



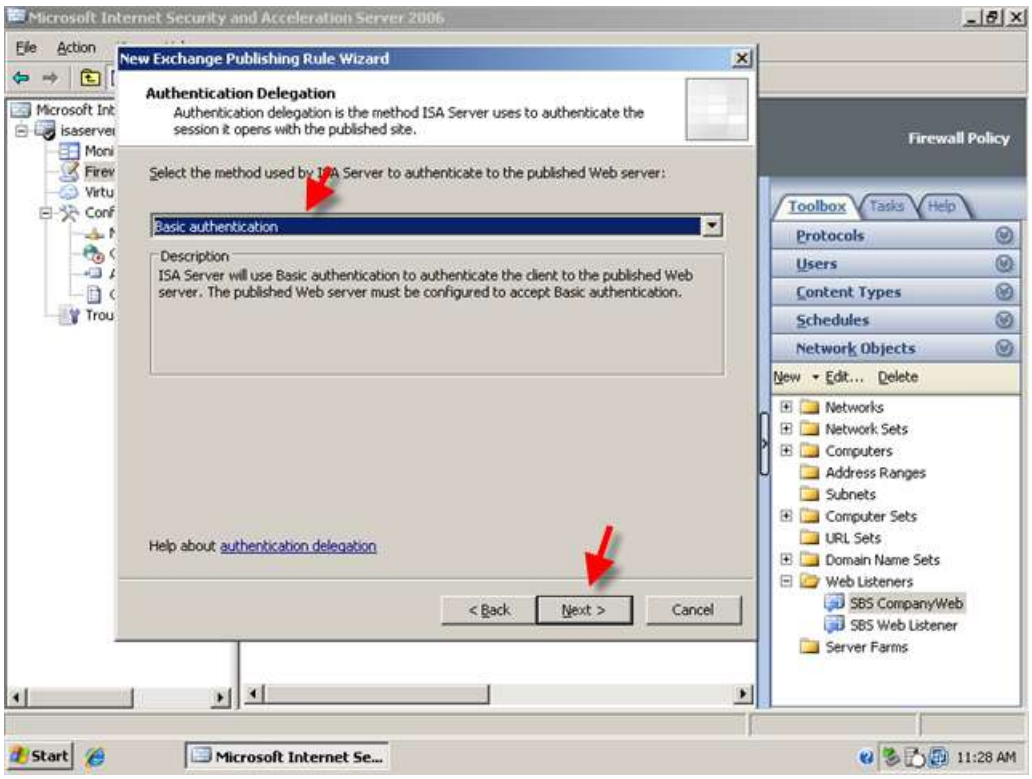
8. On the public name details page enter 'remote.domain.com' (where remote.domain.com is your public DNS name) Click Next.



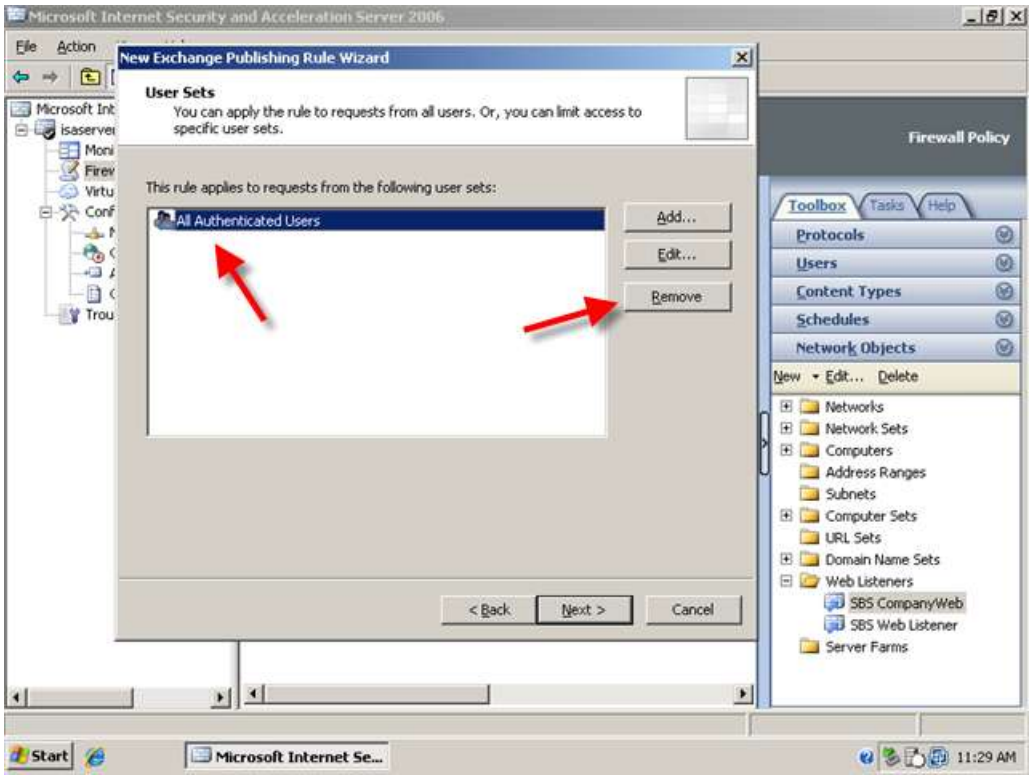
9. On the Web Listener page, select your SBS Web Listener from the drop down menu. Take note of the Message displayed regarding session timeout. Click Next

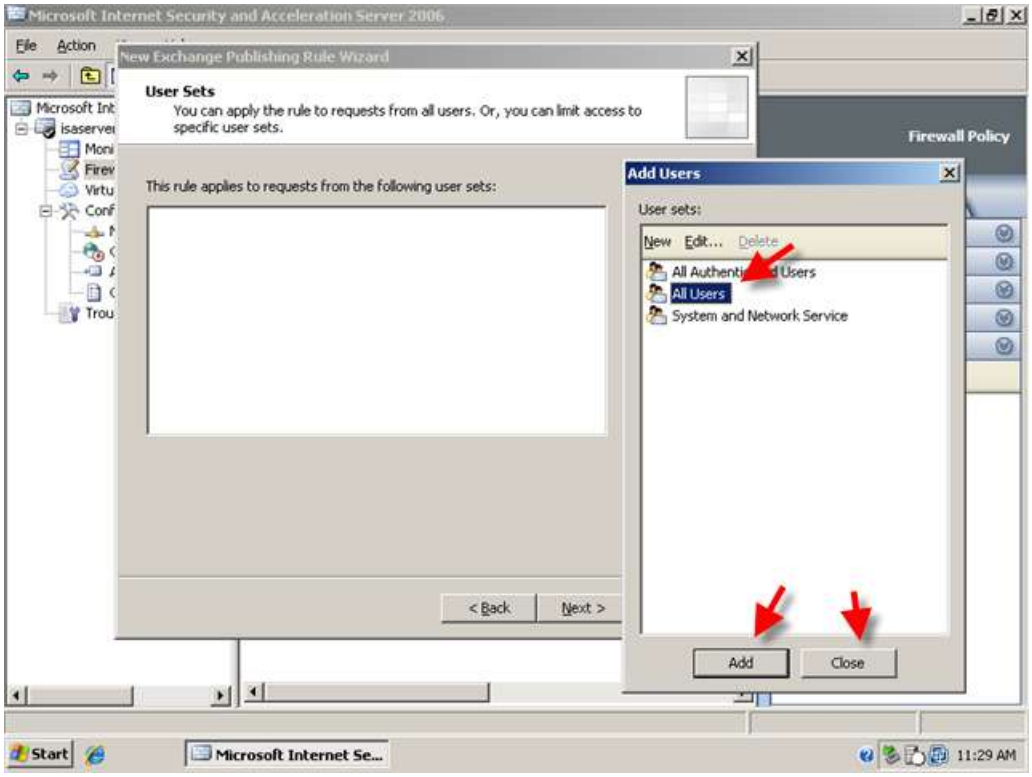


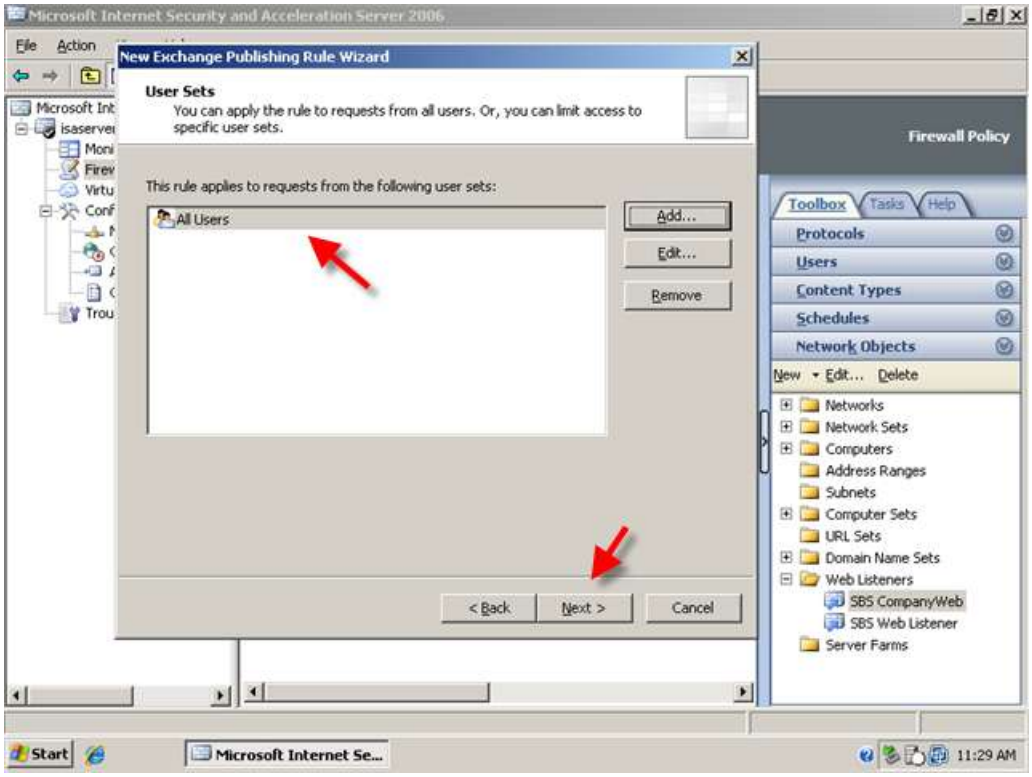
10. On the Authentication delegation page, select Basic from the drop down menu. Click Next.

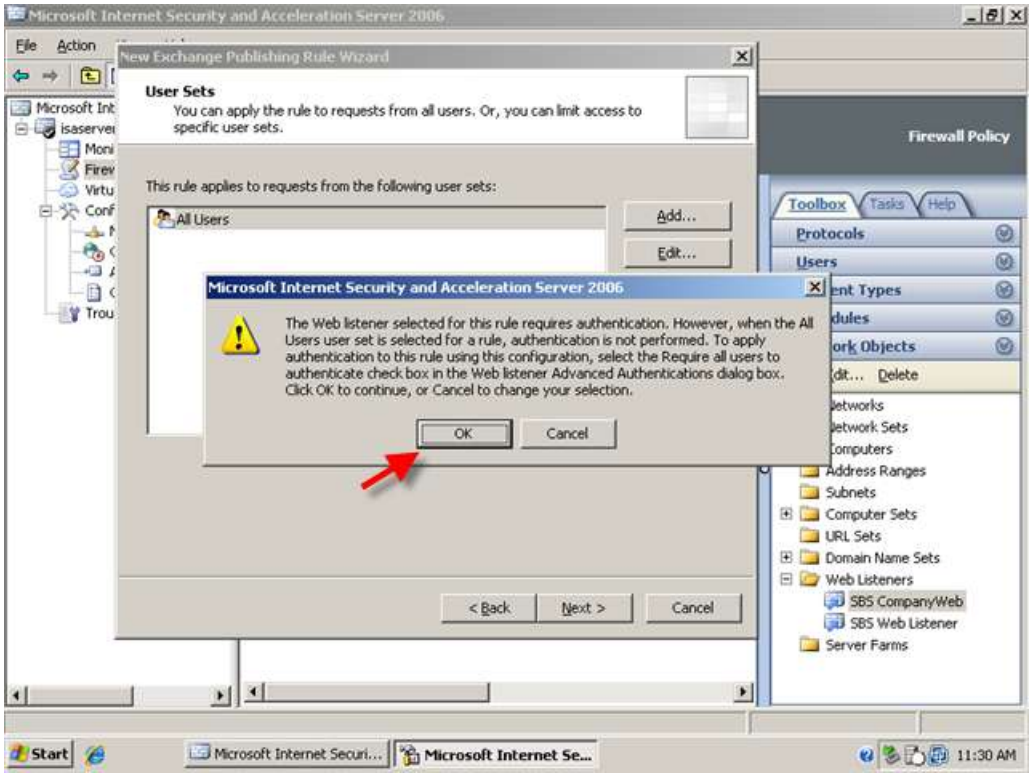


11. On the User select 'All Authenticated users, and click Remove. Click Add and select All Users, Click Add then click Close. Click Next. Acknowledge the Warning regarding authentication by clicking OK.

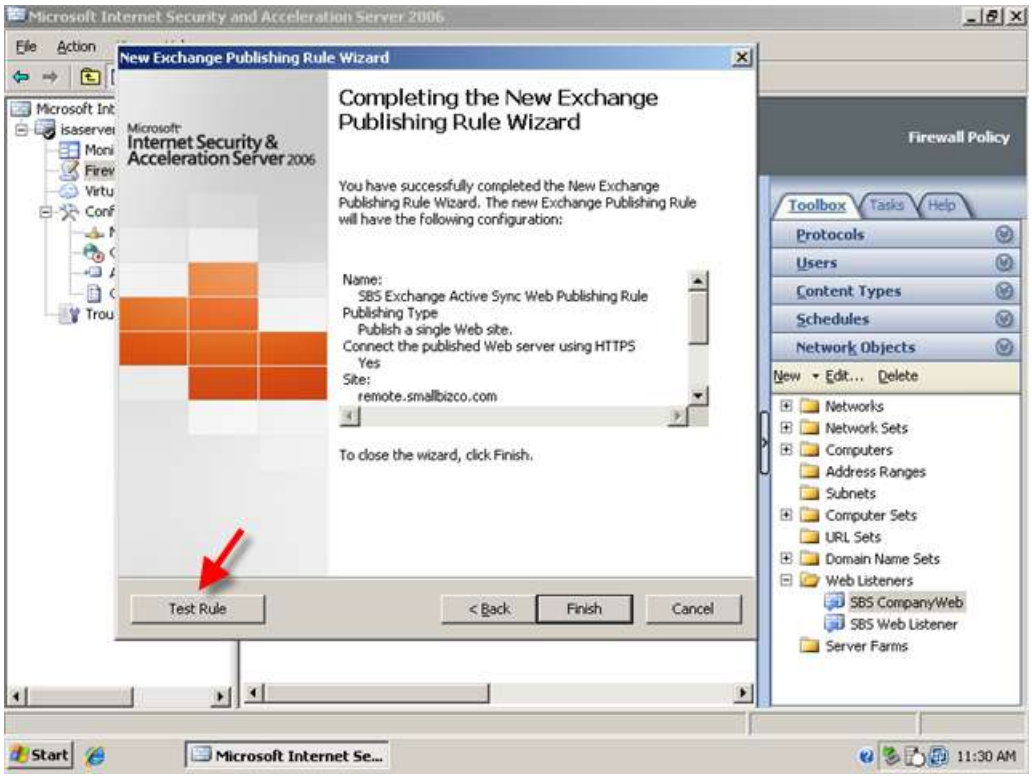


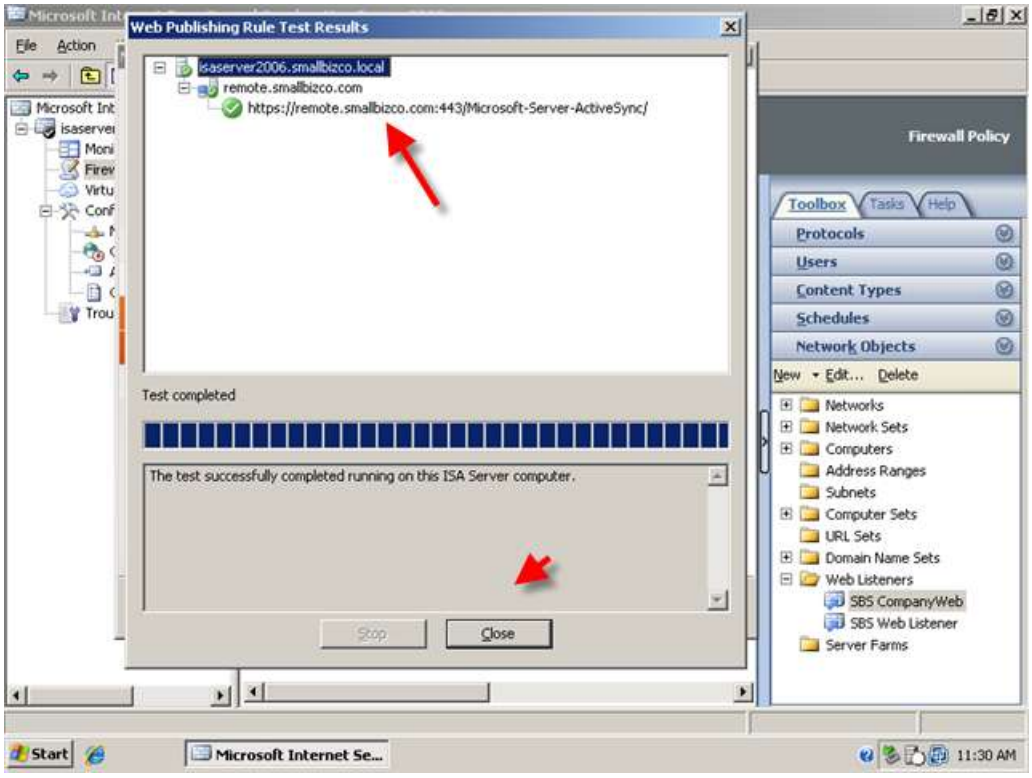



Microsoft Internet Security and Acceleration Server 2006
File Action
New Exchange Publishing Rule Wizard
User Sets
You can apply the rule to requests from all users. Or, you can limit access to specific user sets.
This rule applies to requests from the following user sets:
All Users
Add...
Edit...
Remove
< Back
Next >
Cancel
Firewall Policy
Toolbox
Tasks
Help
Protocols
Users
Content Types
Schedules
Network Objects
New
Edit...
Delete
Networks
Network Sets
Computers
Address Ranges
Subnets
Computer Sets
URL Sets
Domain Name Sets
Web Listeners
SBS CompanyWeb
SBS Web Listener
Server Farms
Start
Microsoft Internet Se...
11:29 AM

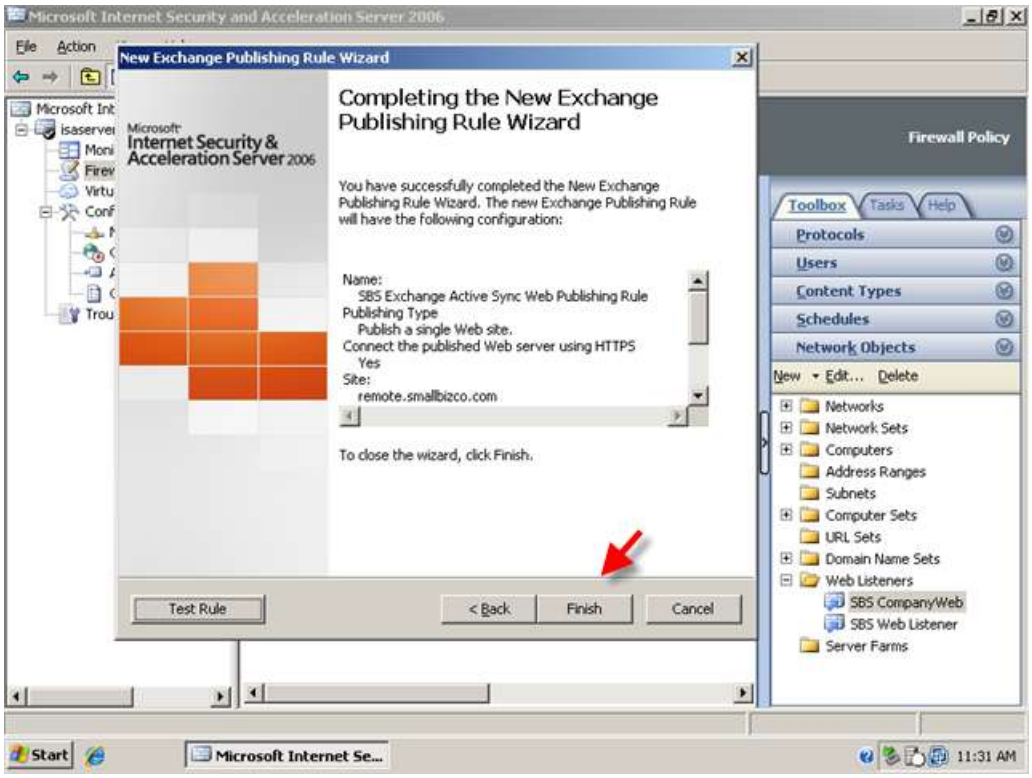

Microsoft Internet Security and Acceleration Server 2006
File Action
New Exchange Publishing Rule Wizard
User Sets
You can apply the rule to requests from all users. Or, you can limit access to specific user sets.
This rule applies to requests from the following user sets:
All Users
Add...
Edit...
Microsoft Internet Security and Acceleration Server 2006
The Web listener selected for this rule requires authentication. However, when the All Users user set is selected for a rule, authentication is not performed. To apply authentication to this rule using this configuration, select the Require all users to authenticate check box in the Web listener Advanced Authentications dialog box. Click OK to continue, or Cancel to change your selection.
OK
Cancel
< Back
Next >
Cancel
Firewall Policy
Toolbox
Tasks
Help
Protocols
Users
Address Ranges
Subnets
Computer Sets
URL Sets
Domain Name Sets
Web Listeners
SBS CompanyWeb
SBS Web Listener
Server Farms
Start
Microsoft Internet Se...
11:30 AM

12. Click Test Rule, to check your rule settings. Click Close when the test has finished.

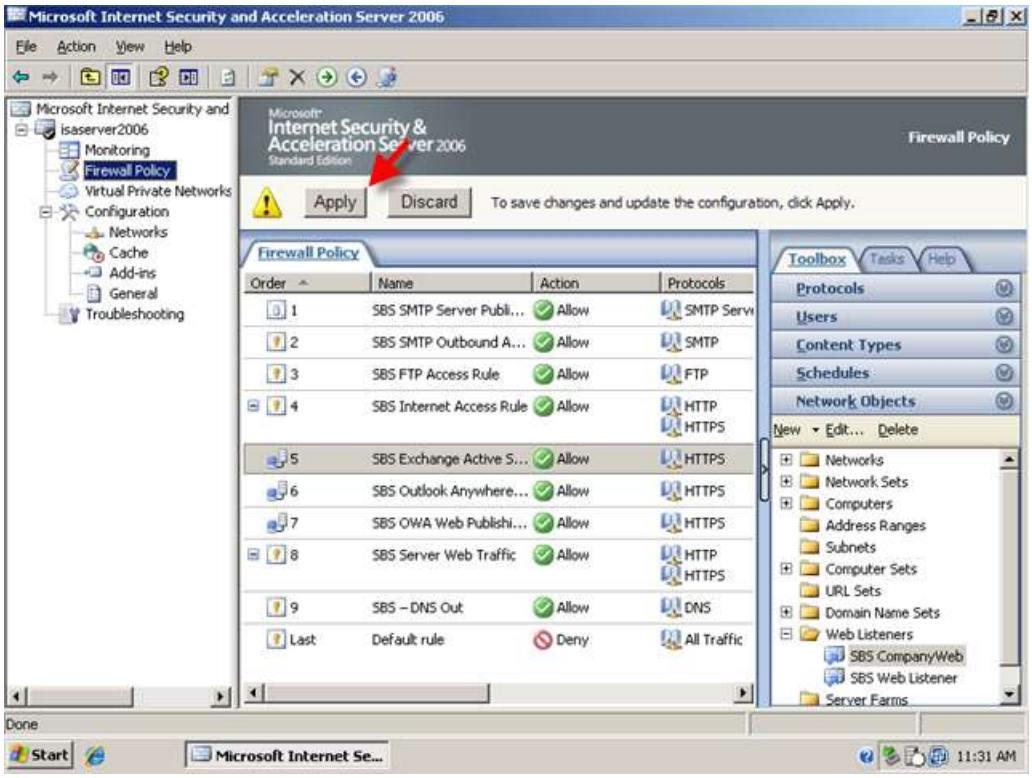




13. Click Finish when you are happy with your rule.



14. Click Apply to accept these configuration changes.

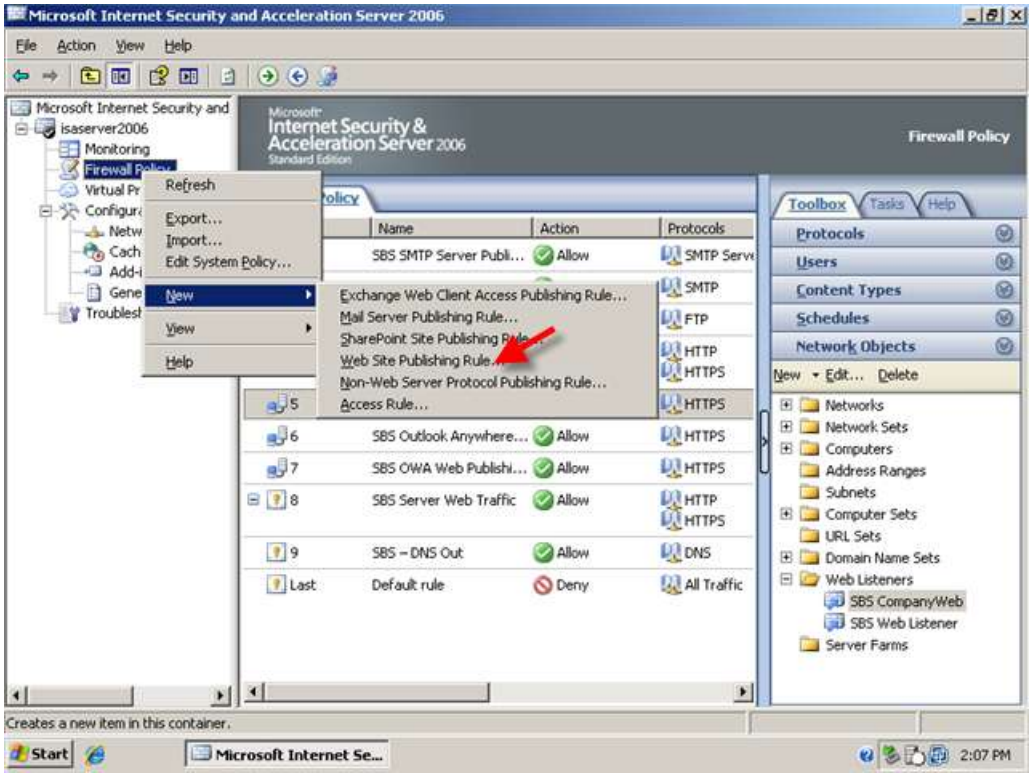


To configure your Outlook Client to connect to your SBS Server using Outlook Anywhere, follow the steps in the following article :
http://www.smallbizserver.net/Articles/tabid/266/articleType/ArticleView/ArticleID/101/PageID/146/Default.aspx

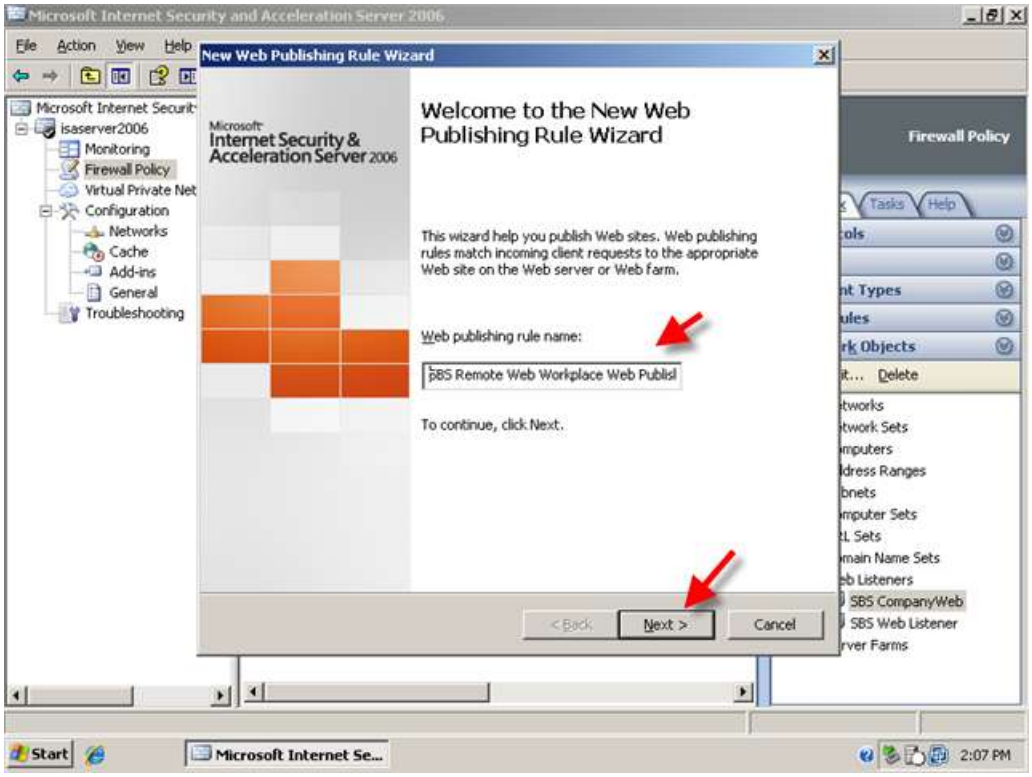
You can customize the ISA Server Forms displayed to your Outlook Web Access clients – this is a new feature of web publishing rules with ISA Server 2006. An excellent guide to this can be found here:
http://blog.msfirewall.org.uk/2008/11/customising-isa-server-2006-html-forms.html

Creating a Web Publishing Rule For Remote Web Workplace

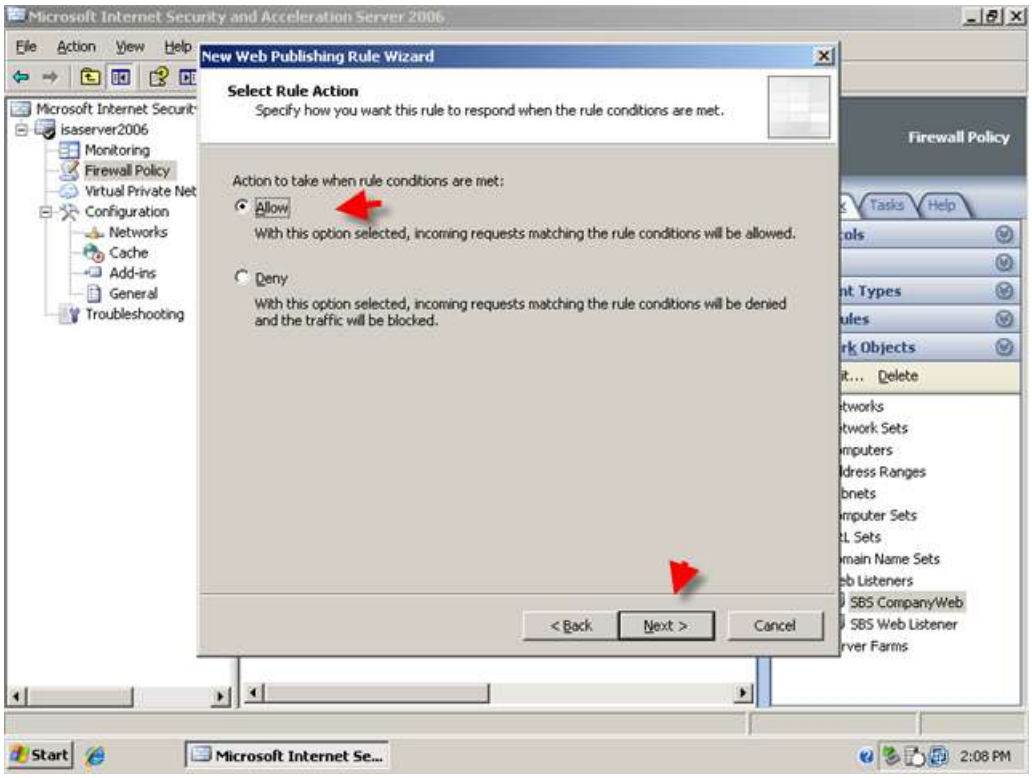
1. Creating the RWW Publishing Rule. On your ISA Server open ISA Server Management Right click the Firewall Policy and click New > Web Site Publishing Rule.



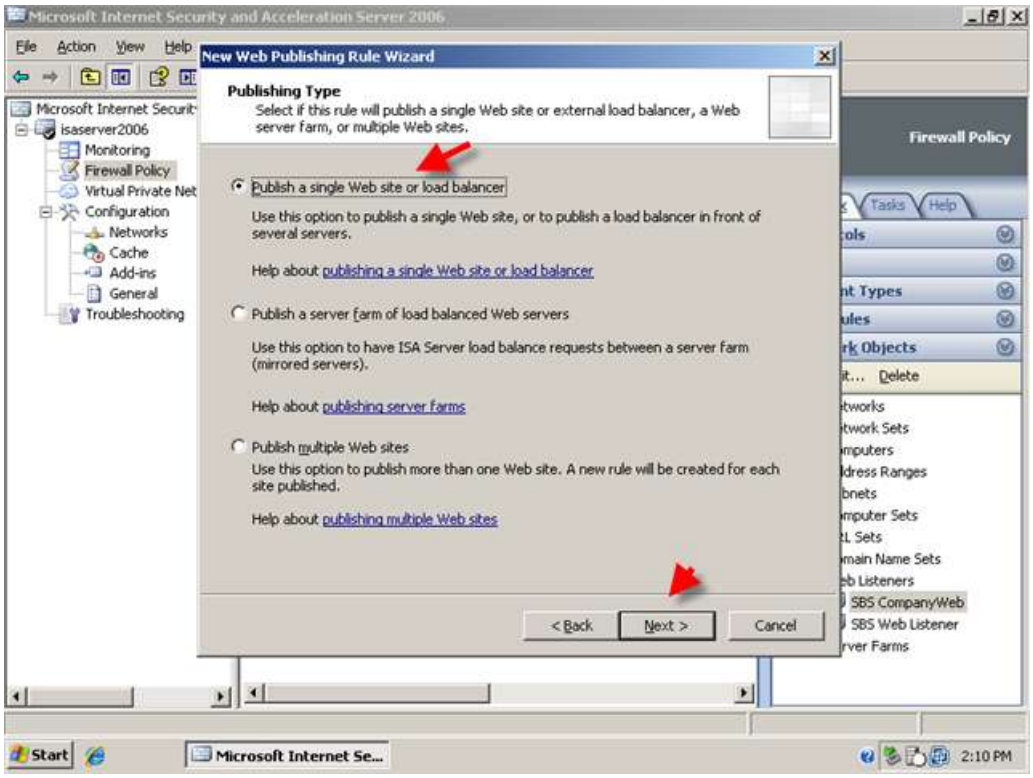
2. Enter a name for your rule, I am calling my rule SBS Remote Web Workplace Web Publishing Rule, click Next.



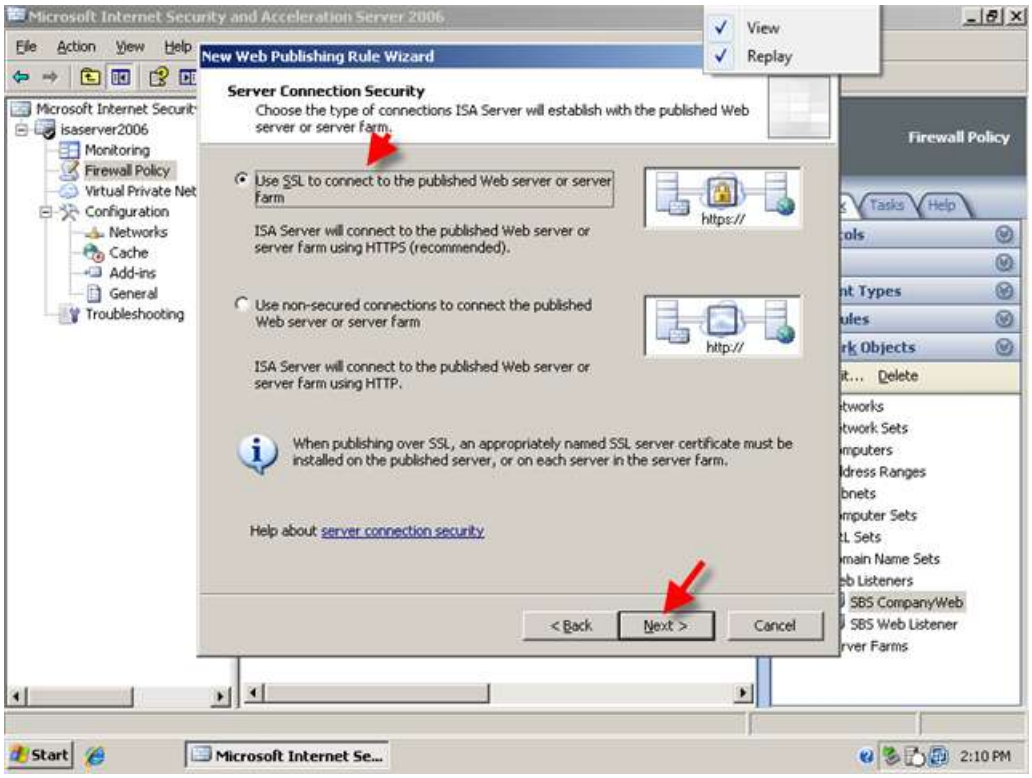
3. Set the rule to Allow, and click Next.



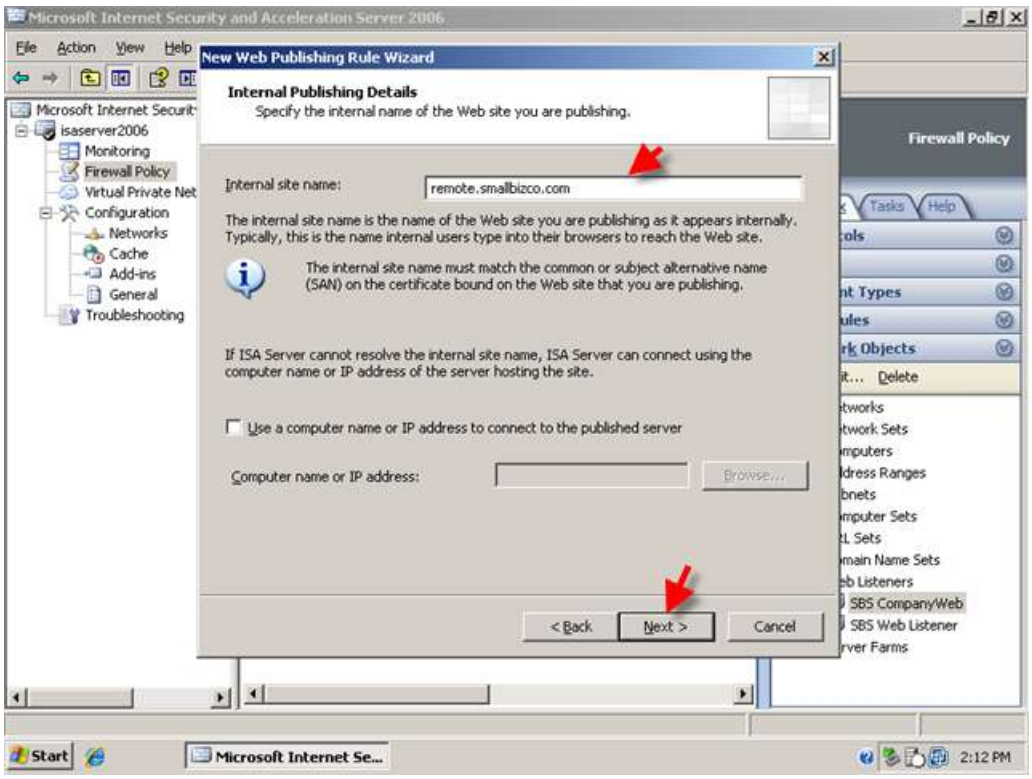
4. Accept the default for publishing a single web site or load balancer and click Next.



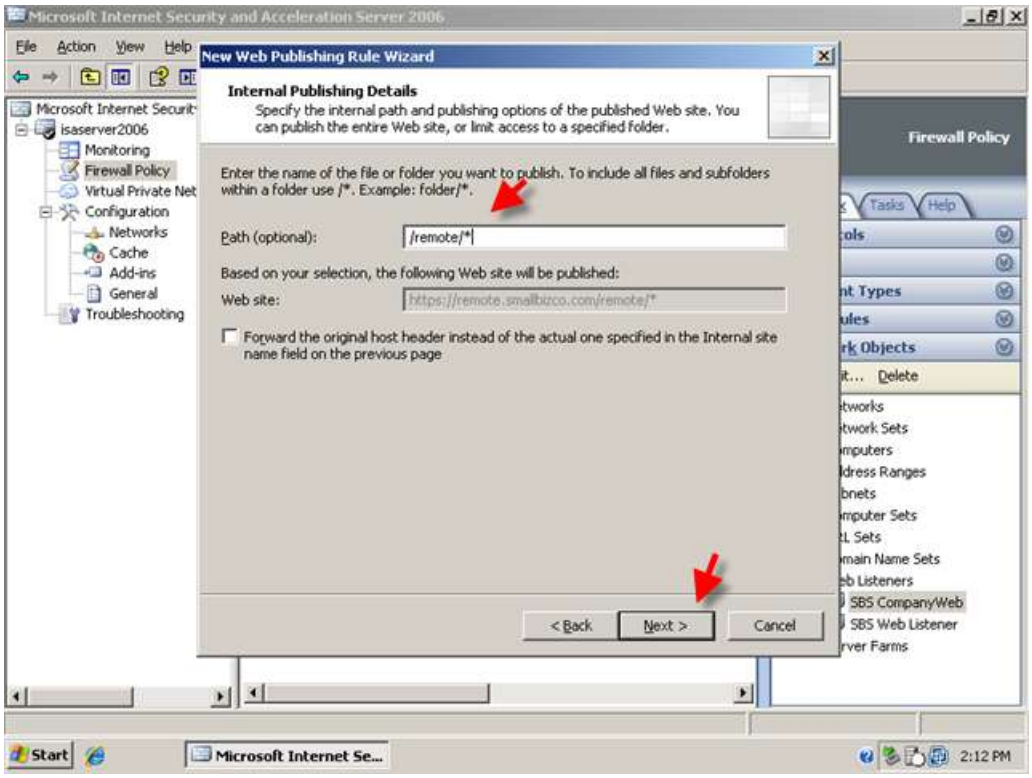
5. Accept the default to use SSL to connect to the published web server.



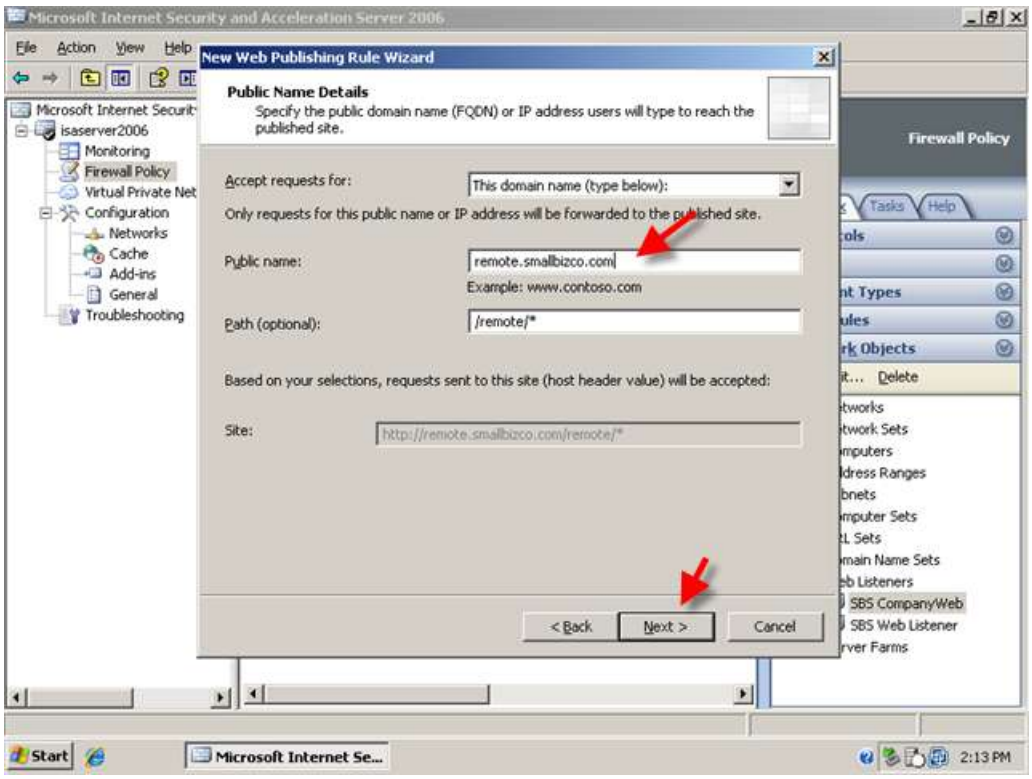
6. On the internal site name page, enter 'remote.smallbizco.com' (where remote.smallbizco.com is your public DNS name) and click next.



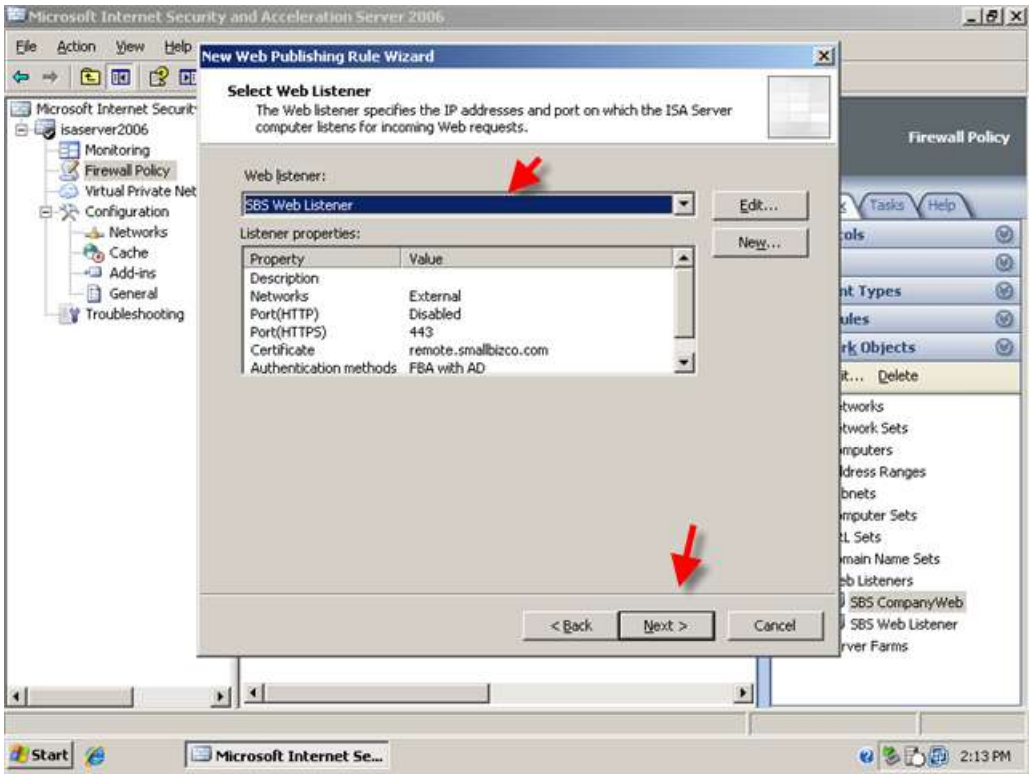
7. On the Path page, enter /remote/* and click next.



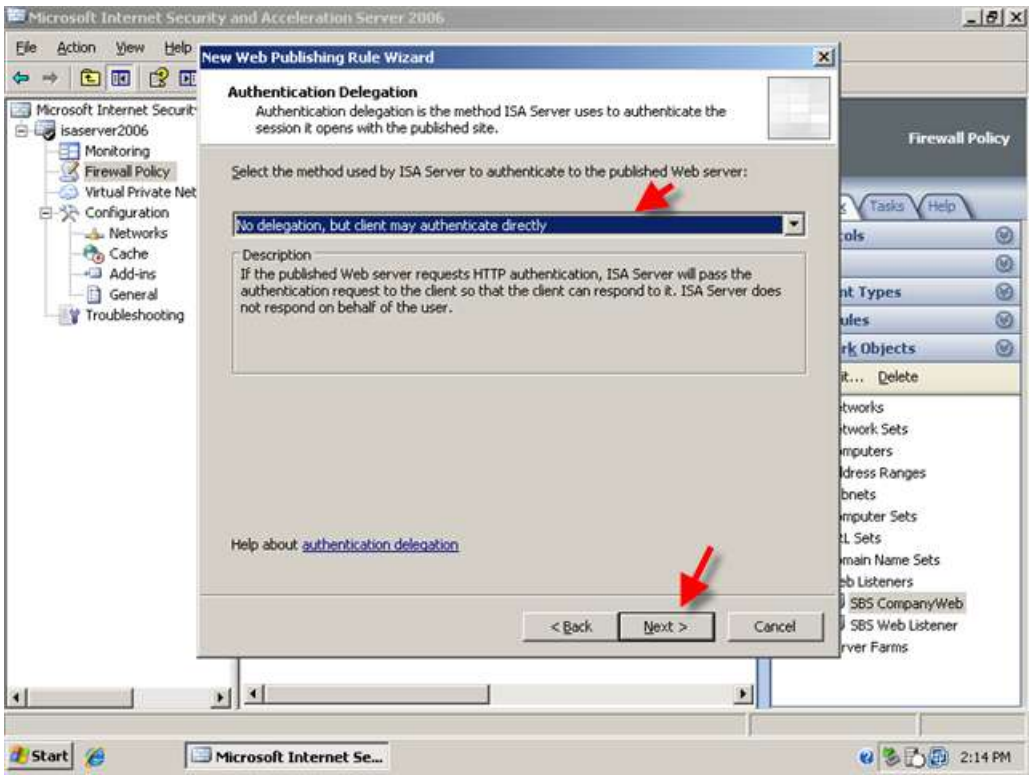
8. On the public name page, enter 'remote.domain.com' (where remote.domain.com is your public DNS name) and click next.



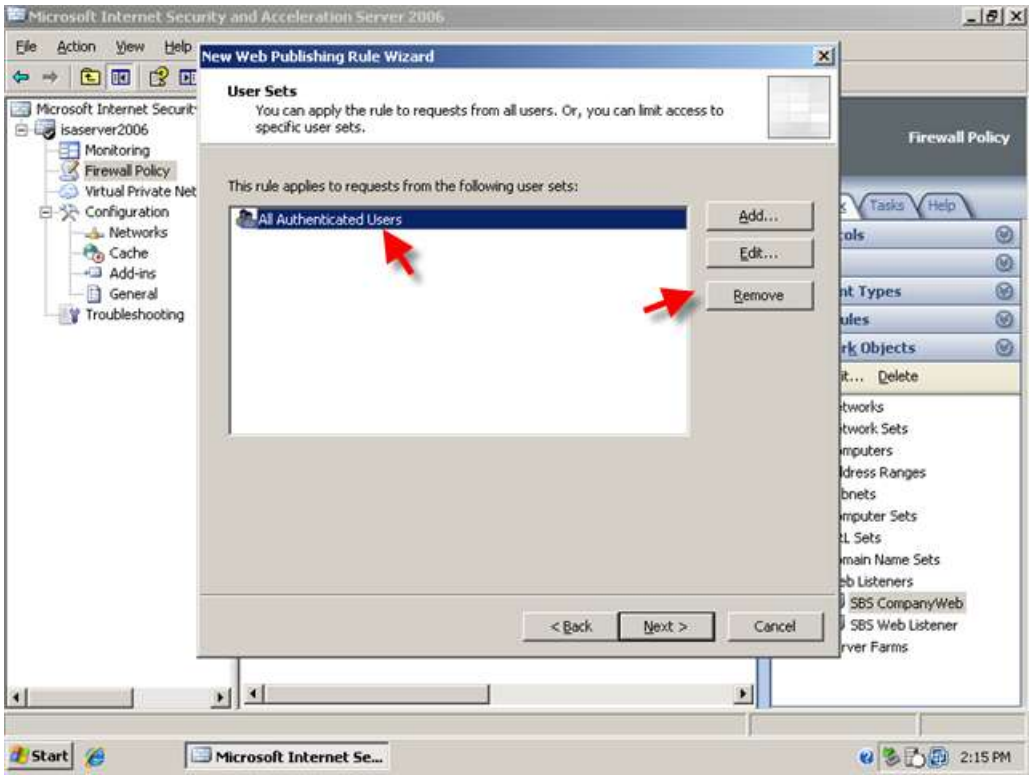
9. On the Web Listener page, select the SBS Web Listener, and click Next.

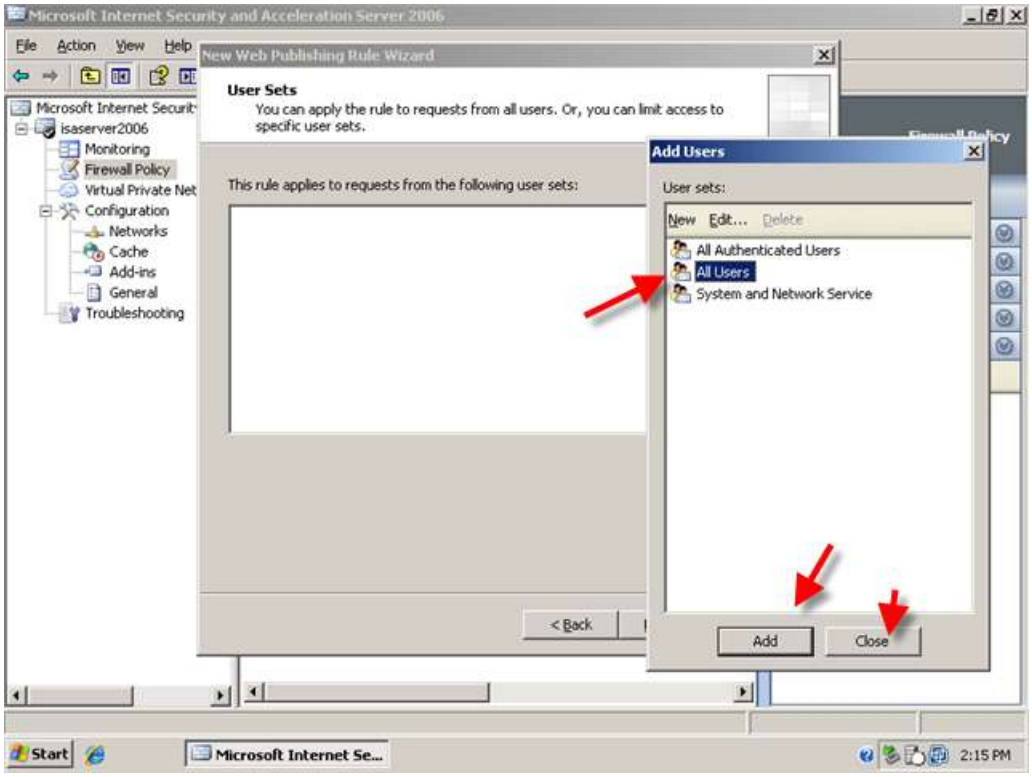


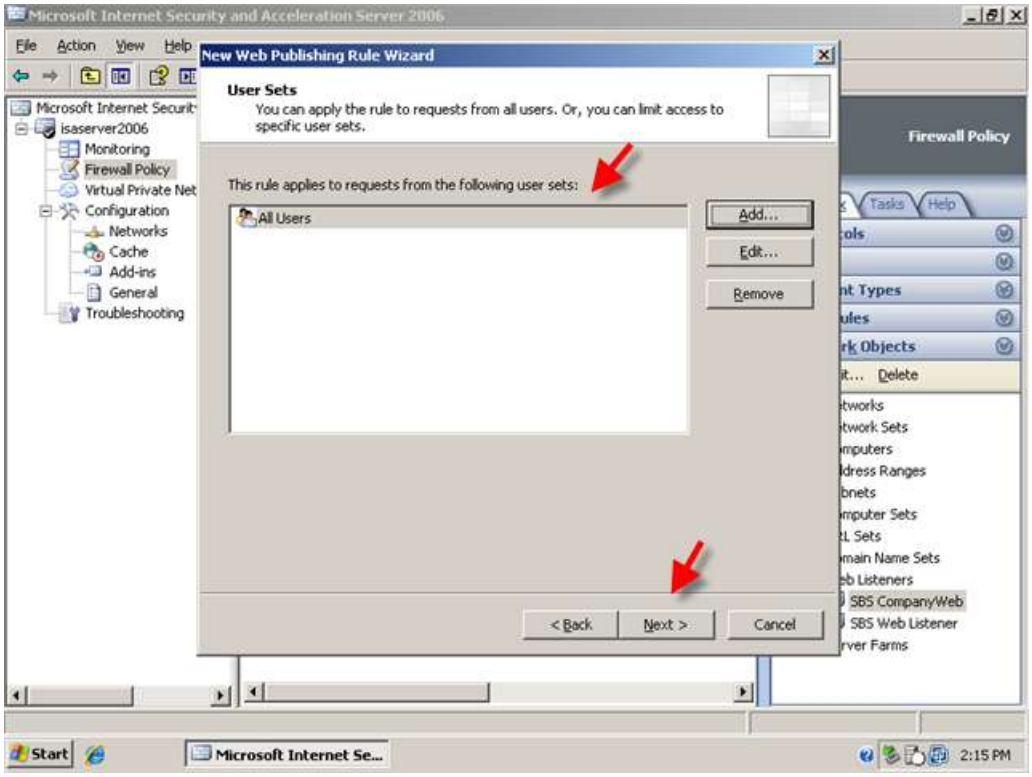
10. On The Authentication Delegation page, use the drop down menu to select, No Authentication Delegation but client may Authenticate directly, and click Next.



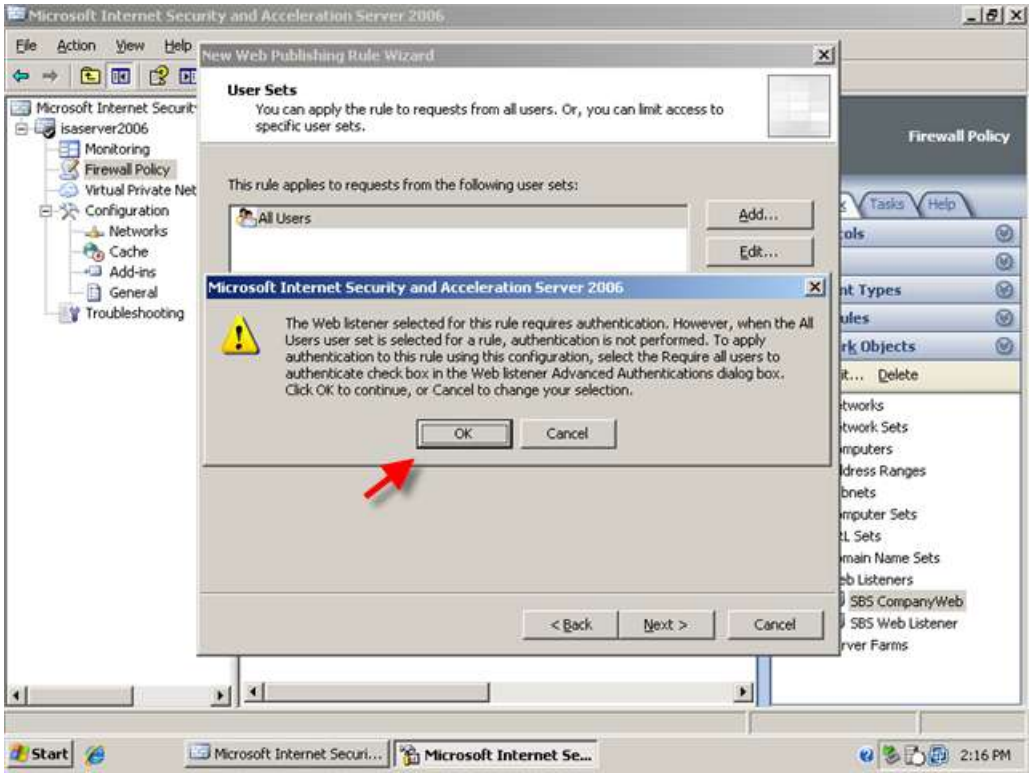
11. On the user sets page, select 'All Authenticated Users', and click remove then click Add. Select the All Users user set, then click Add. Click Close. The All users user set is displayed in the list, click next.



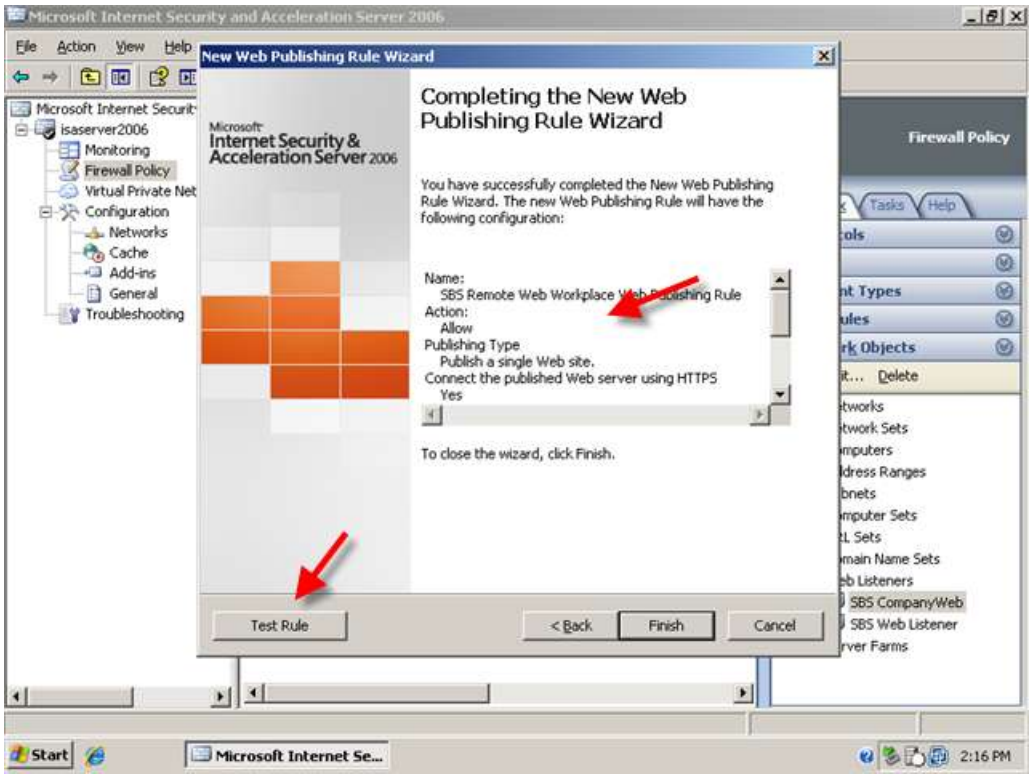


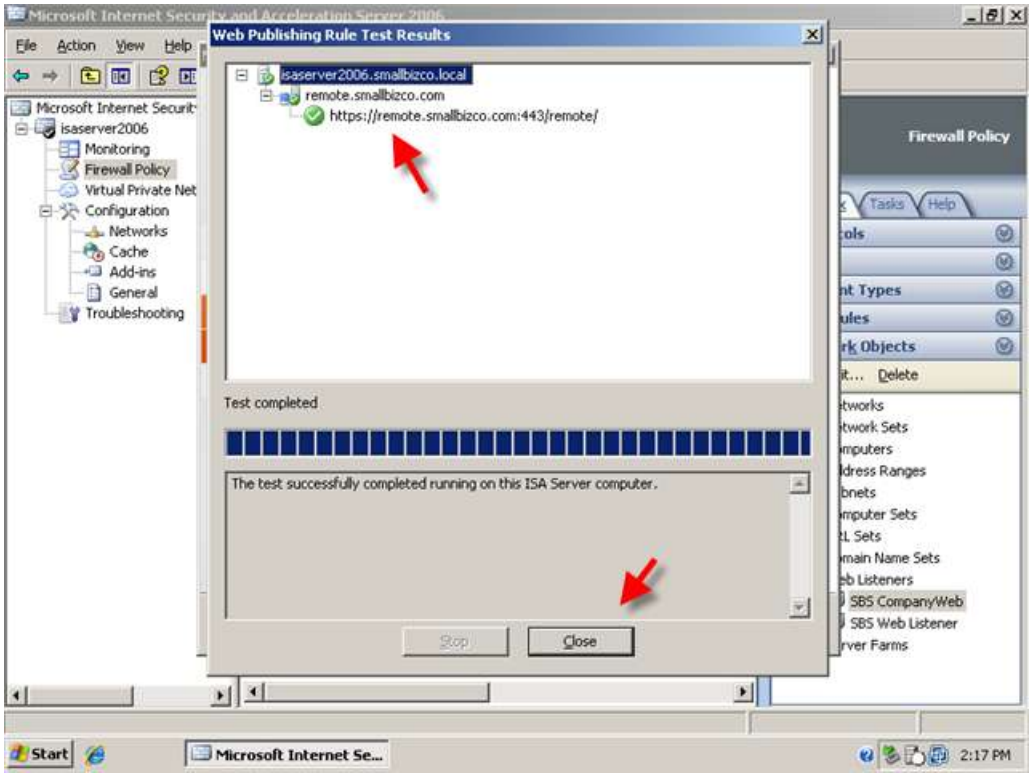


12. Accept the warning regarding authentication by clicking OK.

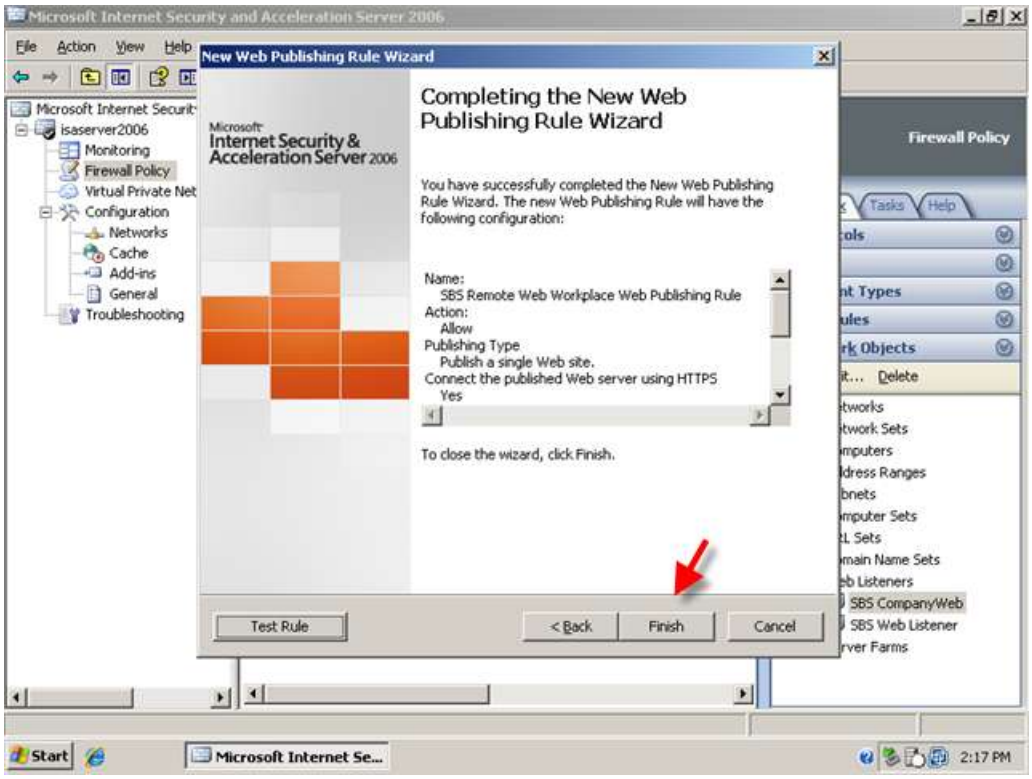


13. Review your rule settings, click Test Rule to test your settings.



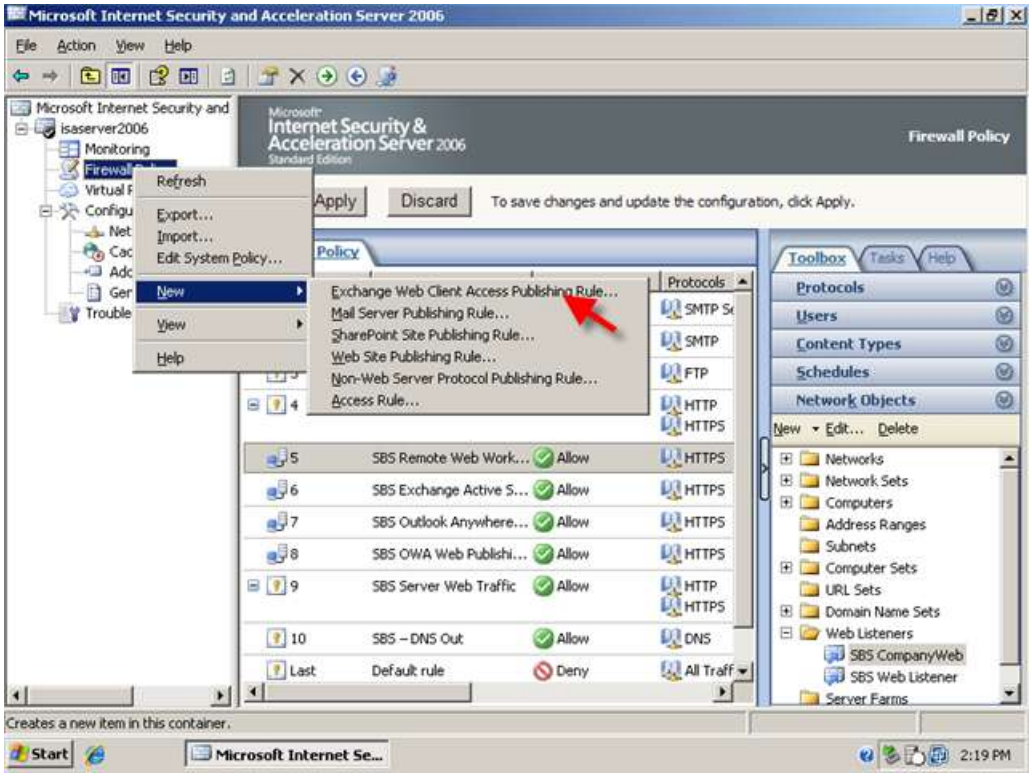


14. Click Close, then click Finish to save your rule to the Firewall Policy. We will add the RPC rule before we save our changes.

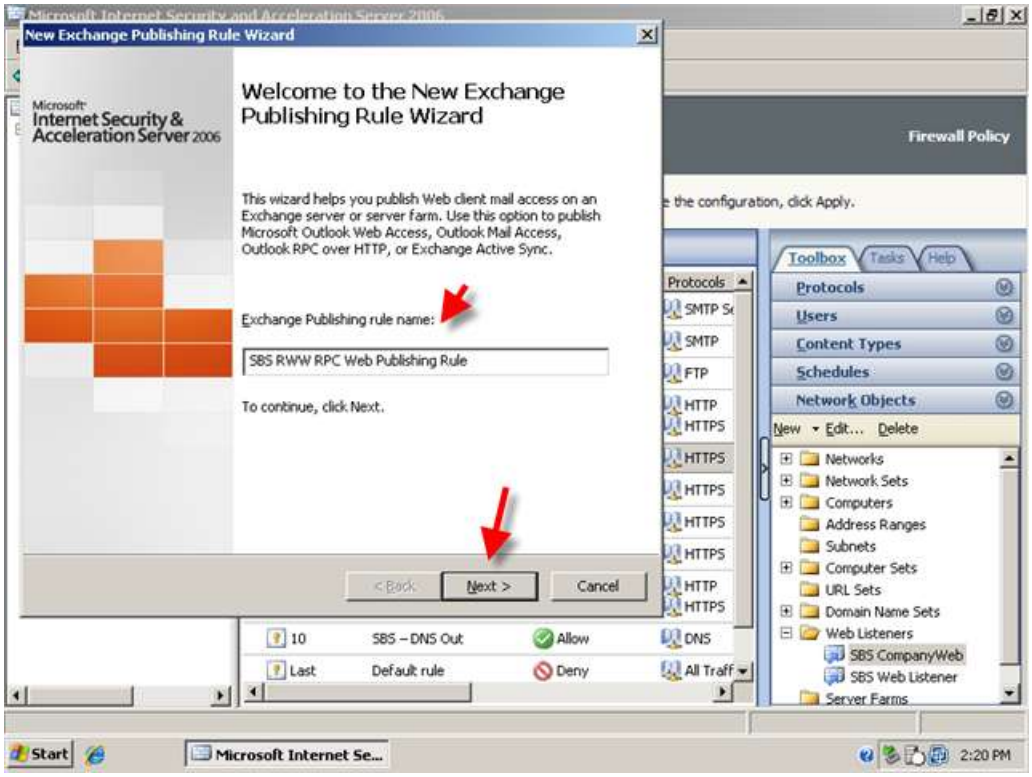


Creating a Web Publishing Rule For Remote Web Workplace RPC Traffic

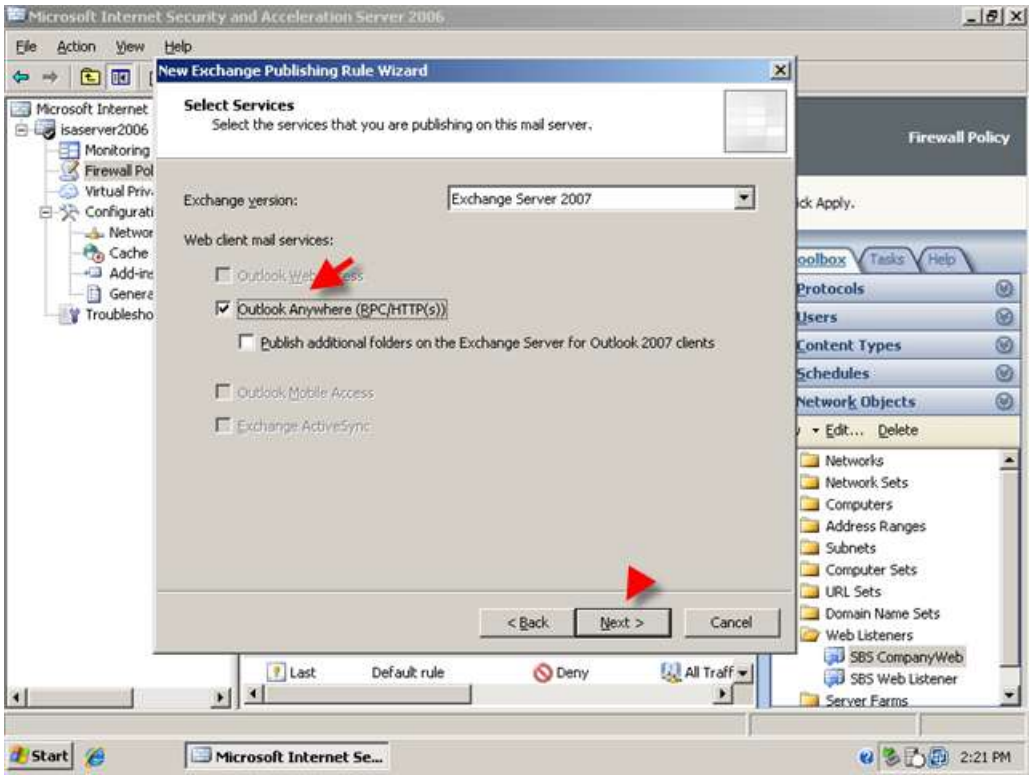
1. Right click the Firewall policy and click New > Exchange Web Client Publishing rule>



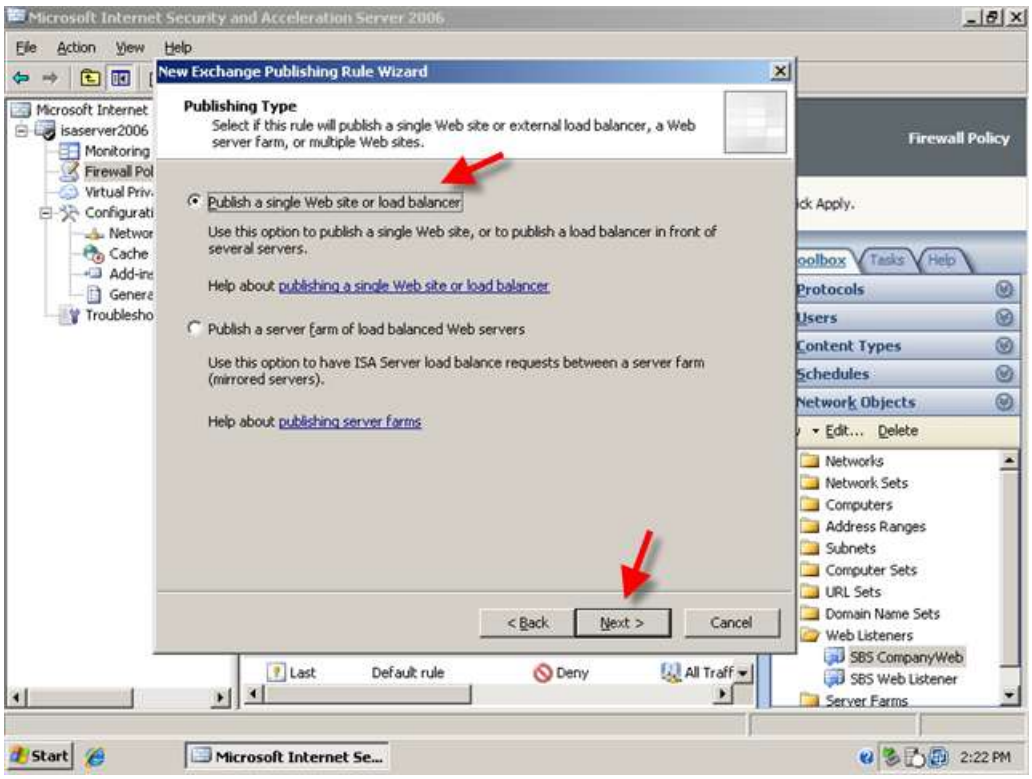
2. Name your rule 'SBS RWW RPC Web Publishing Rule' and click Next



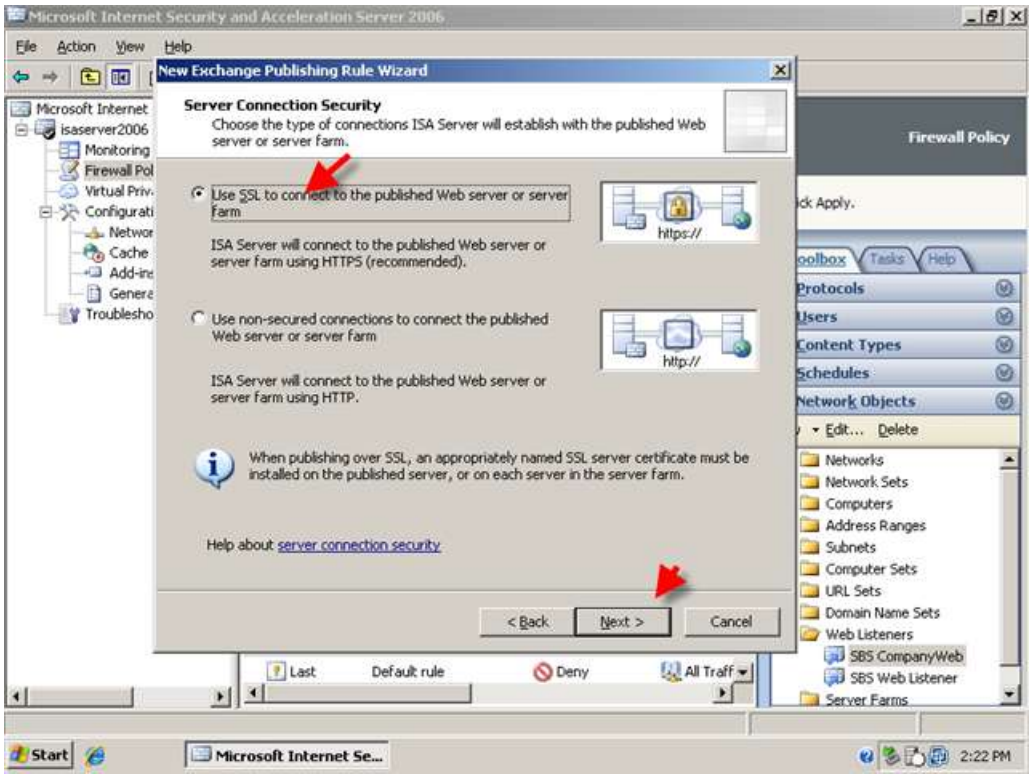
3. In the dropdown menu select Exchange 2007 and in the boxes below, select the box for 'Outlook Anywhere'. Do not check the box for additional folders. Click Next.



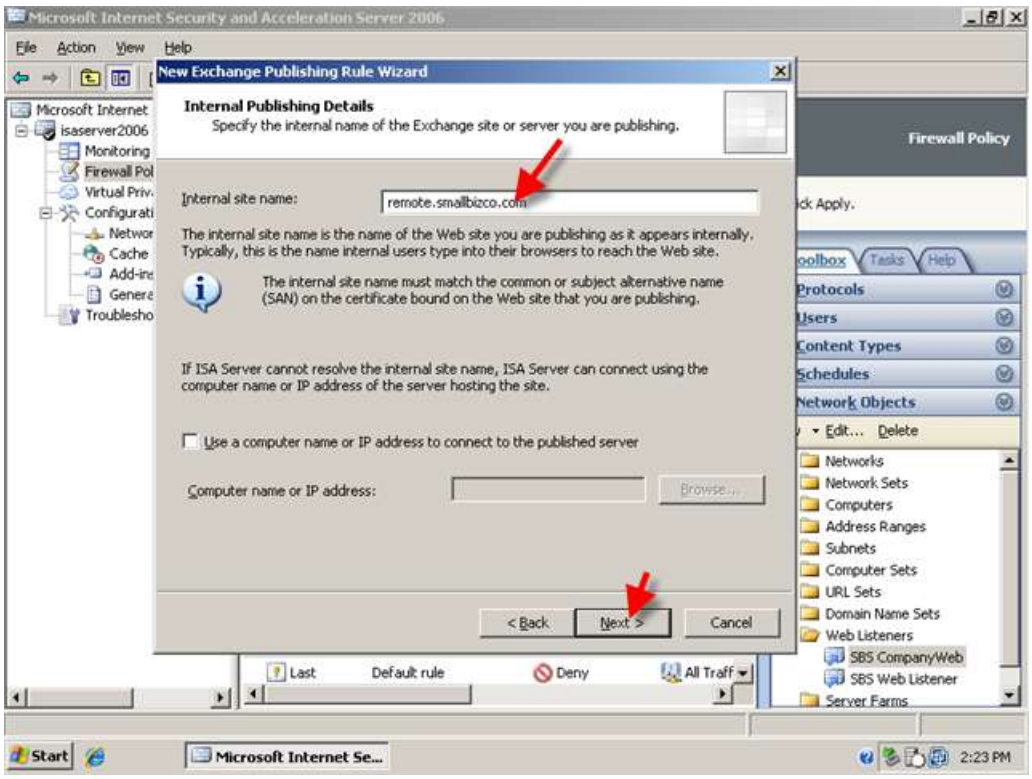
4. Accept the default for 'single website or load balancer' click next.



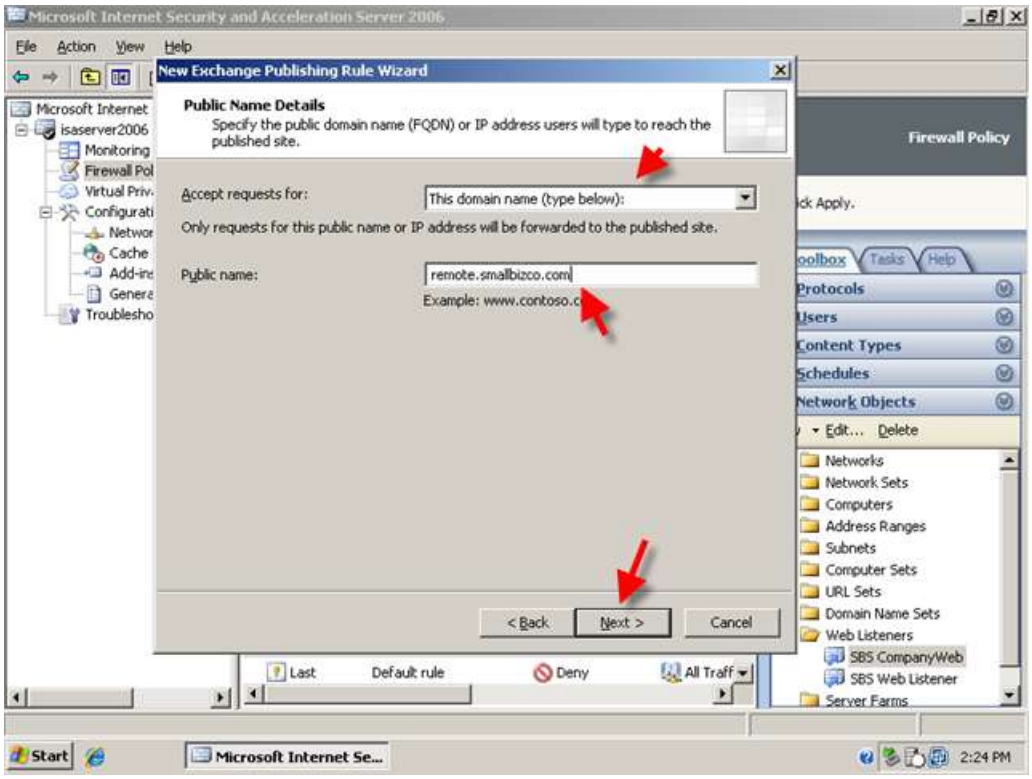
5. Accept the default for 'use SSL to connect to the published web server' and click next.



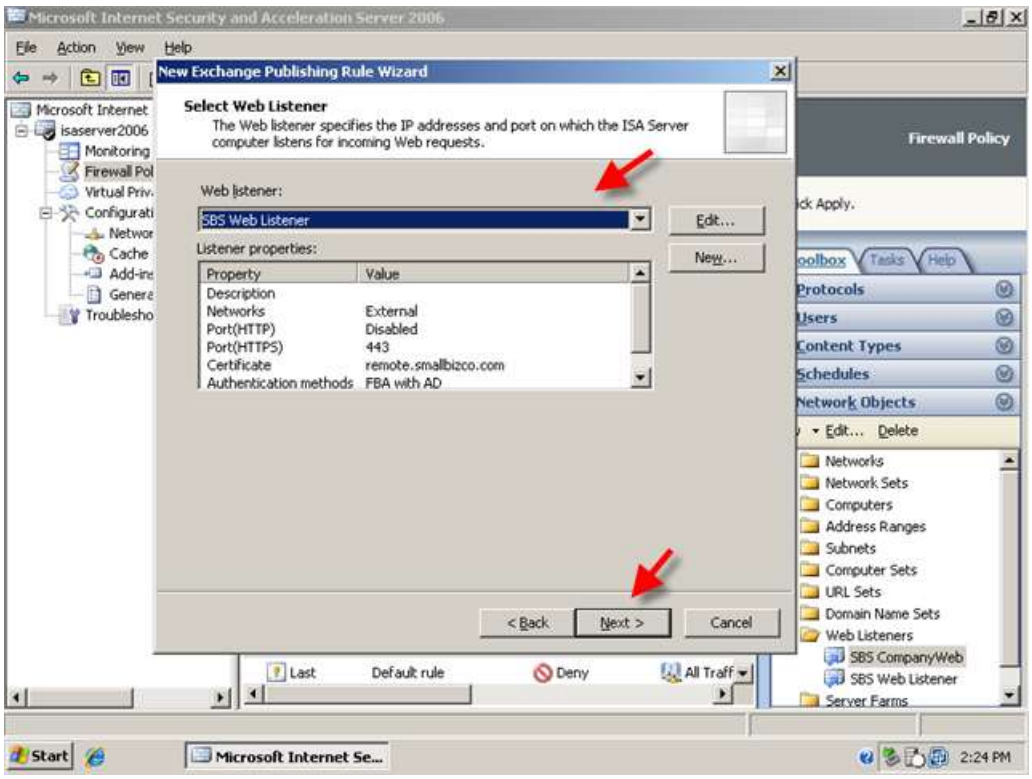
6. On the internal site name page enter, 'remote.smallbizco.com' (where remote.smallbizco.com is your public domain name) and click next.



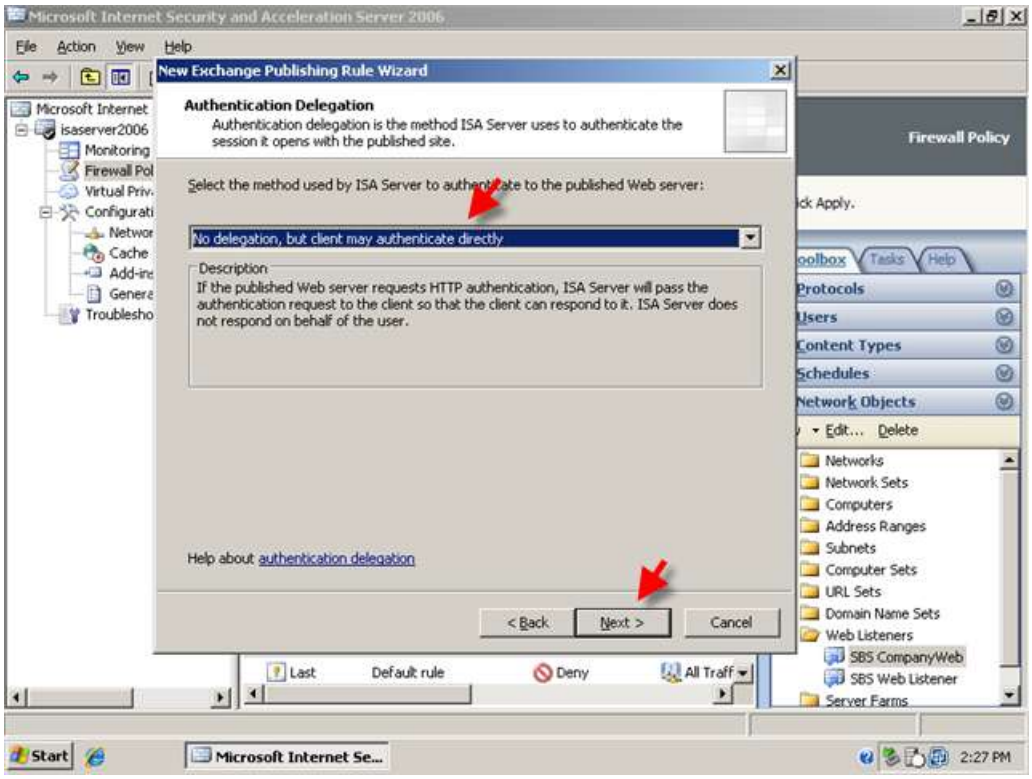
7. On the public domain name enter 'remote.domain.com' (where remote.domain.com is your public domain name) and click next.



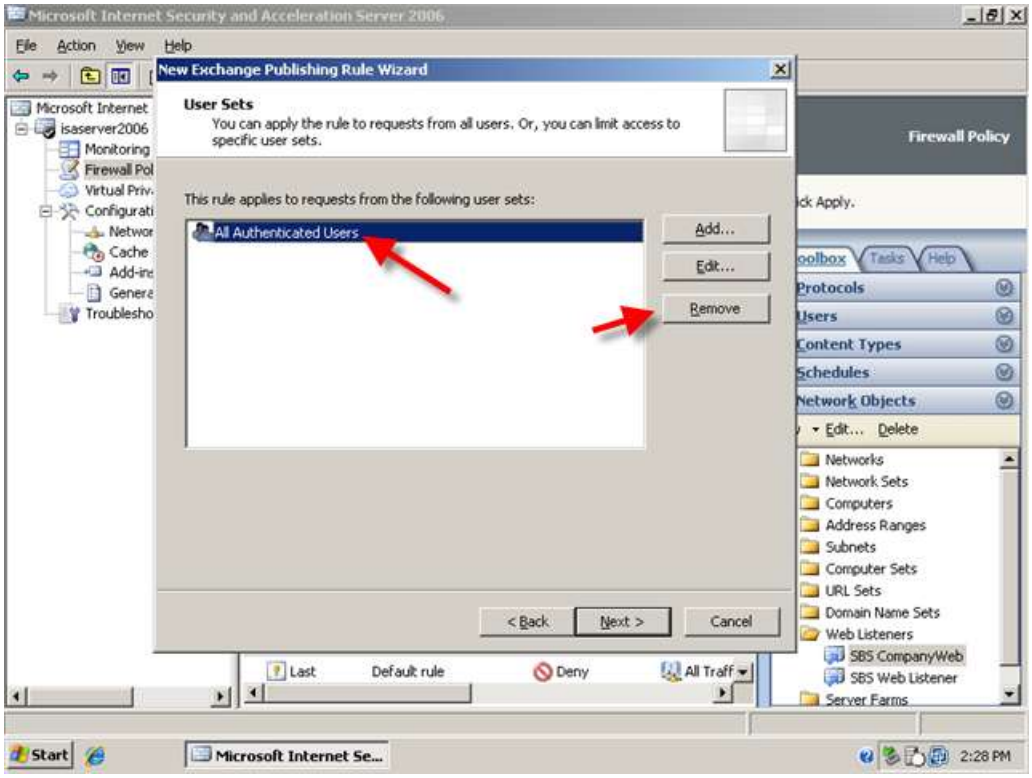
8. On the web listener page, select your Exchange Web Listener and click next.

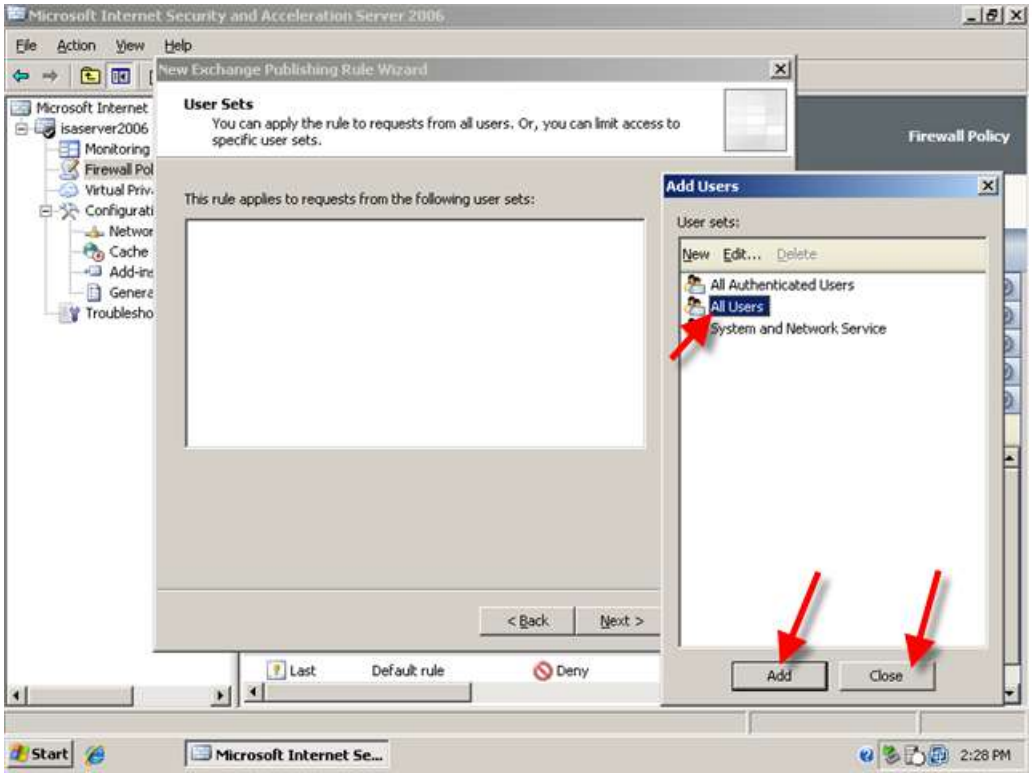


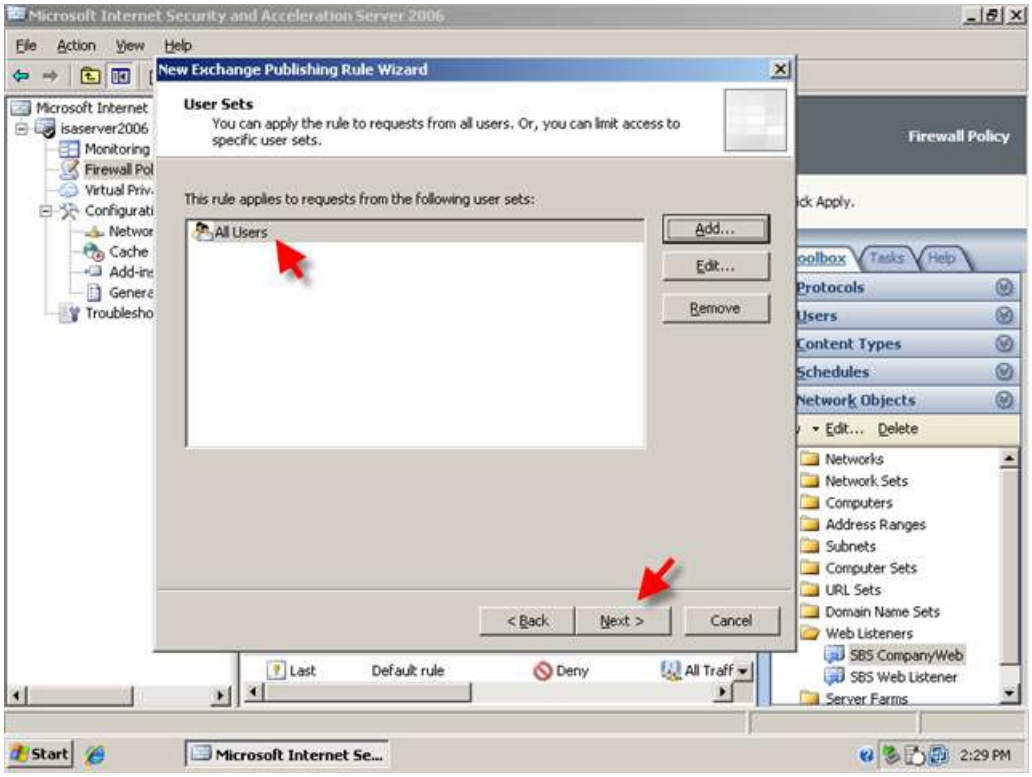
9. On the authentication delegation page, select 'no delegation, but client may authenticate directly' and click next.



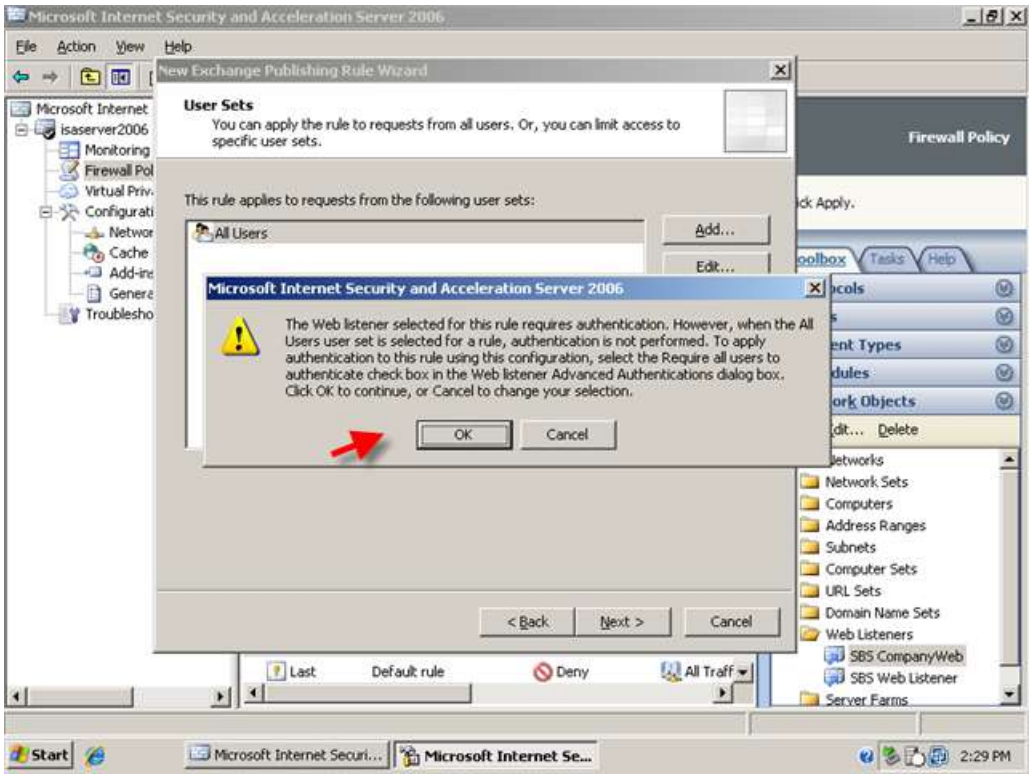
10. On the user sets page, remove the 'all authenticated users' user set and add the 'All Users' user set and click next.



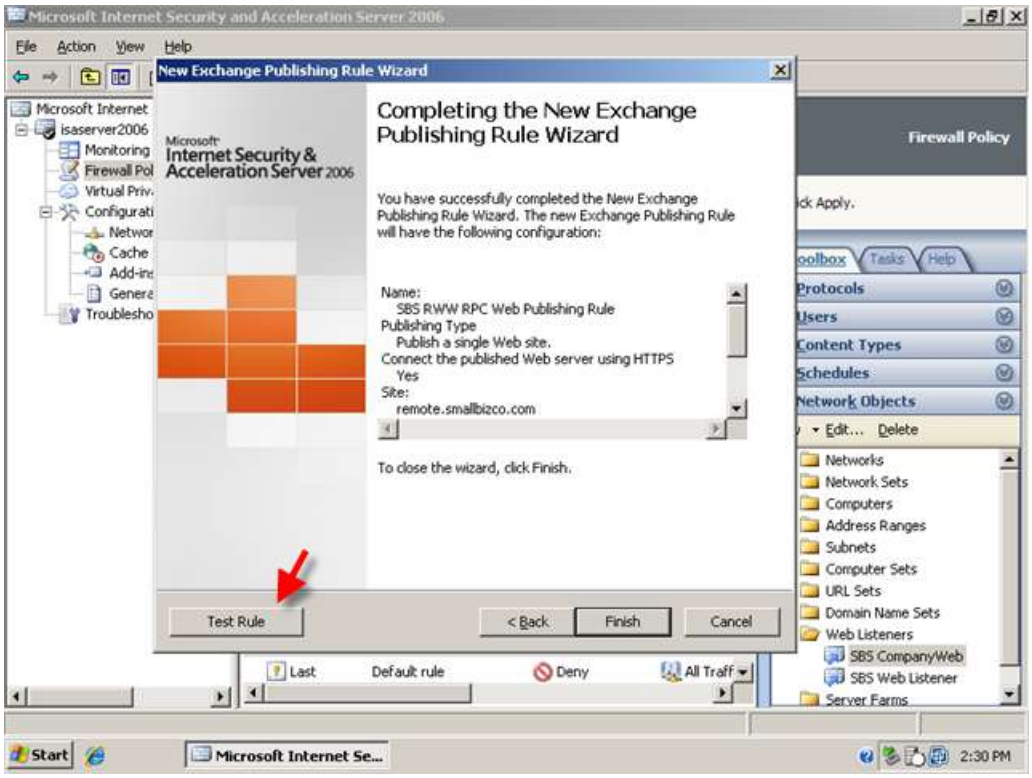

Microsoft Internet Security and Acceleration Server 2006
File Action View Help
New Exchange Publishing Rule Wizard
User Sets
You can apply the rule to requests from all users. Or, you can limit access to specific user sets.
This rule applies to requests from the following user sets:
< Back
Next >
Add Users
User sets:
New Edit... Delete
All Authenticated Users
All Users
System and Network Service
Add
Close
Firewall Policy
Last
Default rule
Deny
Start
Microsoft Internet Se...
2:28 PM

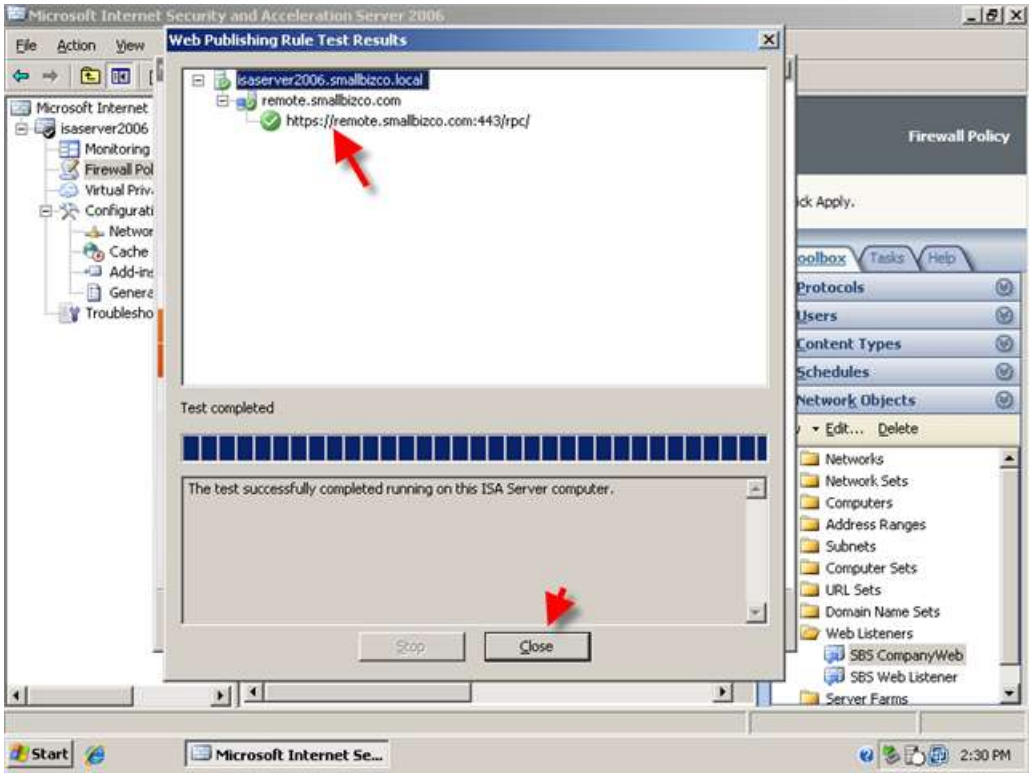

Microsoft Internet Security and Acceleration Server 2006
File Action View Help
New Exchange Publishing Rule Wizard
User Sets
You can apply the rule to requests from all users. Or, you can limit access to specific user sets.
This rule applies to requests from the following user sets:
All Users
Add...
Edit...
Remove
< Back
Next >
Cancel
Firewall Policy
Protocols
Users
Content Types
Schedules
Network Objects
Edit... Delete
Networks
Network Sets
Computers
Address Ranges
Subnets
Computer Sets
URL Sets
Domain Name Sets
Web Listeners
SBS CompanyWeb
SBS Web Listener
Server Farms
Last
Default rule
Deny
Start
Microsoft Internet Se...
2:29 PM

11. Acknowledge the warning regarding authentication by clicking OK.

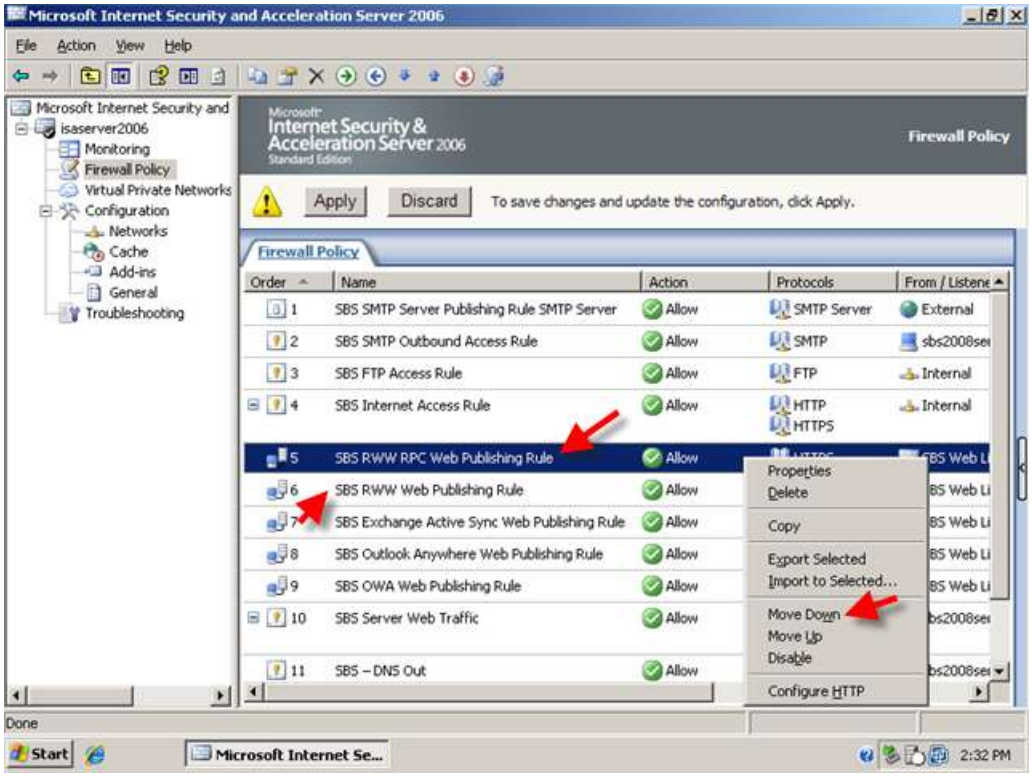


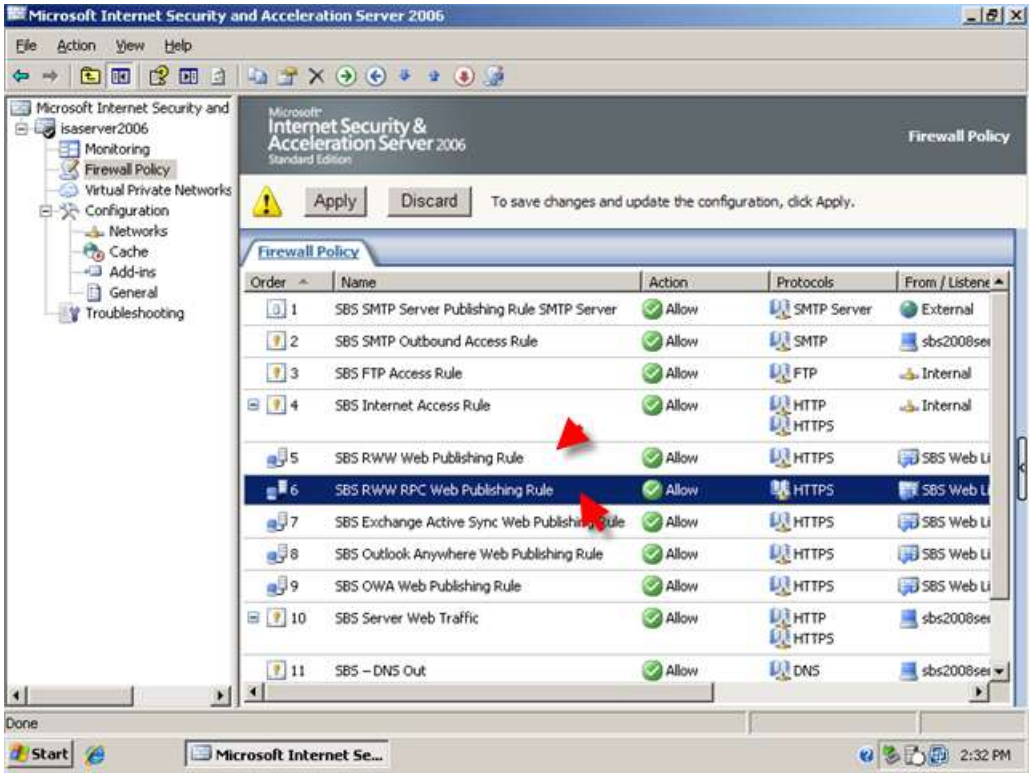
12. Review and test your rule settings and click Finish.



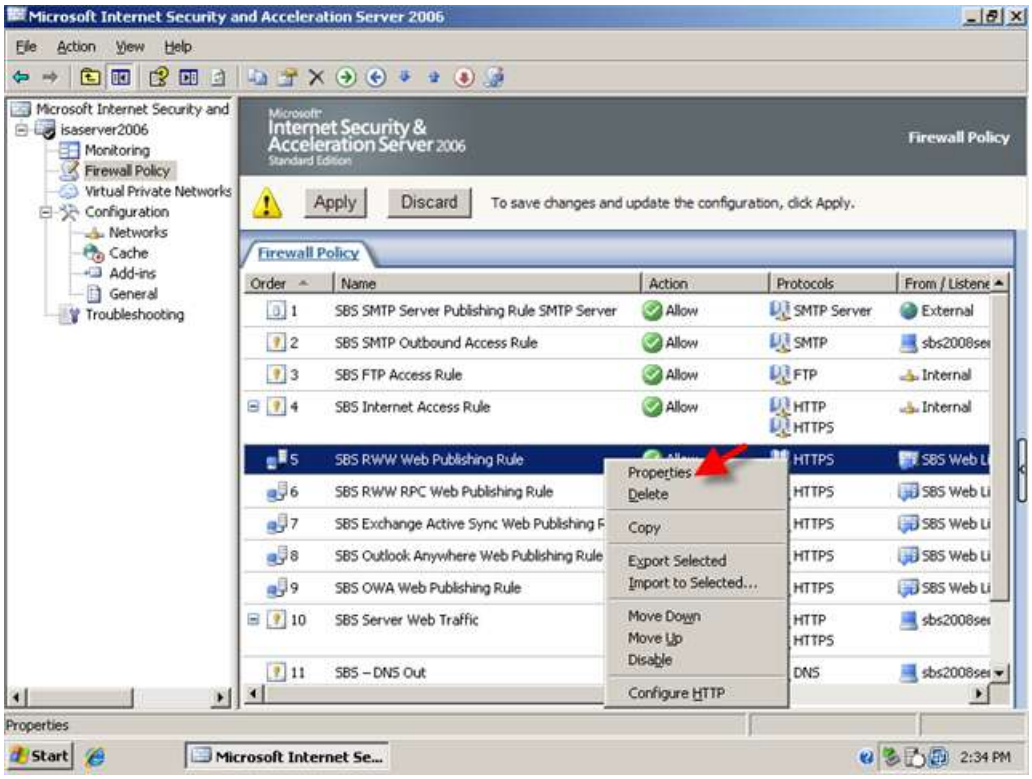


13. We will move this rule below the RWW Web Publishing Rule, right click the RWW RPC Web Publishing rule and click Move Down.

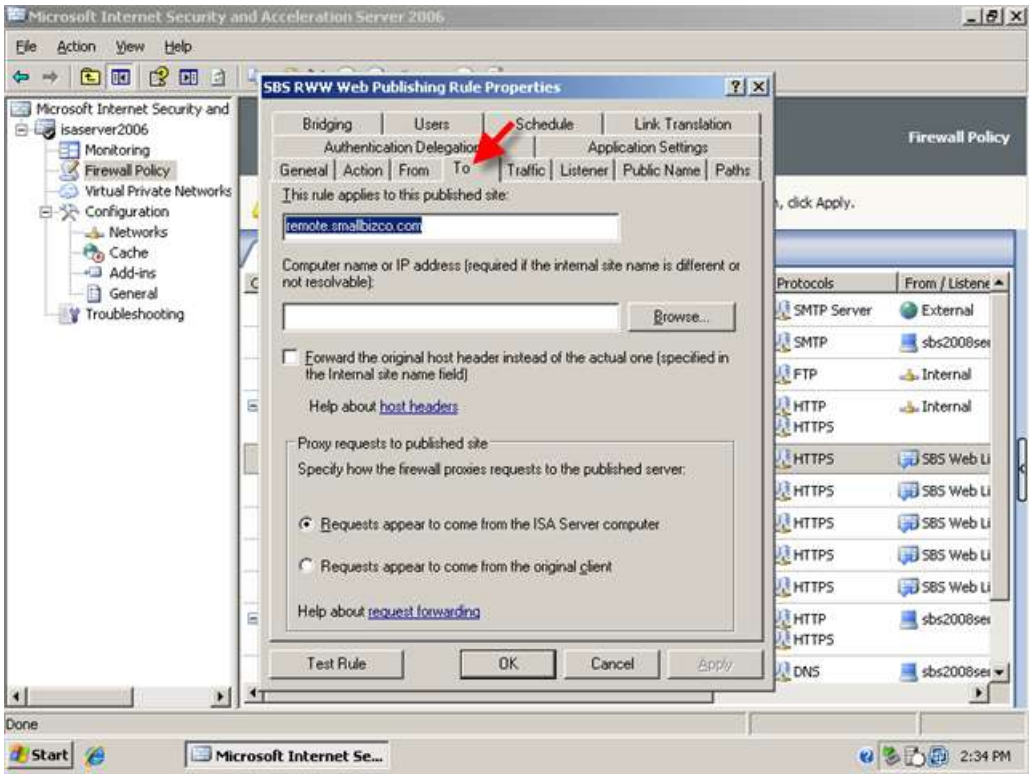




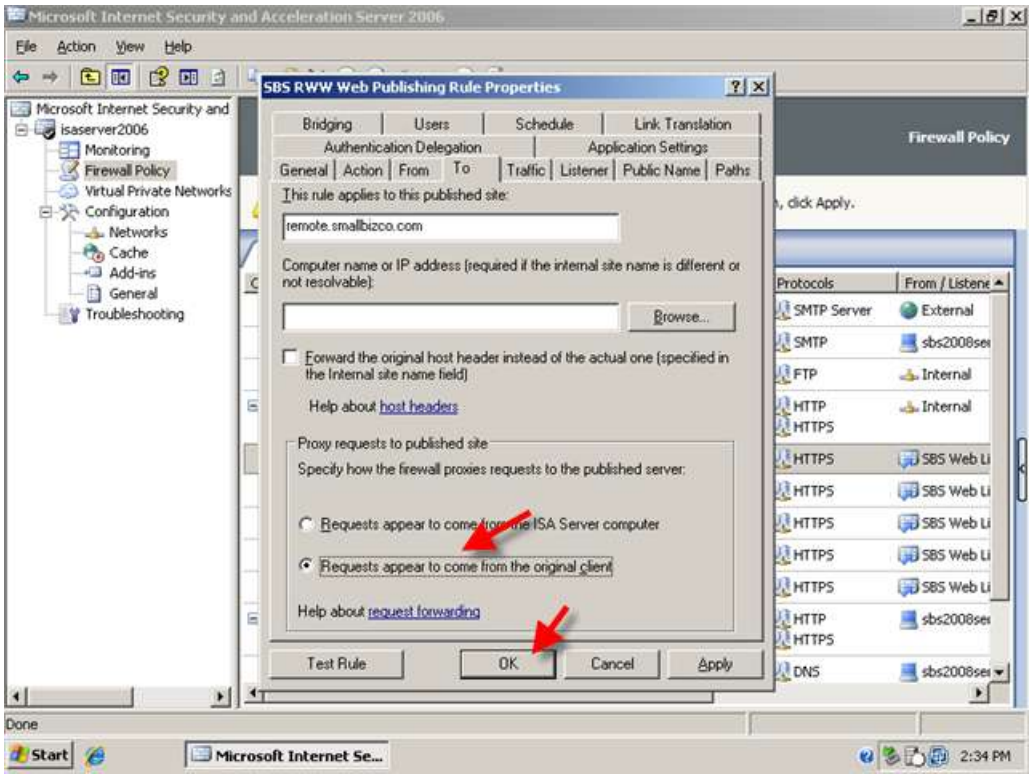
14. We also need to make another small change to both the RWW rules we have created. Right click one of the rules and go to properties.



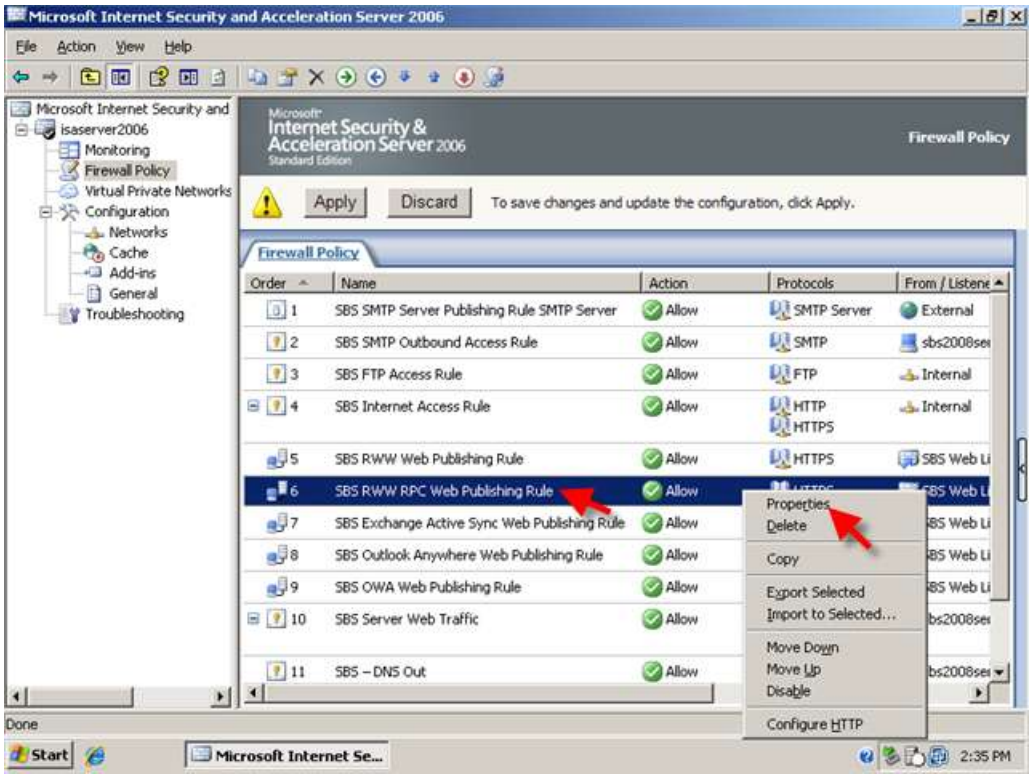
15. Go to the 'To' Tab.



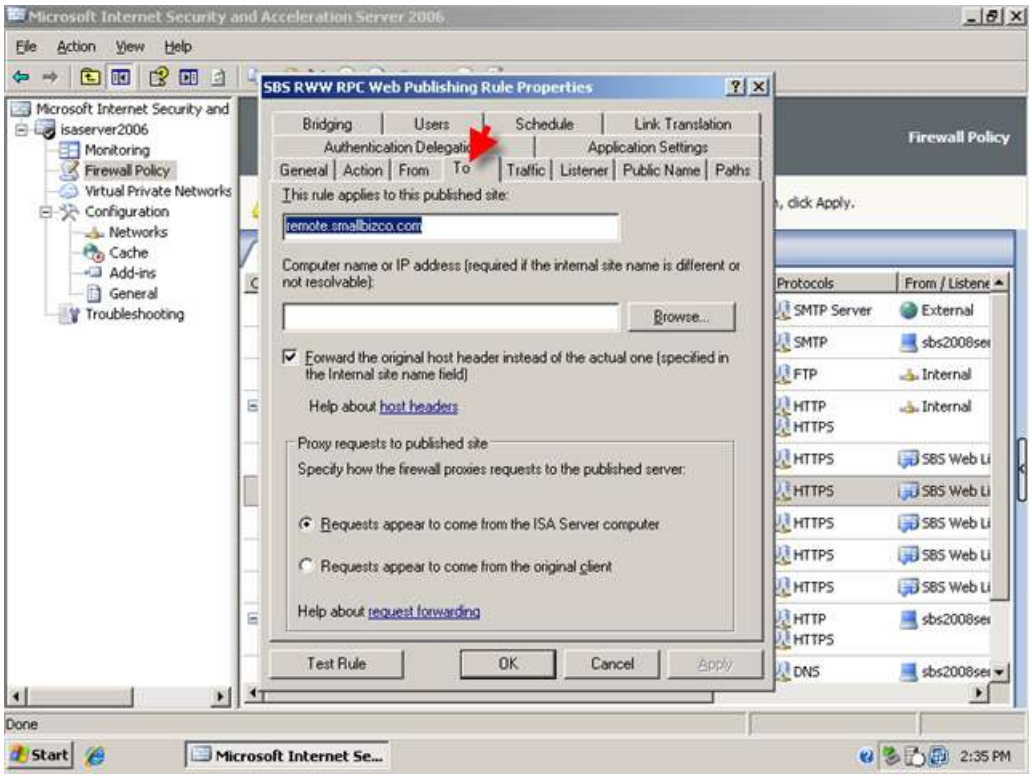
16. Select the radio button next to 'requests appear to come from the original client' then click Ok



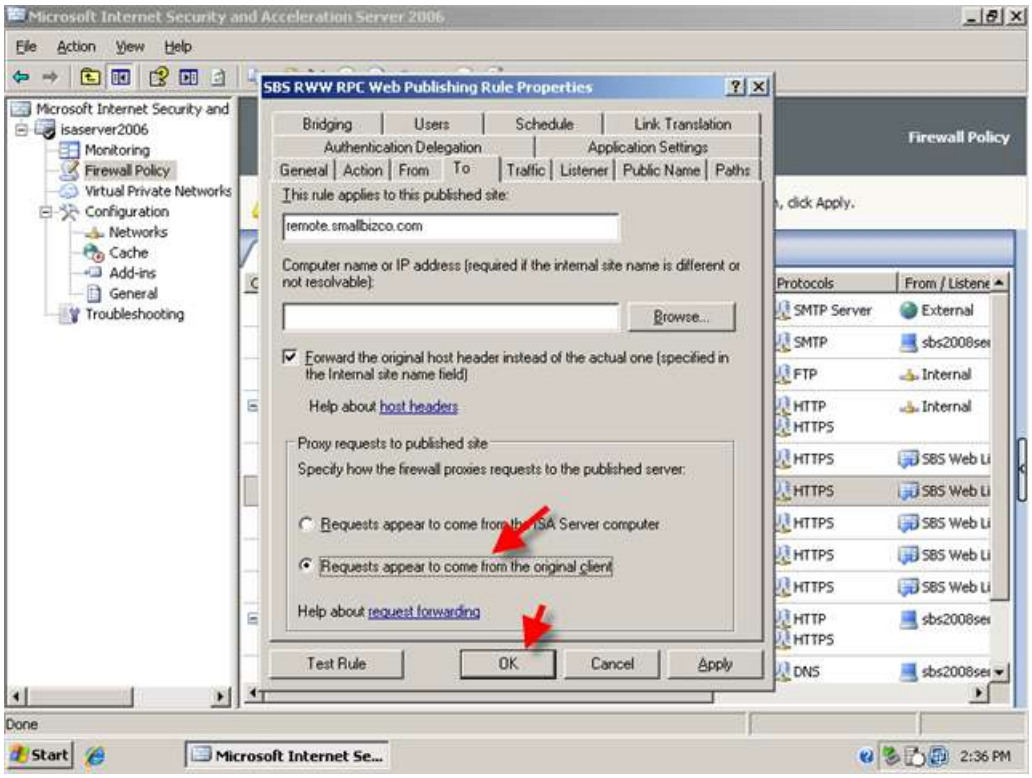
17. Repeat this process for the other rule. Right click the rule, go to properties.



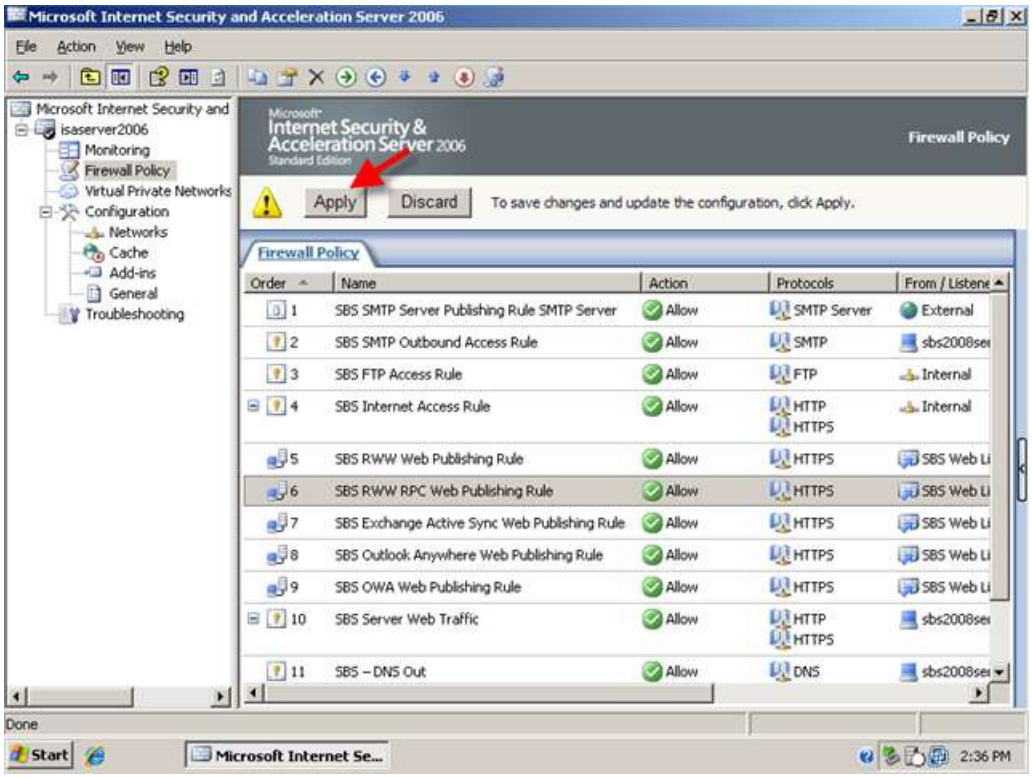
18. Go to the 'To' Tab.



19. Select the radio button next to 'requests appear to come from the original client' then click Ok



20. Click Apply to save your changes to the firewall policy.

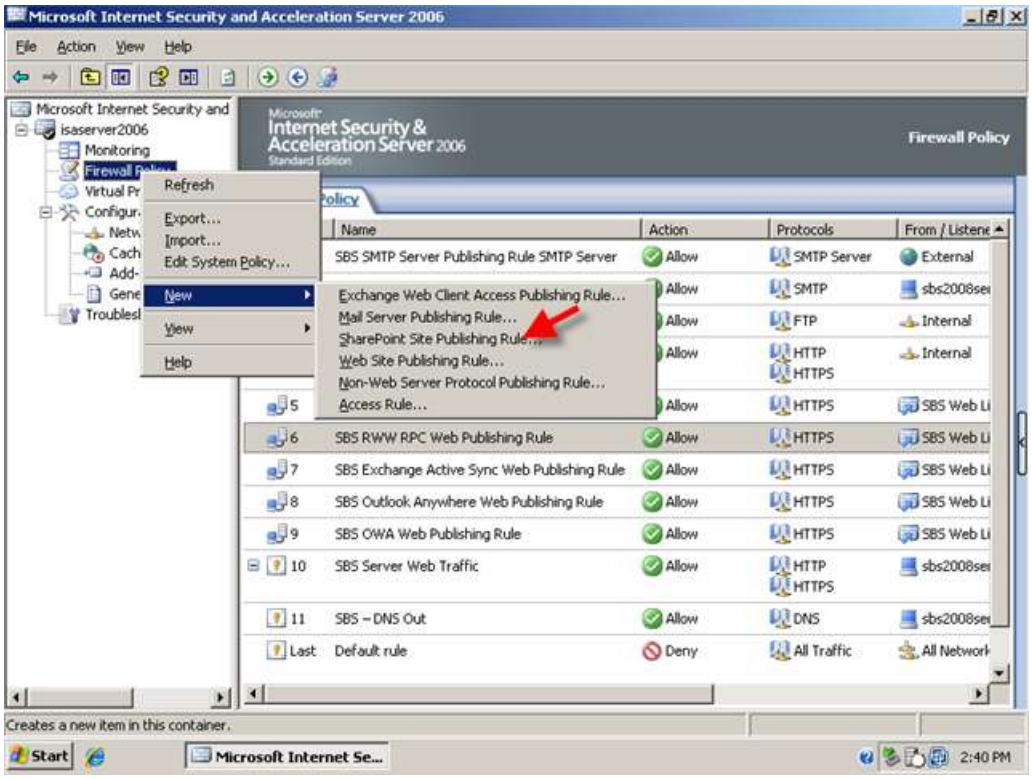


21. You can now apply your settings and from a remote computer access https://remote.smallbizco.com/remote to access your Remote Web Workplace.

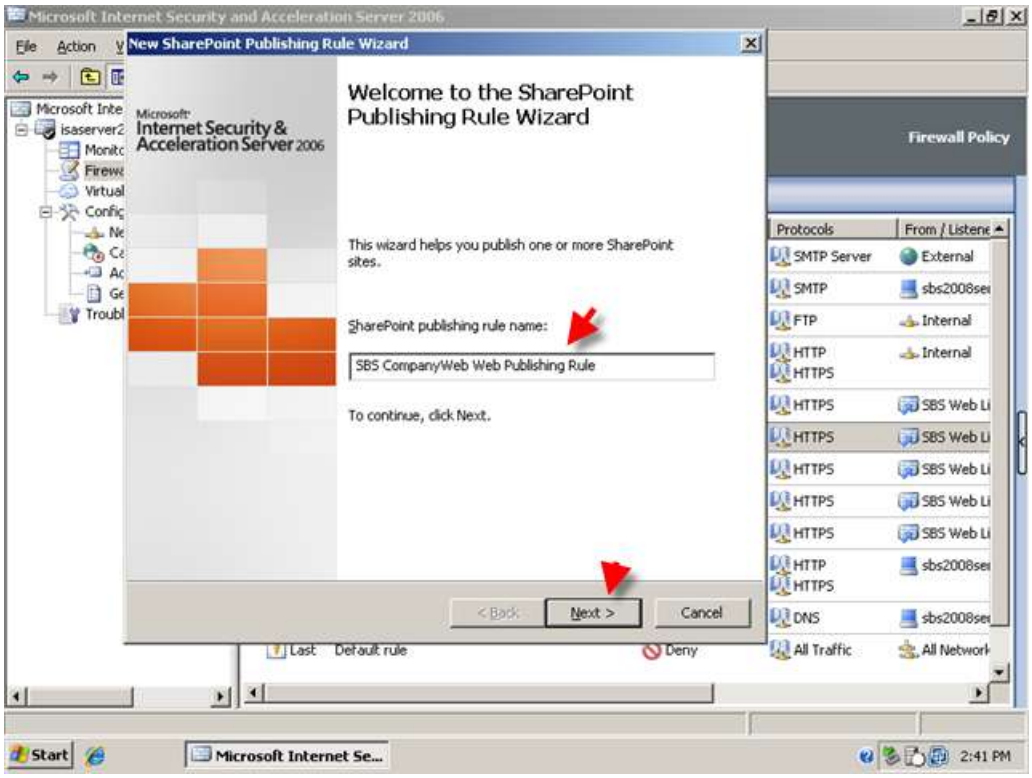
Creating a Web Publishing Rule For CompanyWeb

To publish your CompanyWeb site, we must create a new Sharepoint Publishing Rule.

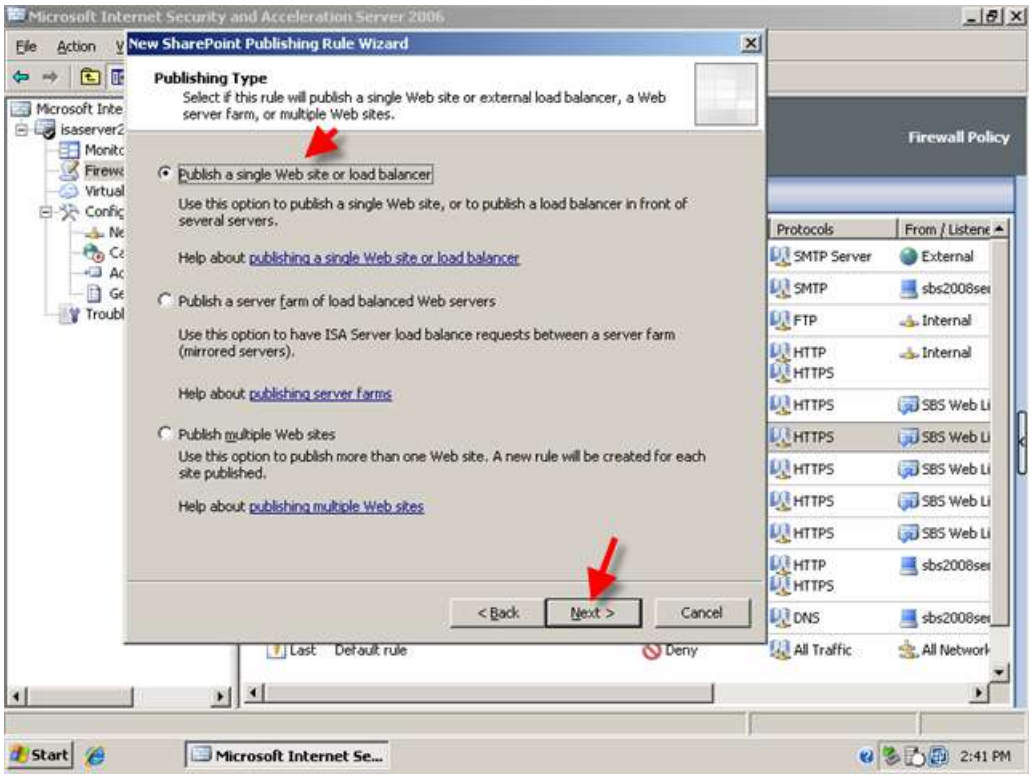
1. Right click the Firewall Policy, and click new > Sharepoint Publishing Rule.



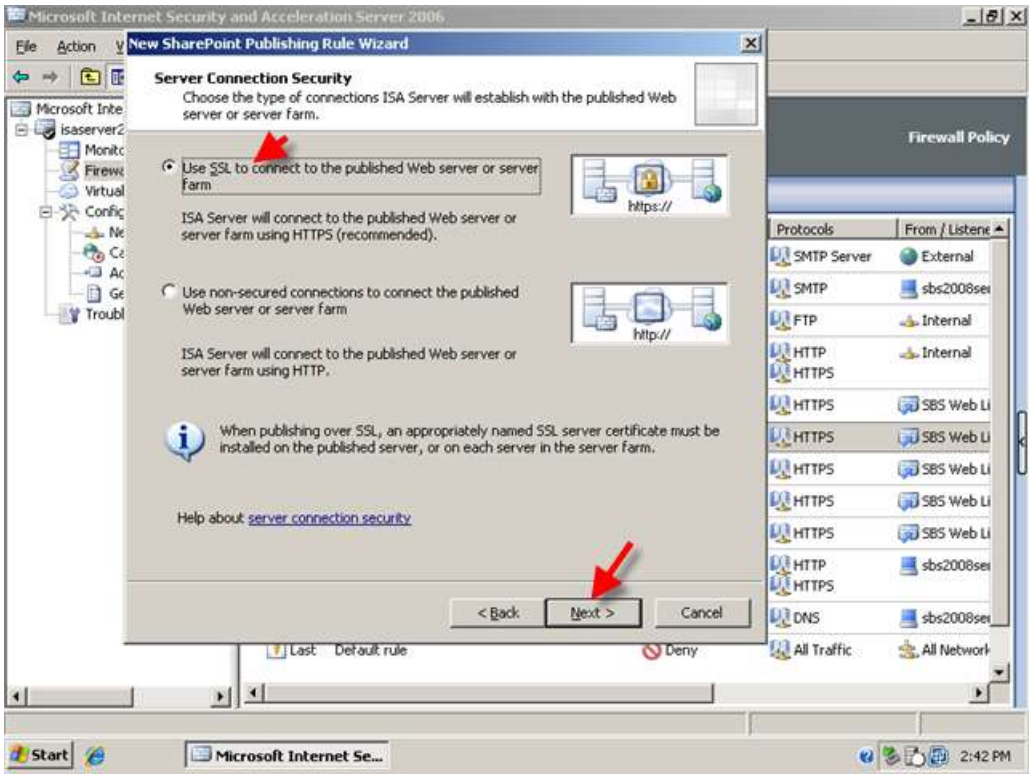
2. Enter a name for your rule, I am using SBS CompanyWeb Web Publishing Rule, click Next.



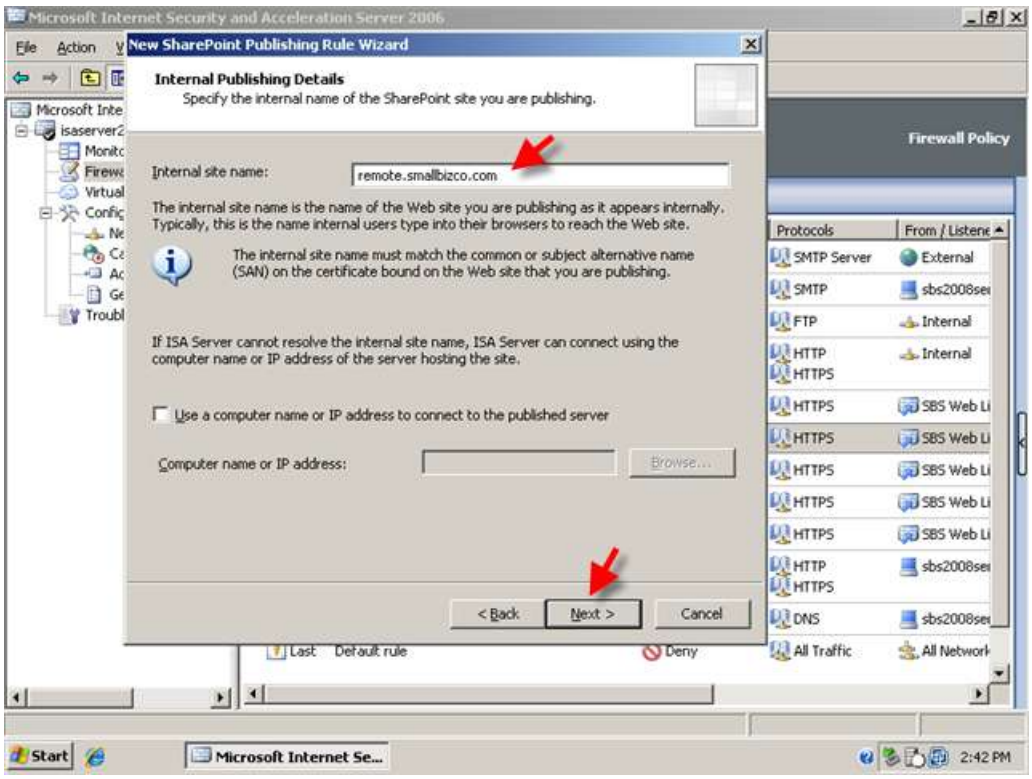
3. Accept the default to publish a single web site or load balancer. Click Next.



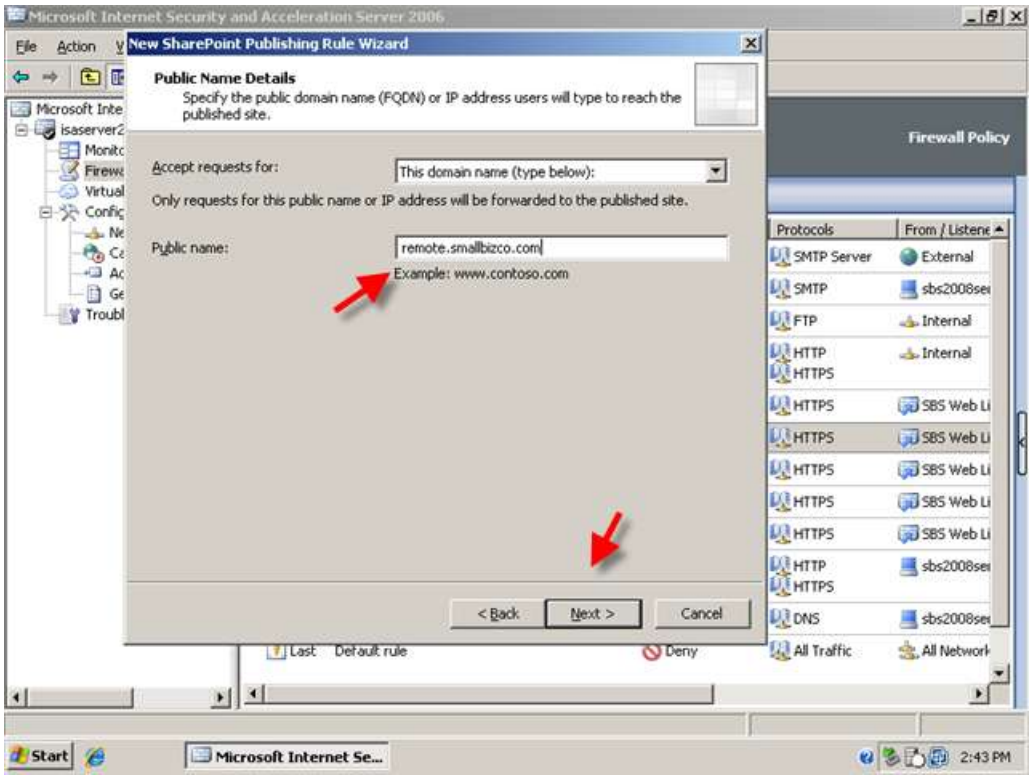
4. Change the setting to connect to the published web site using secure connections. And click Next.



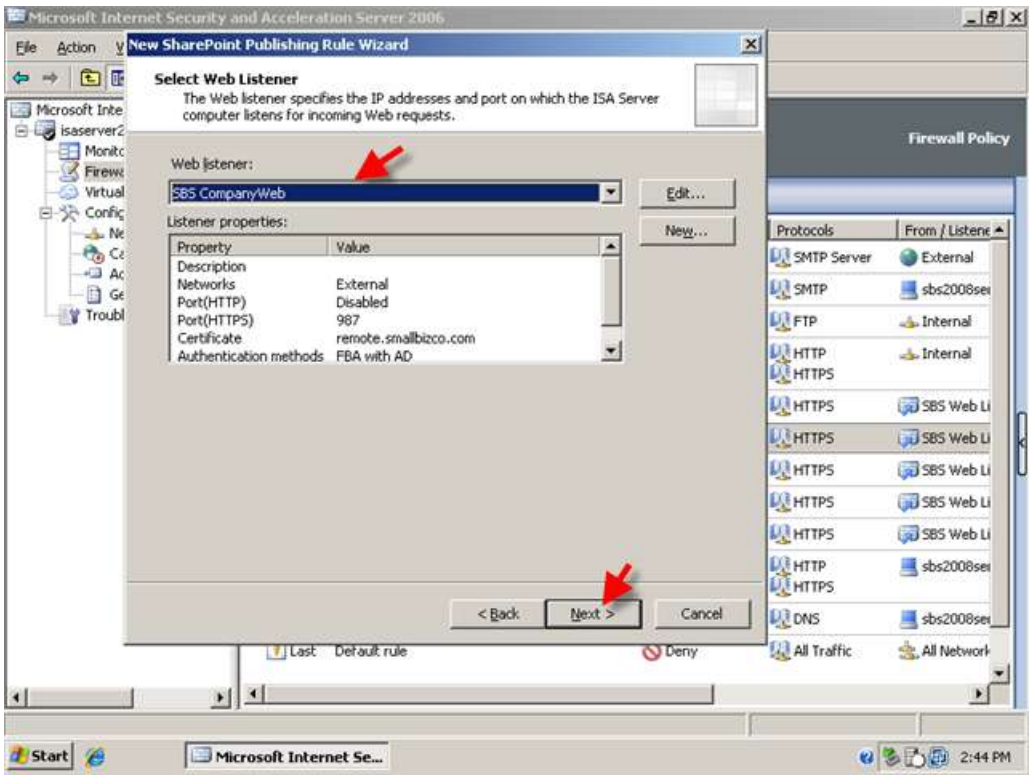
5. On the internal site name page enter, 'remote.domain.com' (where remote.smallbizco.com is your public domain name) and click next



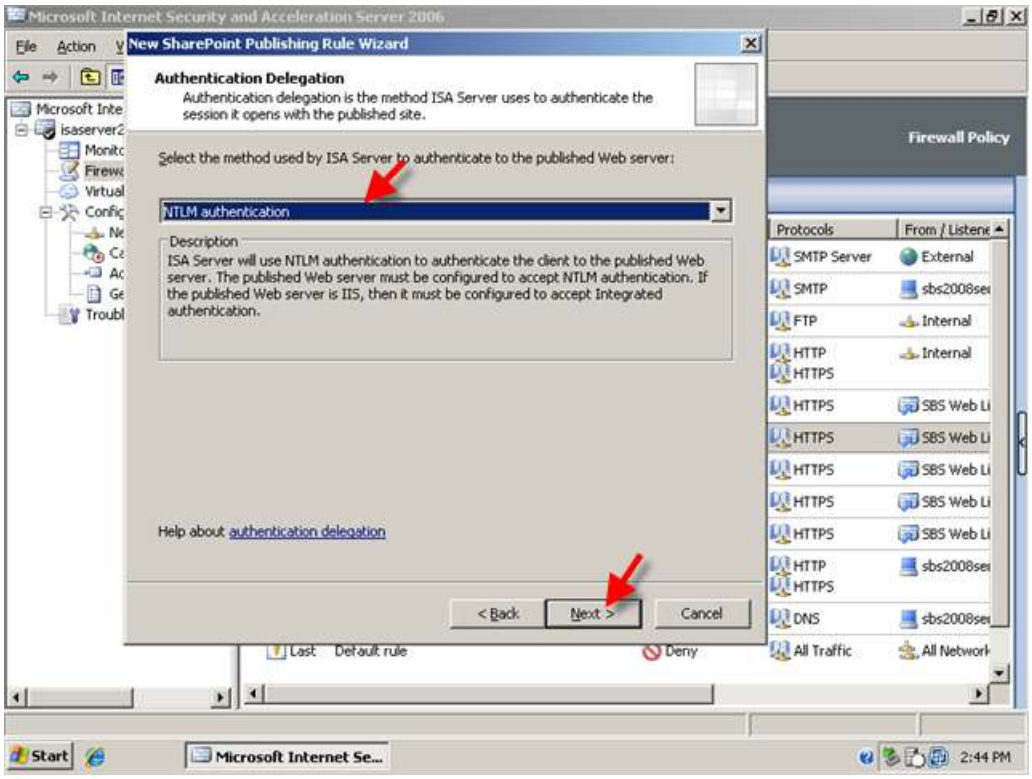
6. On the public domain name enter 'remote.domain.com' (where remote.domain.com is your public domain name) and click next



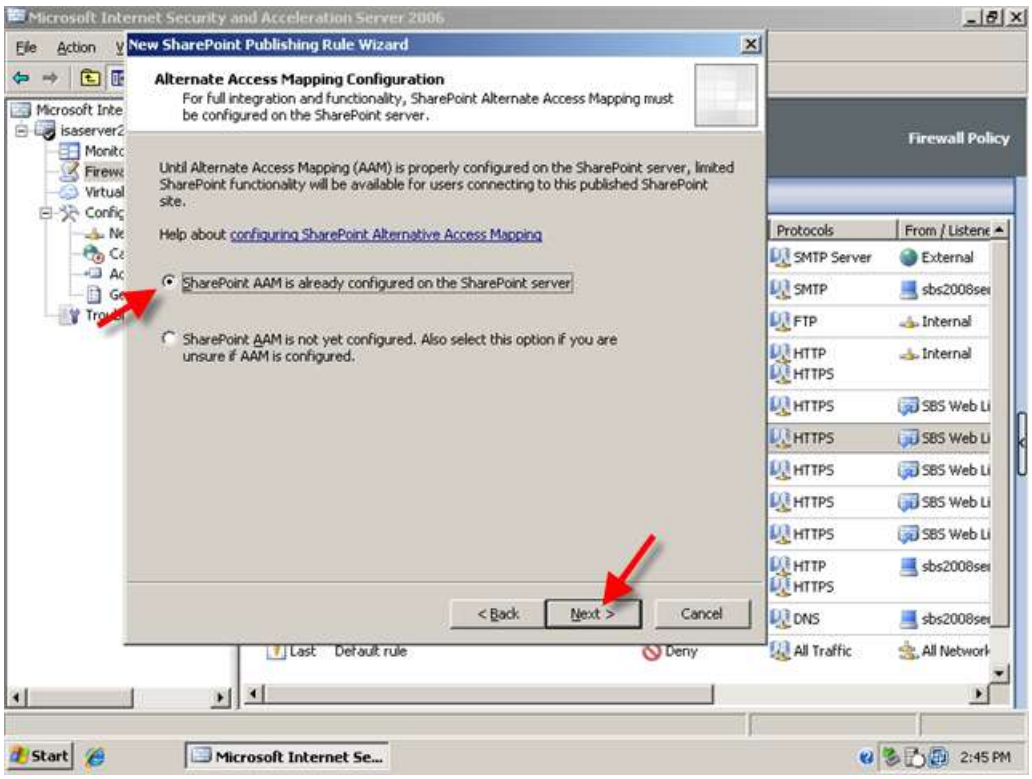
7. On the Web Listener page, choose the SBS CompanyWeb Web Listener, and click Next.



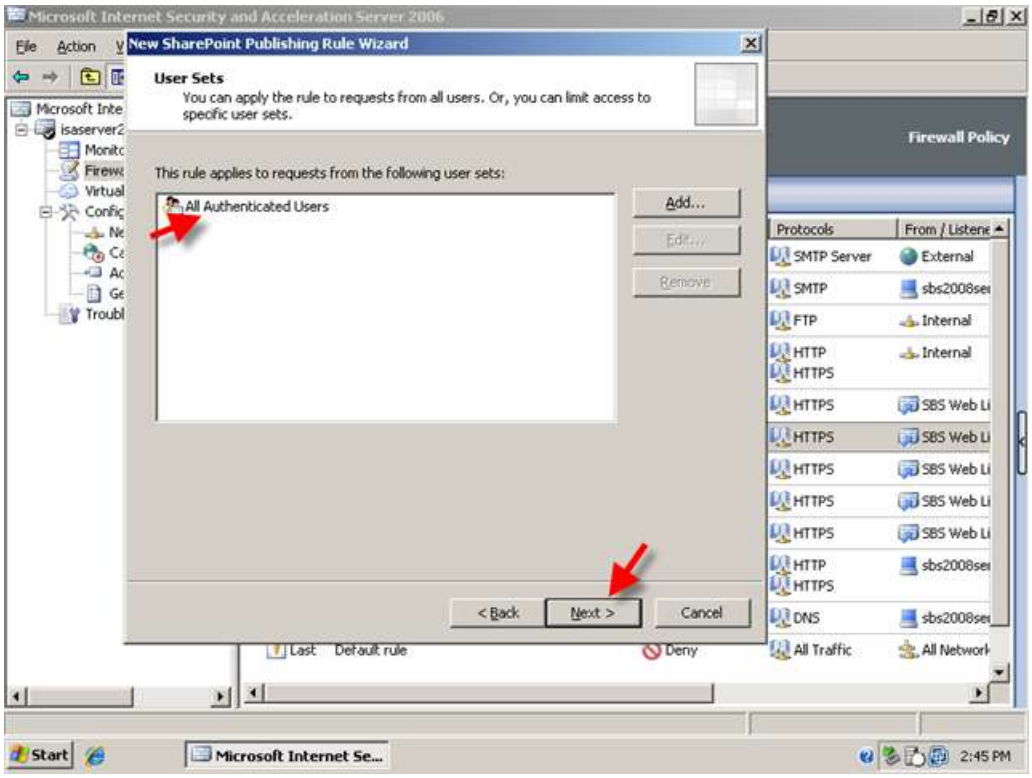
8. On the Authentication Delegation page, use the drop down menu and select NTLM Authentication, and click Next.



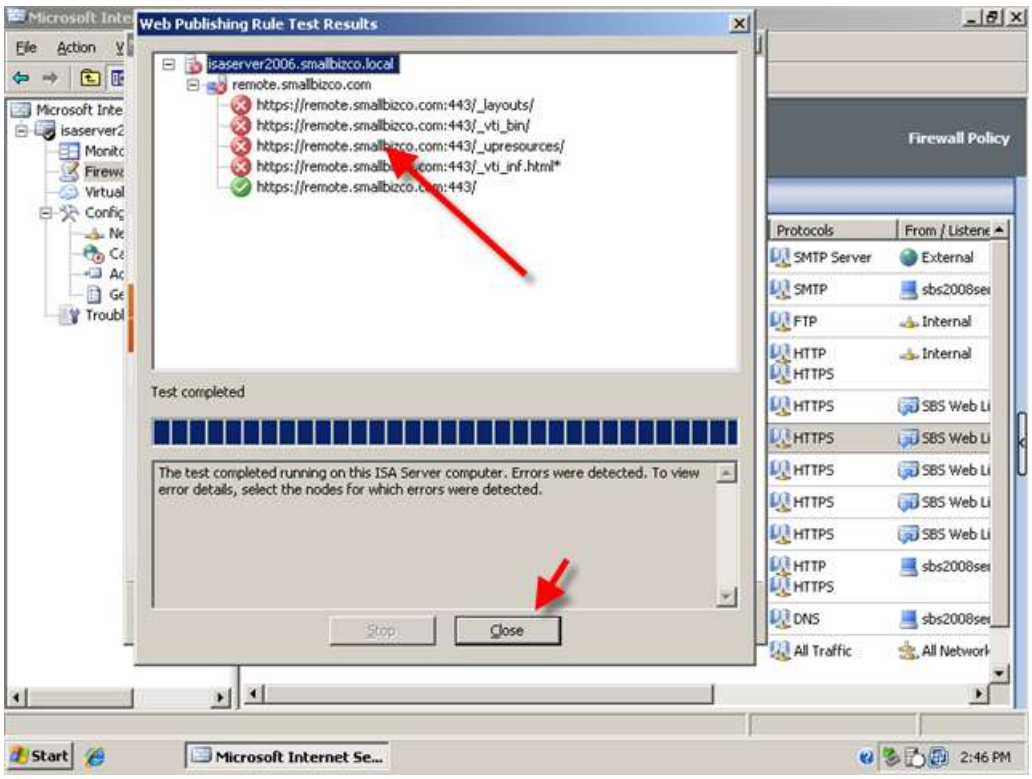
9. In the Sharepoint AAM page, choose AAM has already been configured, and click Next.



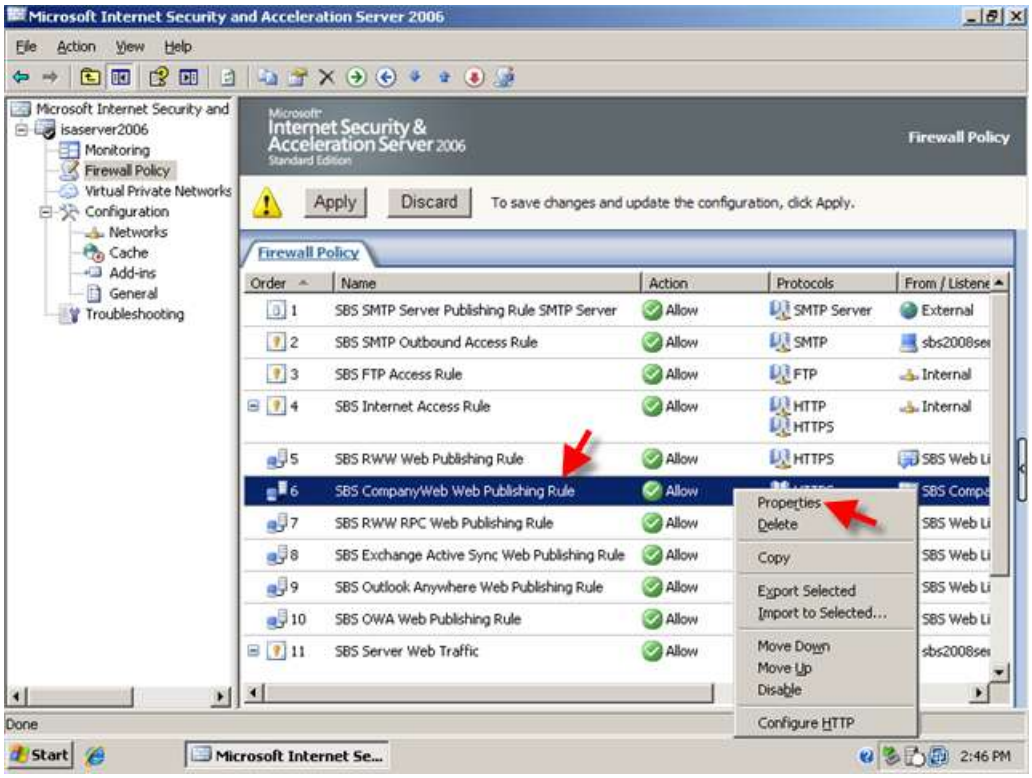
10. Accept the default 'All Authenticated Users' and click Next.



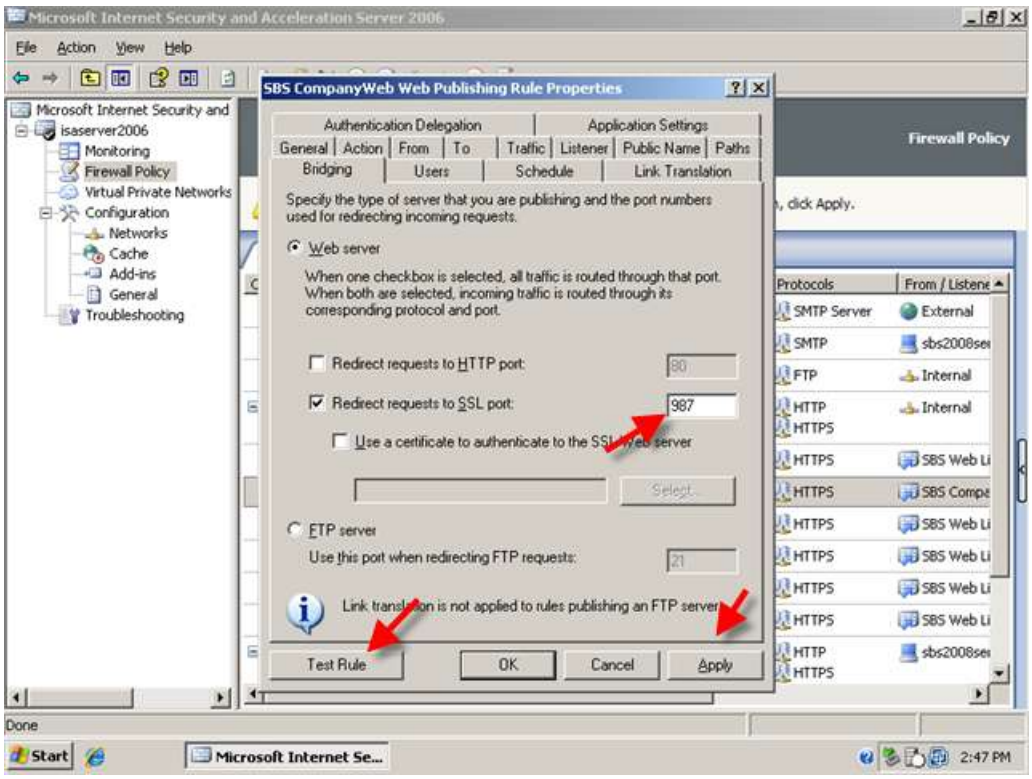
11. Clicking Test Rule to test your rule, will result in failure. We must change some more settings for this to work. Click Close on the test results and click Finish to return to the firewall policy.

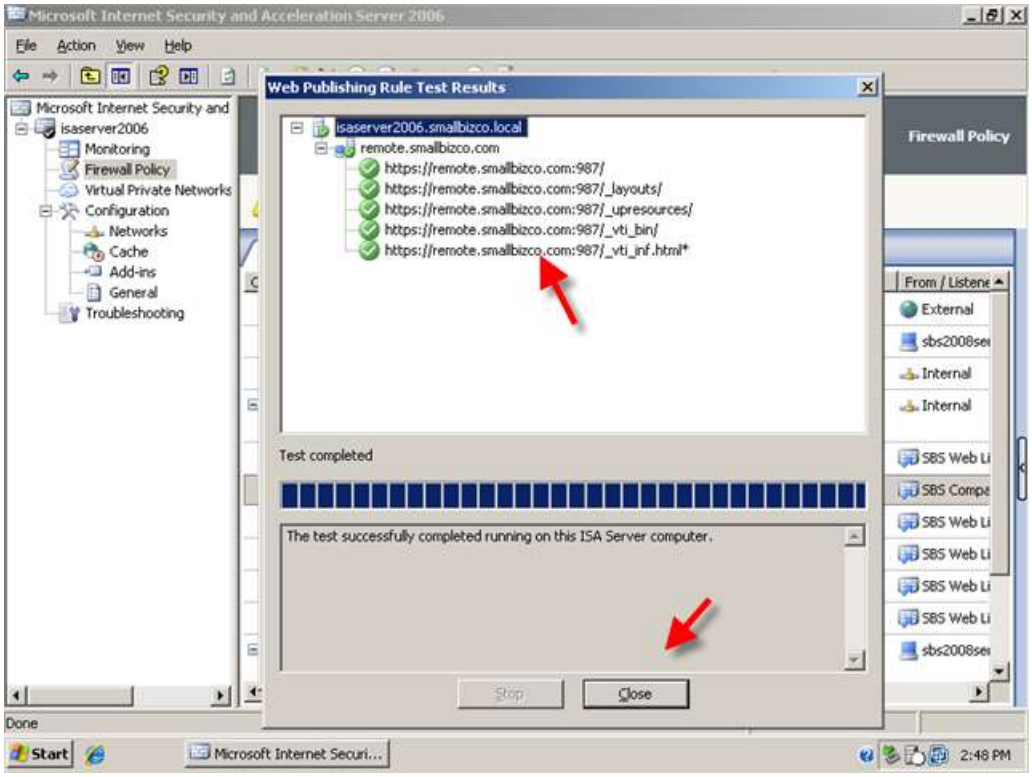


12. Right click your SBS CompanyWeb Publishing rule, and click Properties.



13. Go to the Bridging tab. Change the value 443 to 987 and click Apply. Now you can click Test Rule, and you will see the tests complete successfully. Click Ok and click Apply to save your firewall configuration.



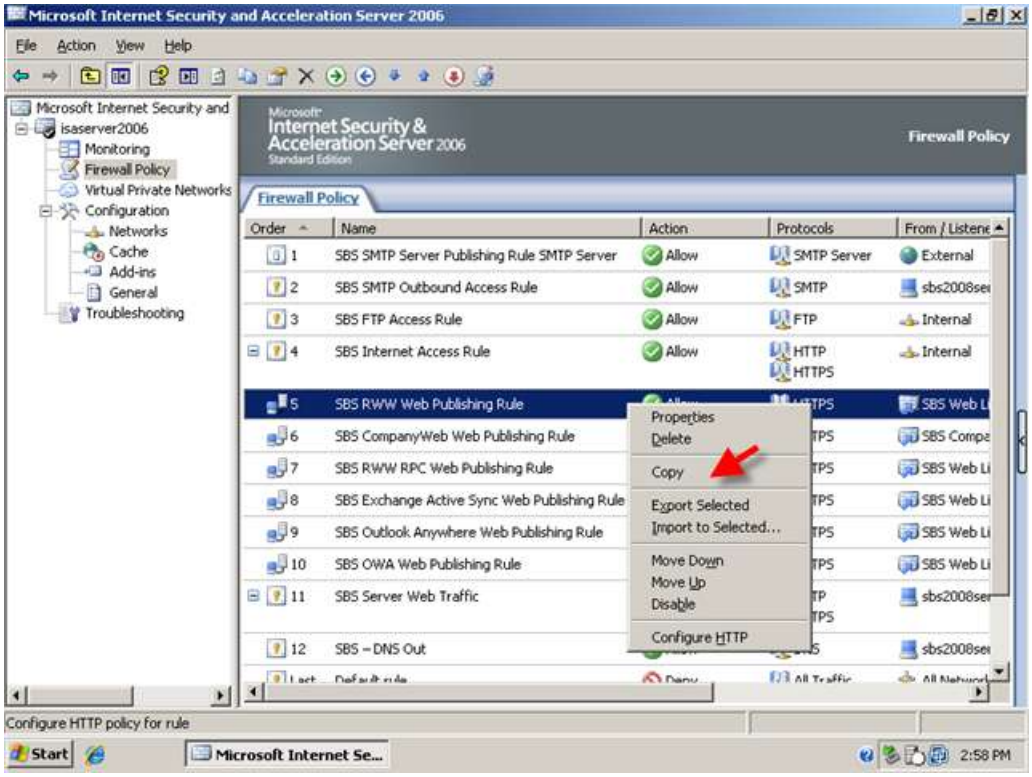


You will now be able to access the CompanyWeb site externally by navigating to https://remote.domain.com:987. You will also be able to login to the CompanyWeb site by first entering the Remote Web Workplace.

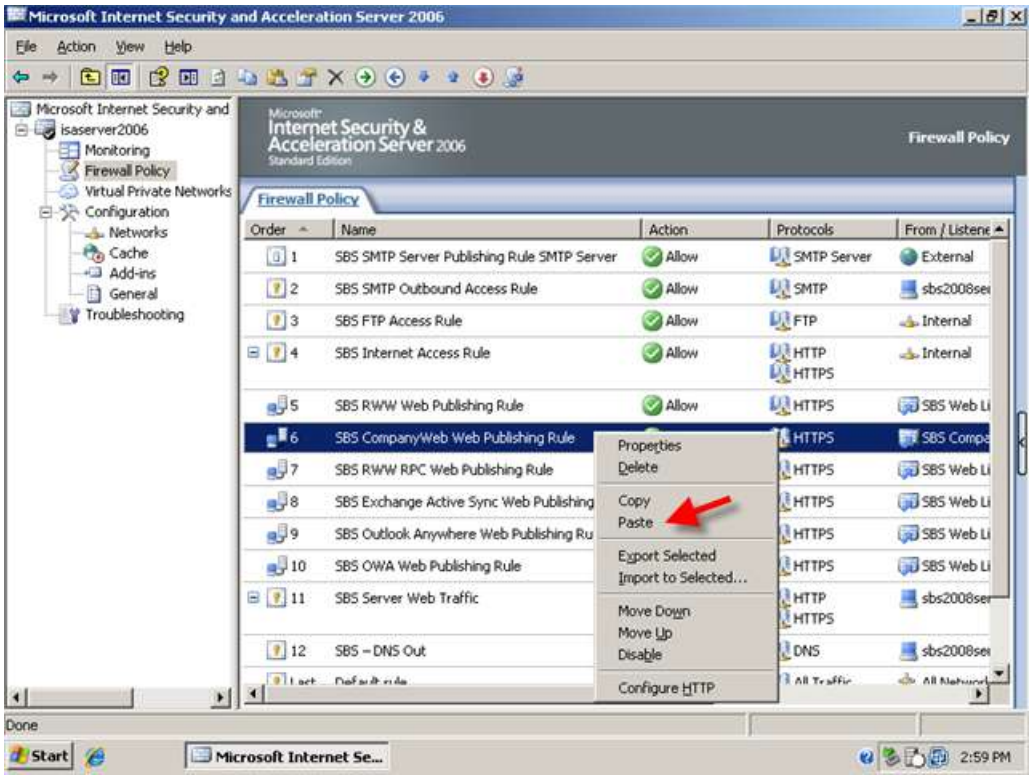
Configuring URL Redirection for Remote Web Workplace and CompanyWeb

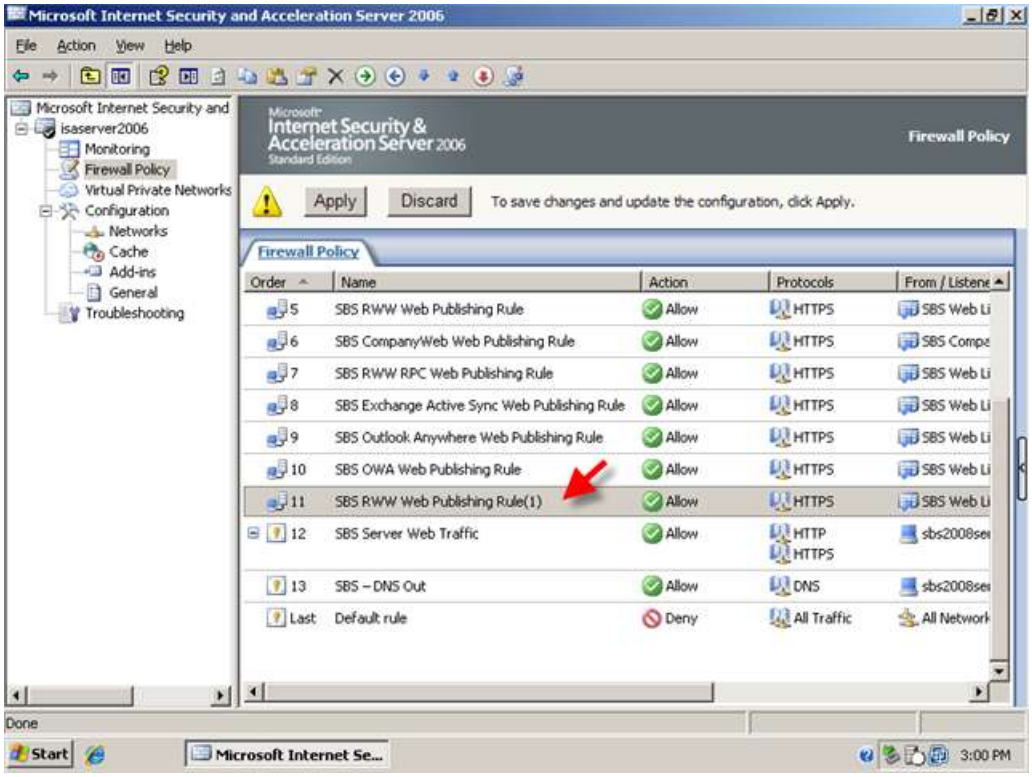
When not using ISA Server, accessing https://remote.domain.com would automatically redirect you to the /remote page and you would be prompted to login to the RWW. With ISA Server this does not work. Unless you enter the specific path of the resource that is published, ISA will tell you to go away. Well, we don't have to leave it that way and we can use ISA to redirect us to the correct pages.

1. Make sure you have selected the rule in the firewall policy directly below your last web publishing rule, in the example screen shot below this is the SBS FTP rule, depending on your rule order it may be something different. It is important to make sure our redirection rules are below any other rule that is publishing a resource.
2. Right click your RWW publishing rule, and click Copy.

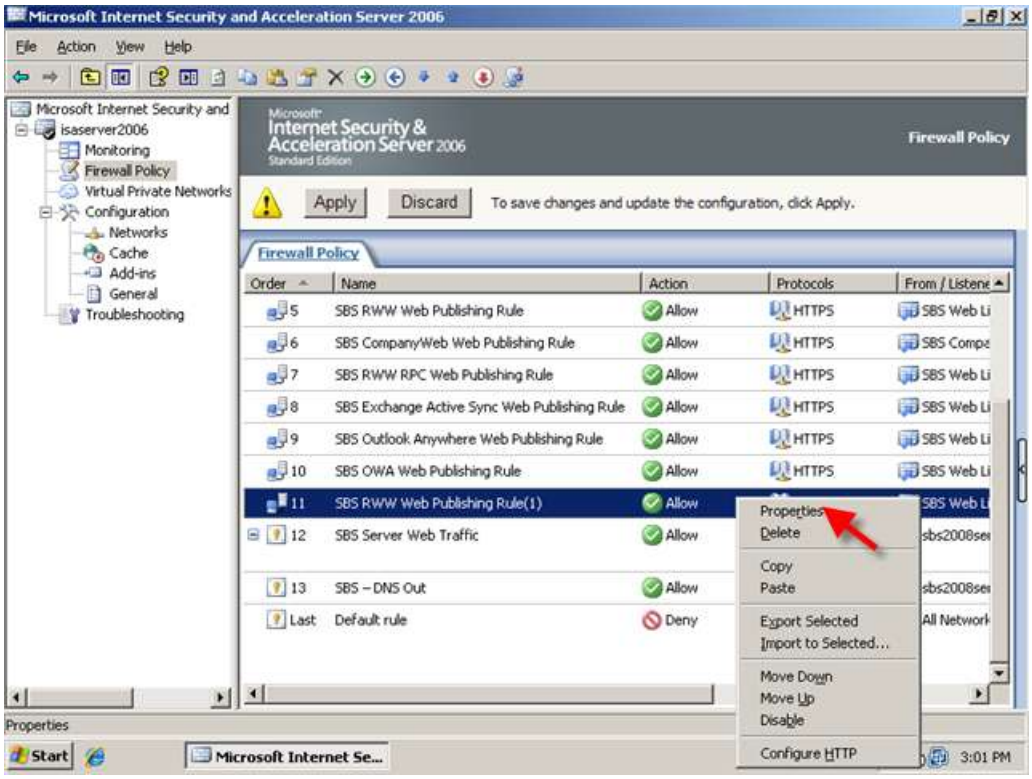


3. Right click a rule in the Firewall Policy and click Paste. You may need to adjust the positioning of this rule, you can do this by right clicking it and clicking Move Up or Move Down as required.

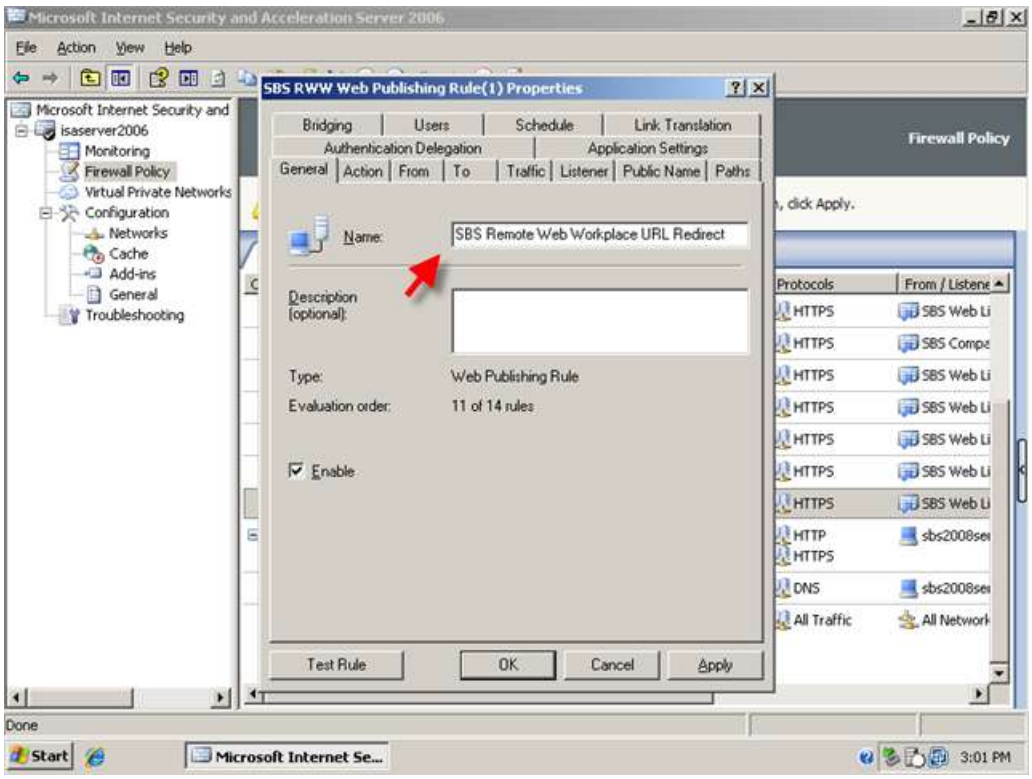




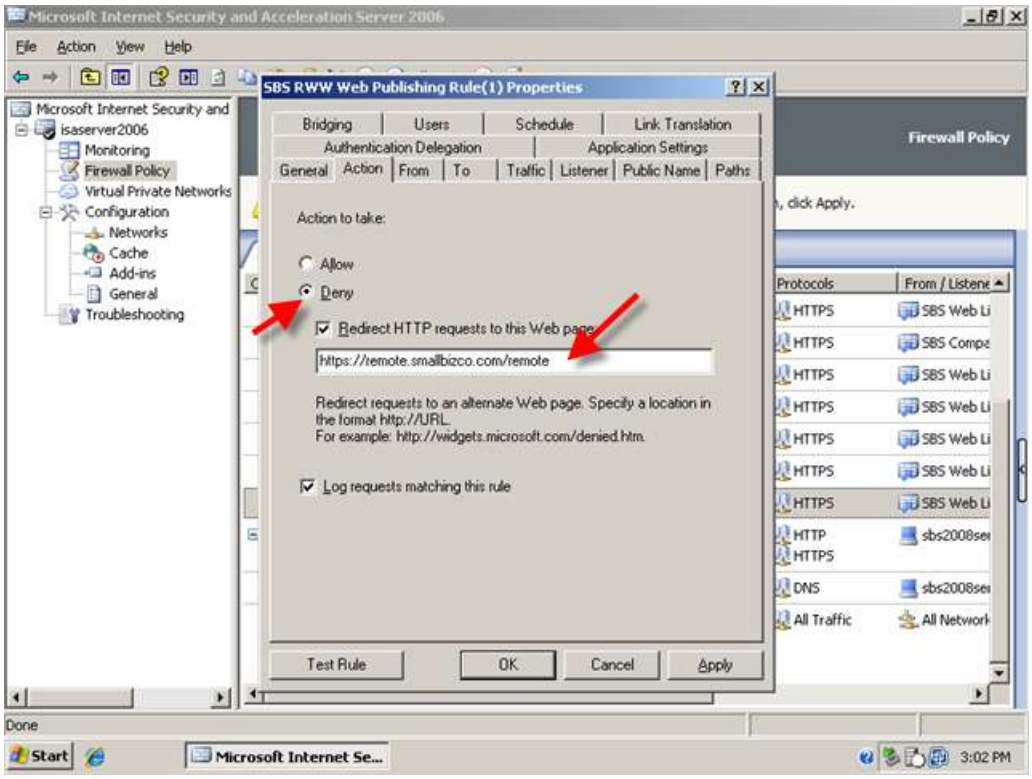
4. You will see the rule is named SBS Remote Web Workplace Web Publishing Rule(1) right click this rule, and click properties.



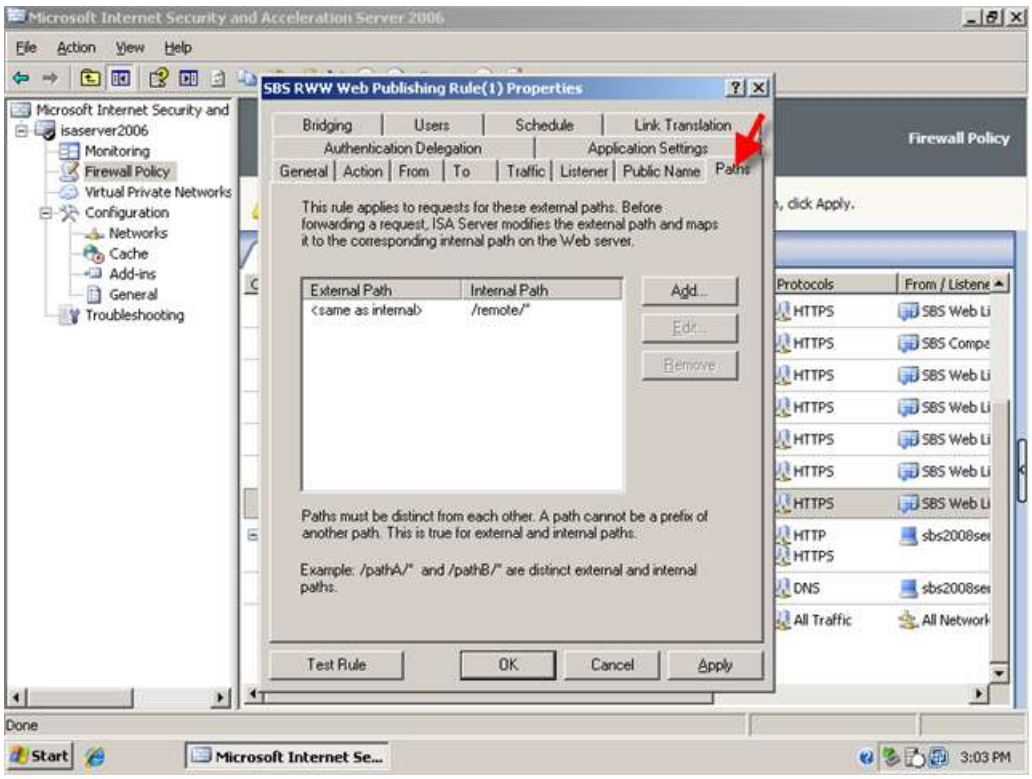
5. On the General tab we can rename the rule, I am calling my rule SBS Remote Web Workplace URL Redirect.



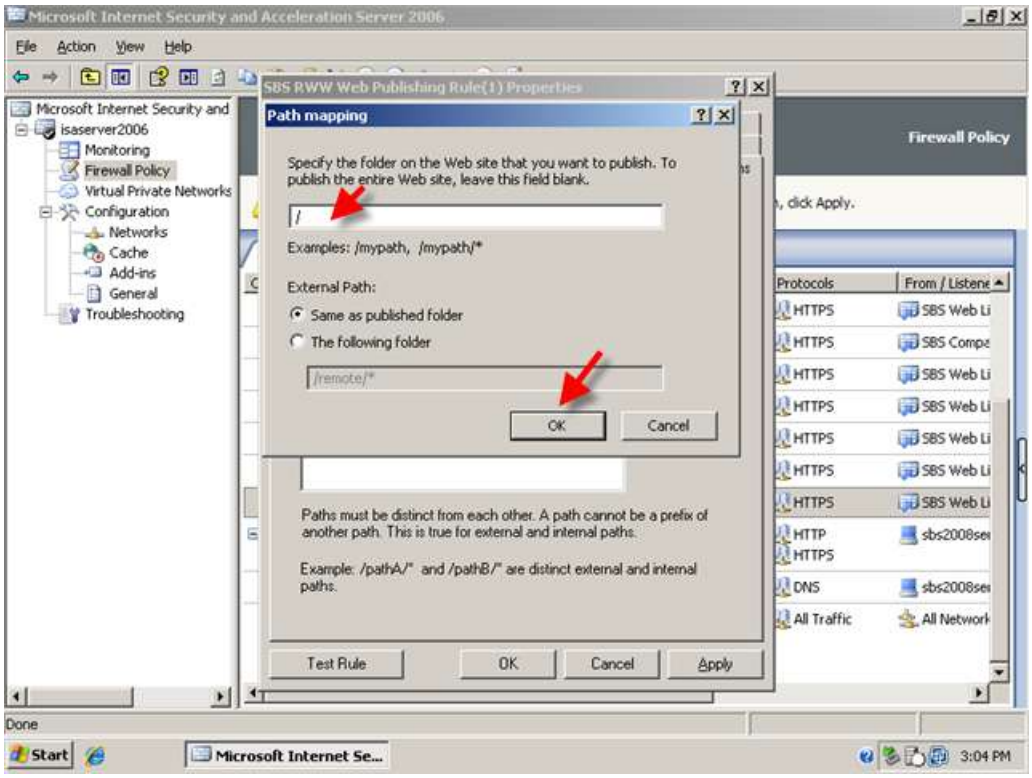
6. Go to the action tab, and change the action from Allow, to Deny. Tick the box to Redirect HTTP requests, and fill in the URL in the box – https://remote.smallbizco.com/remote



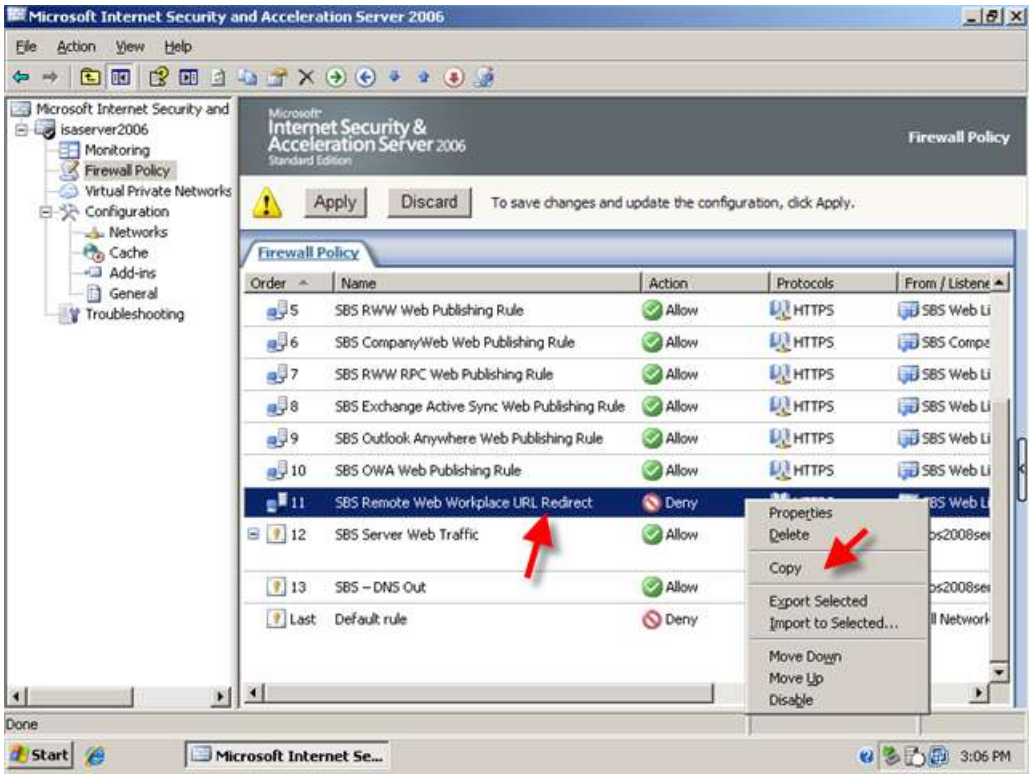
7. Switch to the Paths tab.

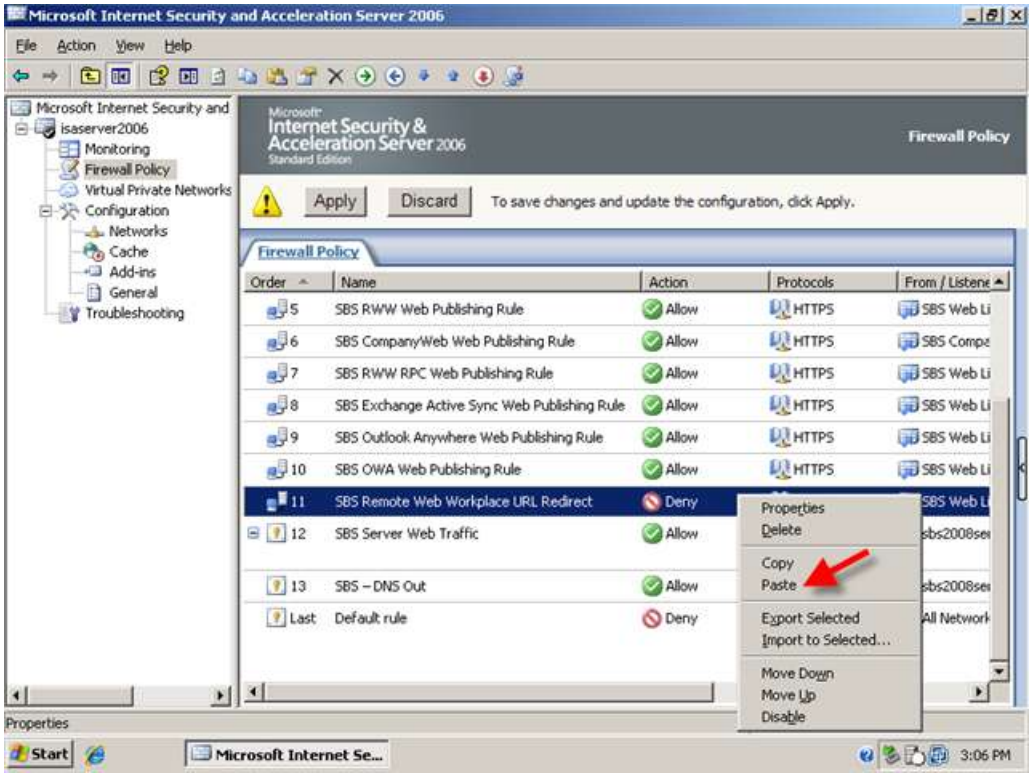


8. We need to edit the path that is used by this rule. Select the path in the list, and click Edit. Remote /remote/* from the internal site name field and leave a single / (forward slash) click Ok. Click OK to close the rule properties page.

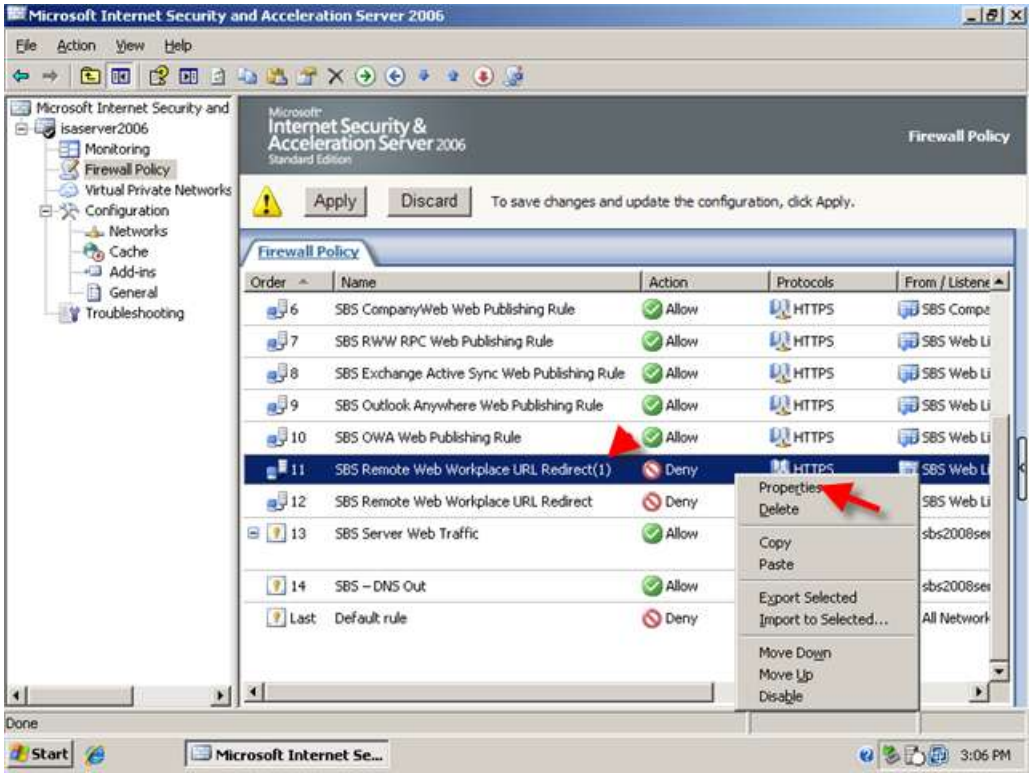


9. Your new URL redirection rule is now shown. Right click this rule and click copy, right click it again and click Paste.

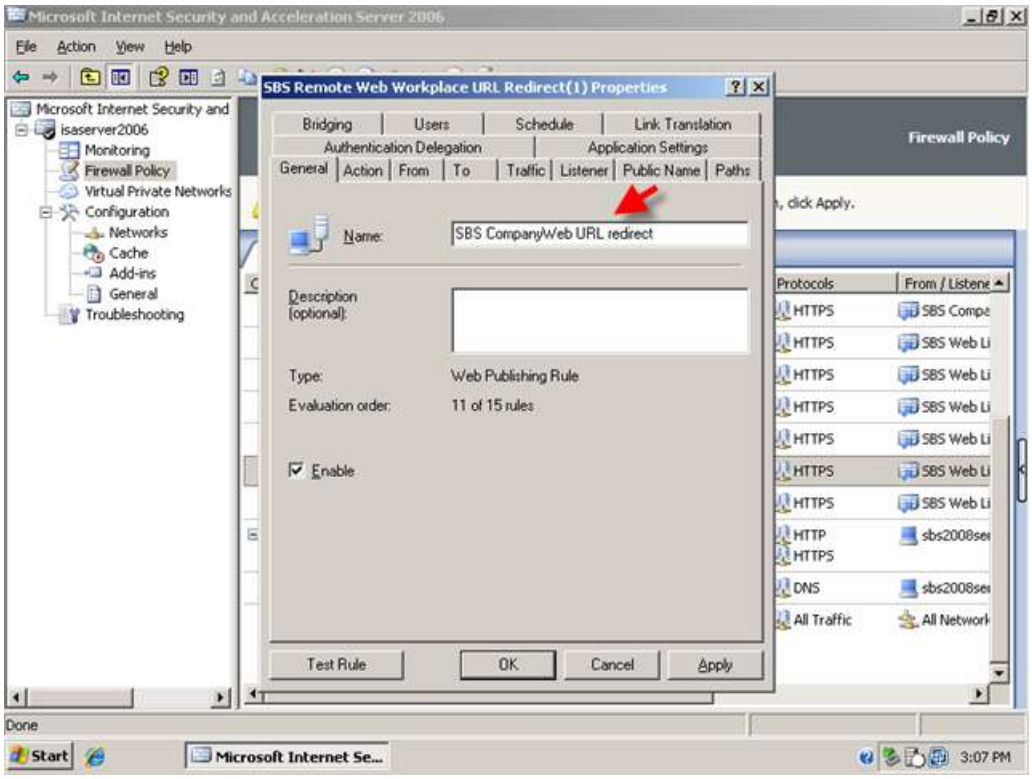


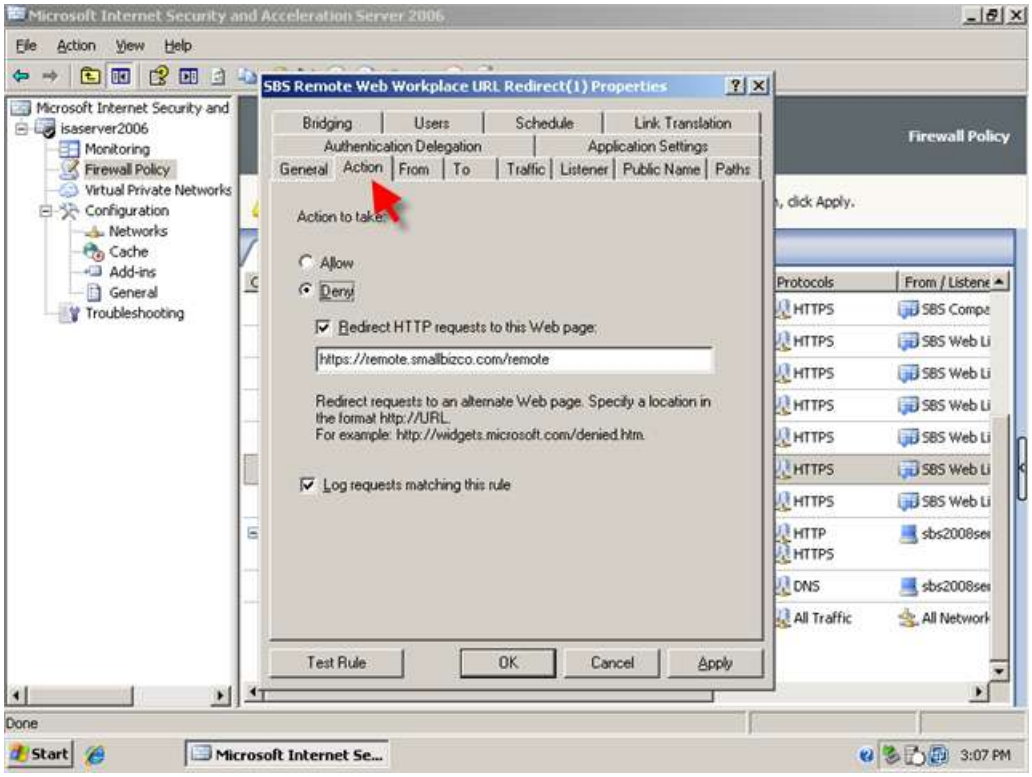


10. Again the rule is displayed with (1) at the end. Right click this rule and go to properties.

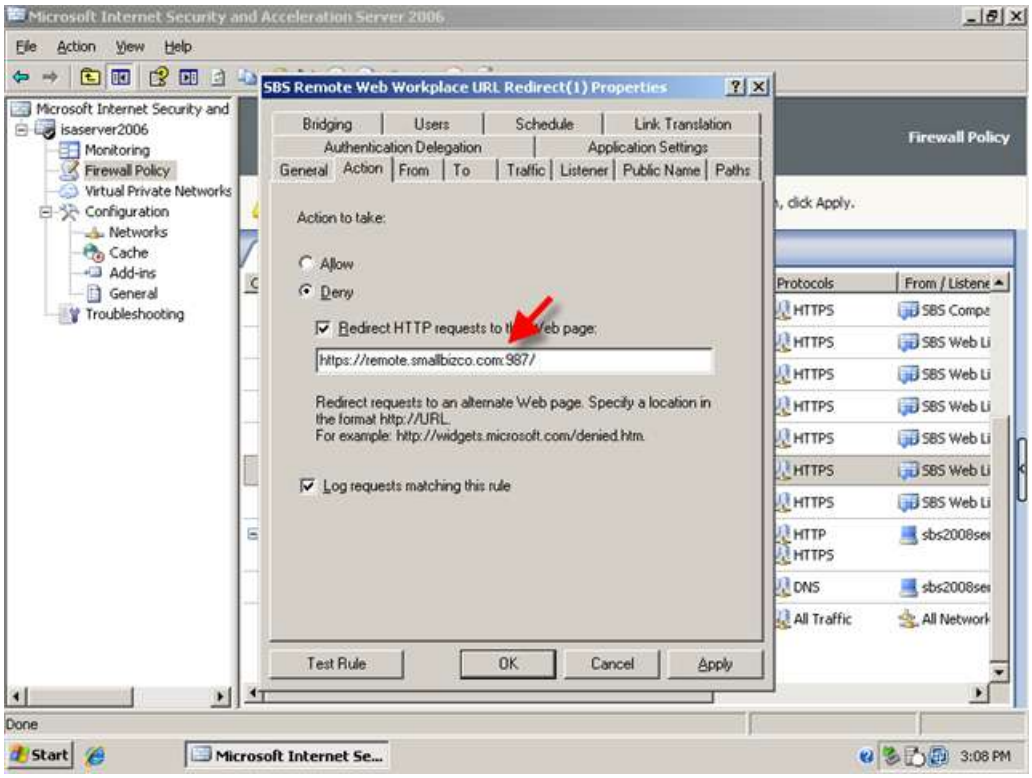


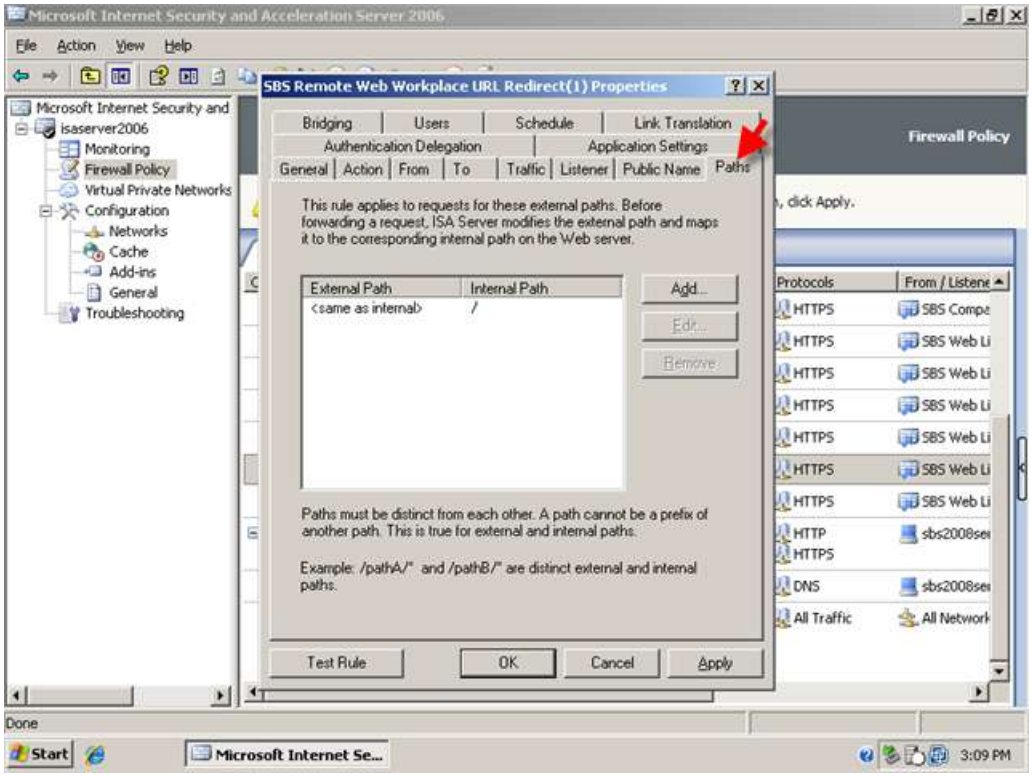
11. On the General tab, rename the rule. I am naming my rule SBS CompanyWeb URL redirect. Switch to the Action tab.



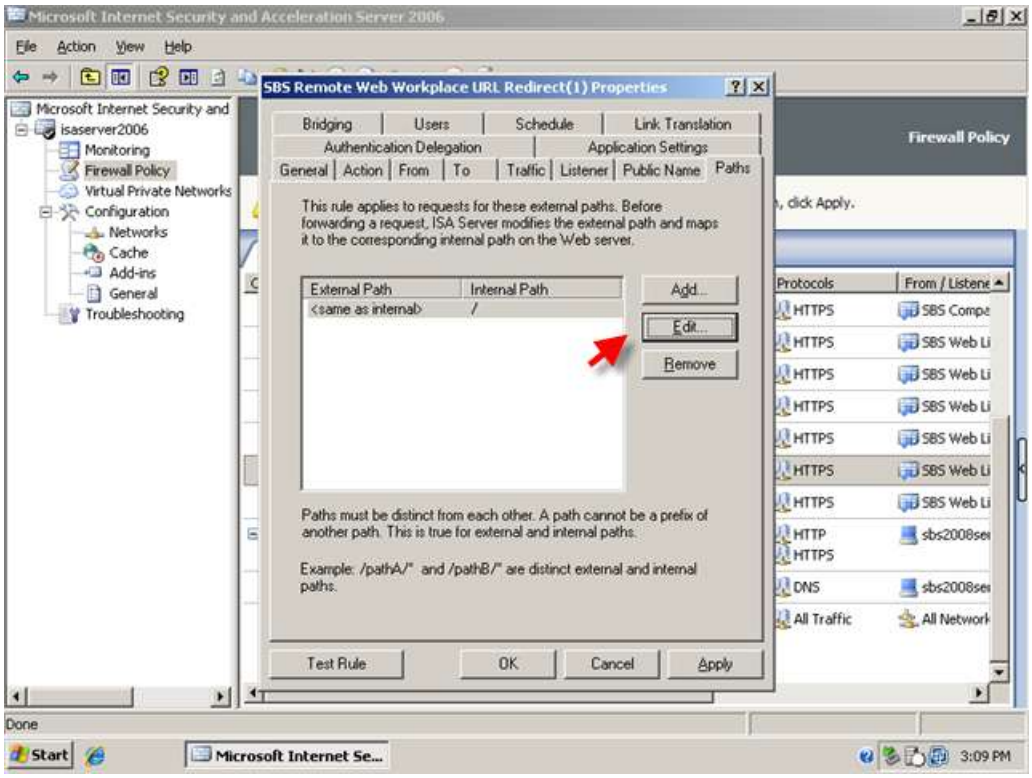


12. On the Action tab, change the URL to https://remote.smallbizco.com:987/ then switch to the paths tab.

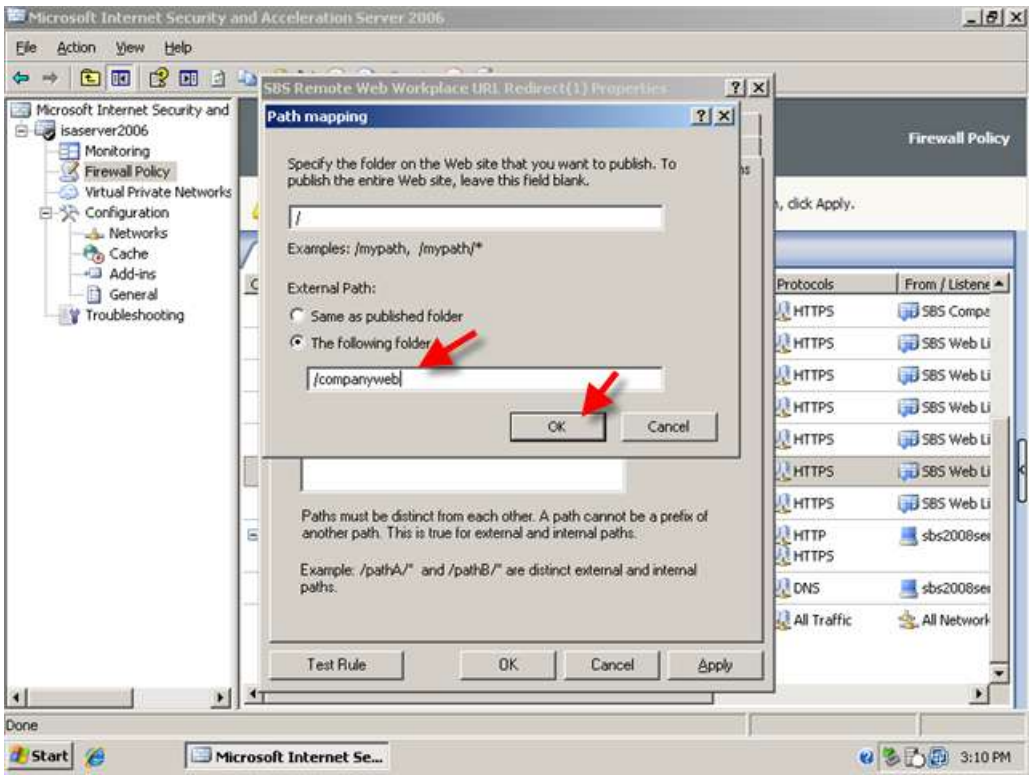




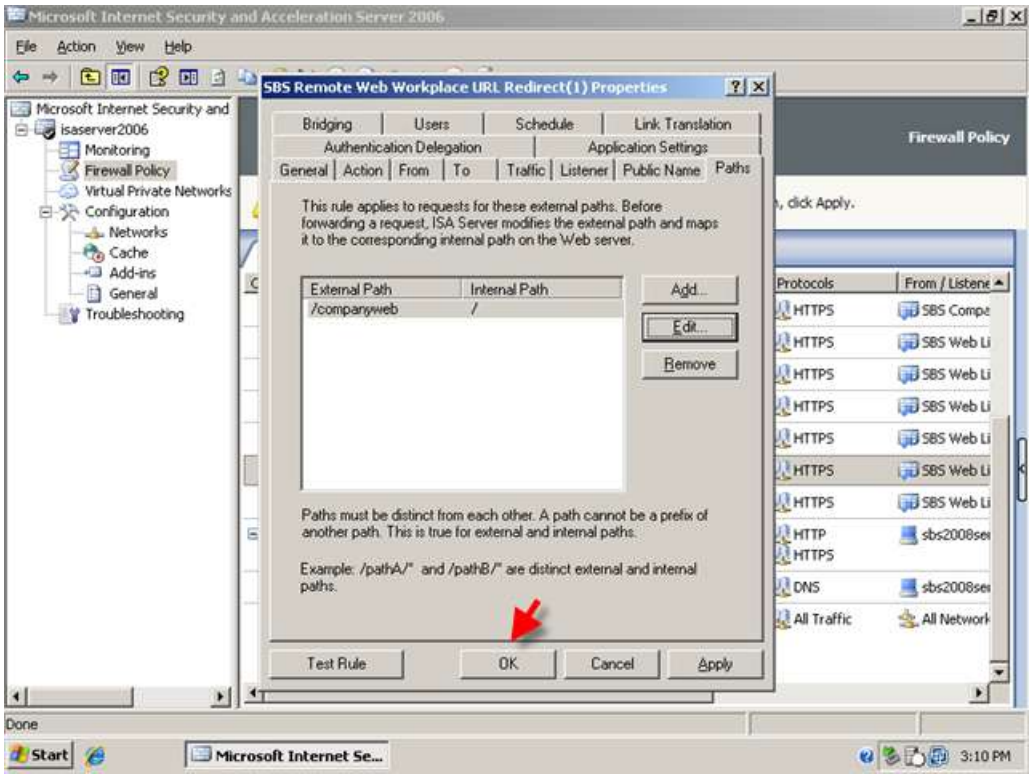
13. Select the path in the list, and click Edit.

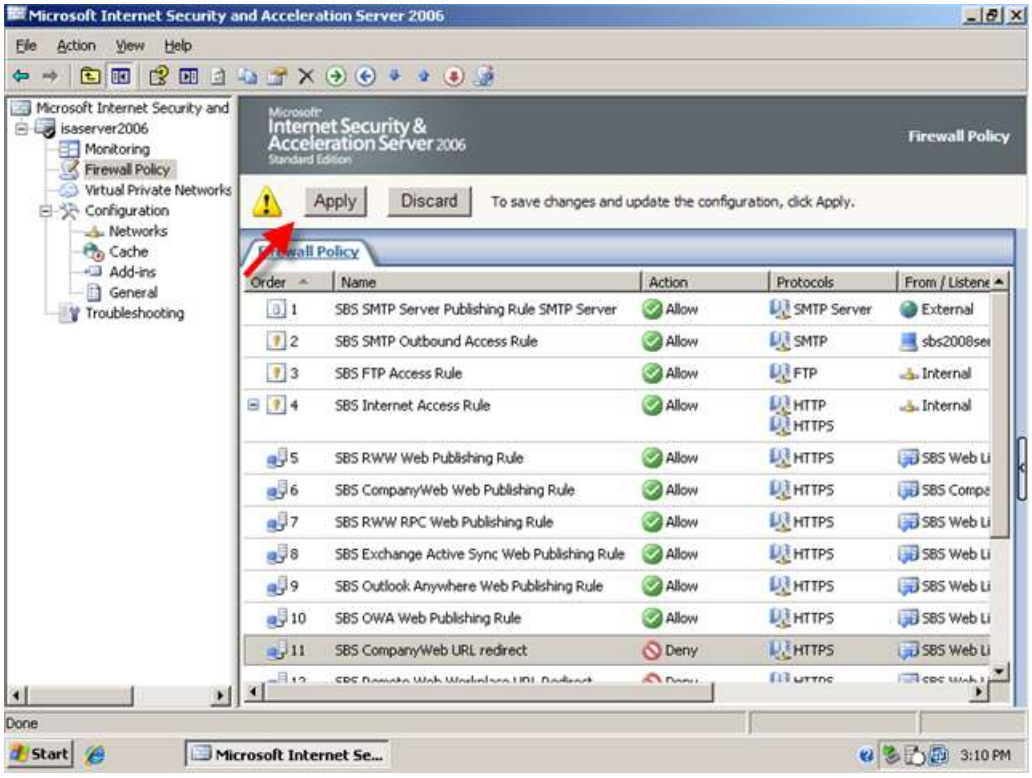


14. You can leave the internal path as a single / (forward slash) but this time, under External path, click the radio button next to 'the following folder' and in the box enter /companyweb then click Ok.



15. Click OK to close the rule properties. And click Apply to save your changes to the Firewall Policy.





You will now be able to navigate to the https://remote.domain.com page and be correctly redirected to the RWW login page and also navigate to https://remote.domain.com/companyweb and be redirected to the CompanyWeb login page. If the above does not work make sure your Deny rules are listed below the Web Publishing Rules. See screenshot: