

**White Paper   
Securing Remote Access to Exchange Server Using IPsec**

##### Greg Taylor, Sr. Program Manager, Exchange Server

February 2011

Contents

[Executive Summary 3](#_Toc277173267)

[IPSEC Secured Outlook Anywhere and Outlook Web App Overview 5](#_Toc277173268)

[How It Works 5](#_Toc277173269)

[Benefits of the Solution 7](#_Toc277173270)

[Limitations of the Solution 7](#_Toc277173271)

[Summary 8](#_Toc277173272)

[Configuration Steps 9](#_Toc277173273)

[Planning Your Deployment 9](#_Toc277173274)

[Enrolling Your Machines for Certificates 10](#_Toc277173275)

[Configuring IPsec Policies and Connection Security Rules 24](#_Toc277173276)

[Configure Forefront TMG/UAG To Allow IPsec Traffic 52](#_Toc277173277)

[Test Your Configuration 60](#_Toc277173278)

[Appendix 67](#_Toc277173279)

[Configuring IPsec Policies on a Windows Server 2003 Computer 67](#_Toc277173280)

[References 81](#_Toc277173281)

[Legal Notice 81](#_Toc277173282)

## Executive Summary

By allowing remote access to Microsoft Exchange to users who are based outside the safety of the corporate network, an organization enables its employees to take full advantage of the technology their company provides. Remote access lets employees use many devices to communicate with their peers and customers from any place and at any time.

Allowing access to corporate resources from any location, perhaps using devices that aren’t controlled by the organization, presents additional risk to the security of the data and services being accessed. Therefore it's critical to take measures to ensure that the data is being accessed securely. This means implementing technologies such as certificates, firewalls, enforcing pre-authentication, and device or endpoint validation. The key concept to understand is that applying security to any solution is a multi-layered task that includes identifying the threats, reducing the attack surface area, removing unnecessary access points, and enforcing authentication. The casual attacker will usually give up after a few failed attempts to access a resource.

Several options exist to solve some of these problems, some of which are available now, some of which require additional software or hardware, and some of which are just not well documented. An important consideration in choosing a solution is the user experience; if the solution requires a lot of user action, the result is security happiness, but user unhappiness, and usually the reverse is also true.

We do not expect that these solutions will be adopted by every customer that deploys Exchange, but that it exists as a well-documented and supported solution, enabling those customers to satisfy their security needs, but still provide their users with an Anywhere Access solution.

The options available are:

* VPN – establishing a VPN connection before connecting Outlook or Outlook Web App (OWA) allows two-factor authentication to be used, but the user experience is sometimes poor – one cannot simply launch an e-mail application and get access to their e-mail.
* Direct Access – Direct Access provides Intranet-like access from any location with no user experience issues, it’s like a VPN without the need for the user to perform any actions – but the requirements for this are significant – Windows 7 Ultimate/Enterprise is the only supported client, domain membership is required, and Forefront Unified Access Gateway is the preferred edge solution.
* Security by obscurity – using private certificate authorities to generate SSL certificates prevents machines without the root certificate from connecting – but is easy to bypass simply by installing the private Certificate Authority (CA) certificate as ‘trusted’.
* Using IPsec to secure the HTTPS connection – When IPsec is enabled and required on the endpoint used for publishing Exchange to the Internet, only machines with the right credentials (a certificate is preferred but a passphrase can also be used) can establish a connection. Outlook and OWA then authenticate as usual, as they have neither visibility into nor involvement with the network security layer.

If a customer wants a solution that works with all versions of Exchange Server, and can be deployed today, without significant additional investment, IPsec is an attractive solution.

When you publish Exchange, Microsoft offers two software-based options: Microsoft Forefront Threat Management Gateway 2010 (Forefront TMG) and Microsoft Forefront Unified Access Gateway 2010 (Forefront UAG). Both options offer publishing wizards and security features to provide secure access to Exchange when it's accessed from outside the safety of the corporate network and both work well with an IPsec based security solution.

There are other ways to publish Exchange besides using Forefront TMG or Forefront UAG. This technical guide isn’t intended to provide the only information you use for a complex organization or one with special security constraints. Instead, it’s intended only as a walkthrough to help you publish Exchange using IPsec on both these platforms, using common configuration options. If you have a large organization, it’s likely that you’ll need additional applications or have to factor in additional considerations. Such applications and security considerations are beyond the scope of this document.

**Acknowledgements**

Based upon a Proof of Concept by Sasa Vidanovic of Microsoft Consulting Services

**Document Reviewers**

Jim Harrison, Program Manager, Anywhere Access Team

Ross Smith IV, Principal Program Manager, Exchange Server

Ian Parramore, Escalation Engineer, Forefront TMG

## IPSEC Secured Outlook Anywhere and Outlook Web App Overview

### How It Works

In the simplest terms, using IPsec to secure communication between a client machine and the server publishing Exchange, results in both computers agreeing to communicate with each other, and securing that connection, before presenting the user or application any opportunity to log in, or launch some kind of attack. Without the two computers agreeing to communicate, no attempt to access data, whether for valid reasons or not is allowed. The success or failure of the solution depends entirely upon the criteria used by the computers to establish and manage the initial connection. If that process is solid and robust, tight control over the communication process is assured. If it is not, the opposite is true.

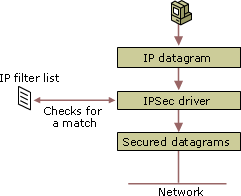
There are several key components that must be configured to enable this solution end to end;

* **Certificates** – both the client and server must have certificates installed that include the correct usage type, and are issued by a trusted certificate authority (CA).
* **Certificate Revocation List** – Certificate Revocation Lists (CRL’s) are used when validating a certificate to ensure it has not been revoked – these lists are typically published to a web server, and in the case of an Active Directory (AD) integrated CA, to AD itself.
* **IPsec policies** – both the client and server require a policy to be configured which specifies the need for IPsec to be used on the specified connection, the type of authentication that connection will use, and the encryption or security settings the connection will apply.
* **Firewall rules** – IPsec uses two different UDP ports (UDP 500 or UDP 4500) and depending on the IPsec policy defined, one of two IP protocols (ESP (IP:50) or AH (IP:51)) during negotiation and connection. These ports must be opened on the server to allow inbound connections to be established. Additionally a small change may be required at TMG/UAG to allow the server to ignore the mismatch between the TCP checksum and the calculated checksum, which can happen as a result of the NAT-T IPsec process.

Planning for a Public Key Infrastructure (PKI) itself is outside the scope of this document as the scope and impact of a PKI is usually far wider than for specific solutions such as IPsec. For this reason, we recommend you use the resources provided at the end of this guide, and engage additional assistance if required.

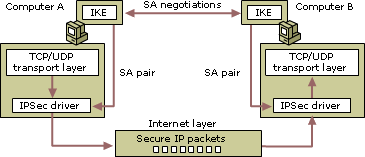
For the purposes of this document, it is assumed that an Enterprise (AD integrated) CA has been successfully deployed with standard configuration options. Once this PKI is in place, all domain member client machines that will use IPsec should be enrolled for machine certificates. The standard ‘Computer’ template provided by a Windows PKI is suitable for this purpose, and it’s simple to configure all domain member computers to automatically enroll for this type of certificate. A simple example showing how to do this is provided later in this document. Creating and using a template for use by non-domain joined computers is also discussed later in this document.

Once the appropriate certificates are in place, IPsec policies and filters need to be created on both the client and the server.



The configuration of the IP Filter List policy can be distributed through AD Group Policy to the client machine (the server policy can be optionally configured this way too). The client is configured so that it will negotiate IPsec when connecting to a specific IP address or subnet and port, and to authenticate that connection using a certificate or pre-shared keys (PSK). Pre-shared keys are generally only useful for testing, because if this were compromised, every host using PSK for IPsec would need updating. The resulting threat window is a large as the time it takes to discover the compromise plus the time it takes to change the policies on each host.

Once the policies have been configured, the operating system detects an IP datagram that matches a policy and the policy is applied as defined.



In the case of a policy that requires the client and server negotiate IPsec when connecting to a specific IP address and port, the client first performs an Internet Key Exchange (IKE) or AuthIP negotiation with the endpoint over UDP 500, or UDP 4500 if (Network Address Translation) NAT is detected. The two machines negotiate a level of encryption/authentication before establishing a Security Association (SA). The SA is subsequently renewed based on either a time interval or the amount of traffic processed.

Once the SA is established, Outlook, OWA or any client is then able to establish a TCP or UDP connection to the remote host. If Outlook or OWA are closed the SA remains open until the expiration of the connection, or until one party disconnects.

The decision as to whether IKE or AuthIP is used is based primarily upon the version of the operating system in use. Windows Vista, Windows 7 and Windows Server 2008 and newer prefer to use AuthIP (an enhanced version of IKE) to establish IPsec security associations. All these operating systems also support IKE, and will in fact use it when connecting to machines that only support IKE. There is one subtle but important difference between these two methods of authentication when using computer certificates however; IKE authentication requires only the ‘Digital Signature’ usage type on the certificate, but AuthIP requires the certificate has the ‘Client Authentication’ usage type. For this reason, the certificate templates described later in this document have both usage types present, to avoid any potential implementation problems.

The ability of you, the administrator, to control which clients can or cannot connect ultimately becomes a function of how the PKI is managed. Machine certificates cannot be exported and copied from one machine to another by default, so only machines that can enroll or are provided with a certificate can connect. If a certificate is revoked, then the client is only able to connect for as long as it takes for the admin to revoke the certificate and for the systems involved to recognize that change. As with the shared key, the threat window is as large as the time it takes for the compromise to be discovered plus the time it takes for the PKI admin to revoke the certificate. The breadth of the threat itself is limited to one client computer, rather than all of them as is the case for PSK.

### Benefits of the Solution

* Clients establish a secure connection to the server with no user or application interaction or visibility. IPSEC operates at Layer 3 of the OSI model (Network).
* Only clients with a valid machine certificate issued by a CA that is trusted by the service endpoint can connect and authenticate. The possibility of Denial of Service (DoS) attacks is reduced as any attempt must first succeed at the IPSEC negotiation layer rather than the username/password layer, which is much harder to exploit. Essentially, this ensures that only ‘trusted’ machines can make inbound connections.
* Works with AutoDiscover, Exchange Web Services (EWS), Outlook Anywhere (OA),and OWA.
* When combined with computer lock policies, this solution could be considered two factor authentication – something you have (the certificate) and something you know (your password).
* Works with NAT and all versions of Windows later than XP SP2.

### Limitations of the Solution

* If the IP address of the service endpoint is changed, the policy becomes outdated and a service outage is in effect until the IPSec policy is updated on all clients. Policies are based on IP address, not fully qualified domain names.
* Performance impact – the performance impact is a potential consideration, though some network cards offer offload capability if performance is a concern. The encryption computation is performed in kernel mode and estimated in most cases to be less than that required for SSL. Additionally an organization has the choice of Integrity and encryption, or Integrity only – as the traffic is already encrypted in SSL, only ensuring data integrity allows the solution to work, but does not result in double encryption of traffic.
* Windows Mobile (WM) does not natively support IPsec in this peer to peer fashion, so cannot utilize the solution; however third party IPsec solutions do exist for WM and other platforms.
  + If Exchange ActiveSync clients are used, AutoDiscover would need to be on a separate IP address from OA, so it can be excluded from IPsec and still used by mobile devices, or a third party IPsec client could be installed on the mobile device.

### Summary

Using IPsec to secure access to Exchange provides an answer to many customers who have security concerns around the security of Outlook Anywhere and OWA access. By restricting the ability to authenticate to devices that possess a certificate and can establish an SA, you can allow only managed devices to access the service. Coupled with support for offline enrollment, and revocation, you can tightly control who can connect to your published service.

## Configuration Steps

Configuring IPsec to secure Exchange communications is a multi-step process. Exchange is unaware of IPsec being used to secure the traffic, and so configuration of Exchange itself, and the steps required to publish Exchange using Forefront TMG or UAG are not discussed in this Whitepaper. For detailed instructions on configuring and publishing Exchange see the following document - “[White Paper – Publishing Exchange Server 2010 with Forefront](http://go.microsoft.com/fwlink/?LinkId=197136)”

It is assumed that you have successfully configured Outlook Anywhere and OWA publishing using either Forefront TMG or UAG prior to beginning this walkthrough.

To secure the traffic between the client machine and the system publishing Exchange, assumed in this document to be either Forefront TMG or UAG, you need to complete the following steps;

Your deployment may require further configuration and customization, though this document is provided to allow you to configure and deploy a complete end to end solution using common configuration defaults.

### Planning Your Deployment

Introducing new technology always requires careful planning and a thorough understanding of the impact of any decisions you make. Deploying IPsec is no exception to this, and because the technology is largely unfamiliar to many people, it sometimes results in deployment challenges and extended troubleshooting. Careful planning is critical to avoiding these problems and ensuring you have a successful deployment.

This solution requires configuration of Windows, Group Policy, certificates, Exchange, networking and other technologies and therefore is likely to affect or require assistance from multiple teams within your organization. It is fundamental to the success of any project involving many people of teams to work together to agree on goals and responsibilities before the project begins.

Some of the questions you may need to address early on in your project are shown below, but almost certainly others will apply based on your specific requirements. This list is provided to get your project started and help begin the planning process.

* Do you already have an existing PKI? What is it used for?
* If you don’t have a PKI, what other requirements do you have for a PKI? Deploying a PKI for just one application is fine, but if you can plan ahead for future requirements you might do things a little differently, saving yourself future changes.
* What process will you follow for issuing certificates? Are there any special approvals required?
* Will you allow automatic enrollment for certificates?
* What lifetime do you want to use for each certificate?
* What process will be used for revoking certificates?
* Can you use Group Policy to distribute IPsec policies?
* Do you require AutoDiscover for mobile devices? If so, make sure you use different IP address externally so that AutoDiscover allows connections from non-IPsec clients.
* How will you communicate changes to your users?
* How will you test the configuration without impacting production?
* How will the solution work if you also have disaster recovery processes? If your policies do not include every IP address a client may contact, the policies will not be used.
* How will you respond to IPsec authentication compromise (PSK or certificates)? Who needs to be involved and what is the reaction process?

Once you have answers to help you in your deployment, consider building a test lab which mirrors your production environment, and using that to test your design.

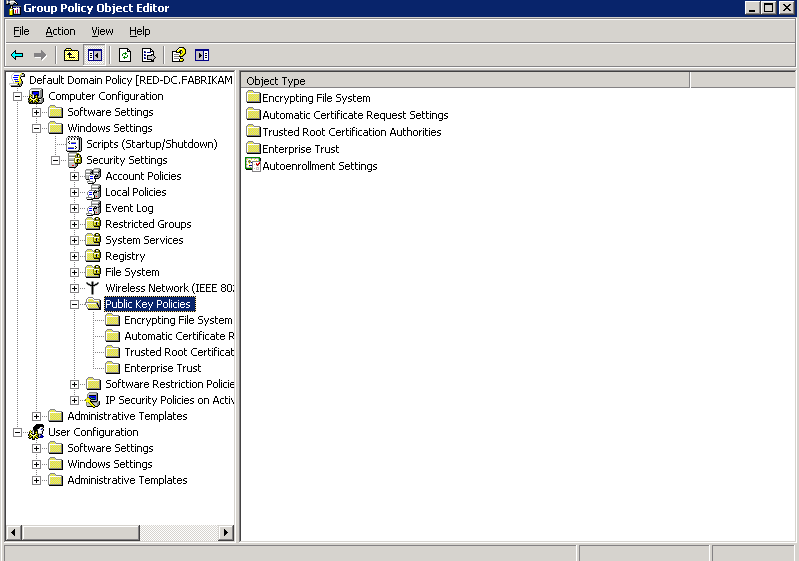
### Enrolling Your Machines for Certificates

Once your PKI has been designed and deployed, you can deploy certificates to any and all client machines that you want to use IPsec when accessing Exchange from outside the corporate network. Assuming that the certificate template you choose allows for automatic enrollment this can be done easily using a Group Policy Object (GPO) and enables all domain joined machines within the scope of the GPO to automatically enroll. It is important to note that this requires that the CA be installed on the Enterprise version of Windows Server.

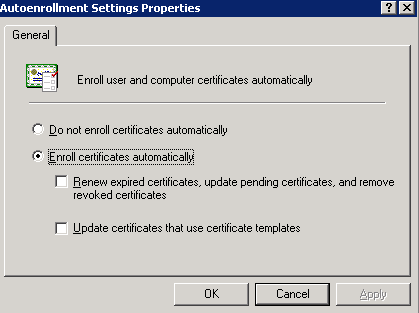
#### Configuring Auto Enrollment Using a Group Policy Object

Once you have decided upon the location of the GPO in AD perform the following steps.

1. Navigate to the **Computer Configuration, Security Settings**, and **Public Key Polices** node of the policy object.



1. Open the **Autoenrollment Settings** object and simply check the radio button for **Enroll certificates automatically**.

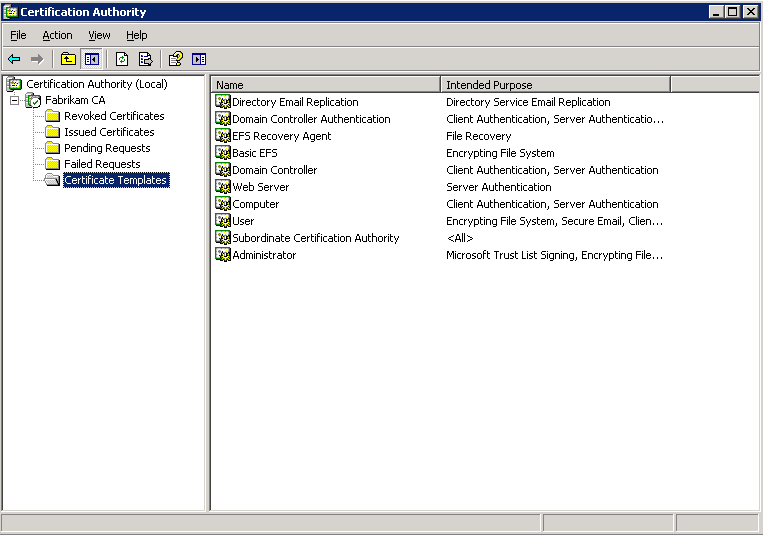


1. When the clients next apply the applicable GPO they should receive a certificate via automatic enrollment.

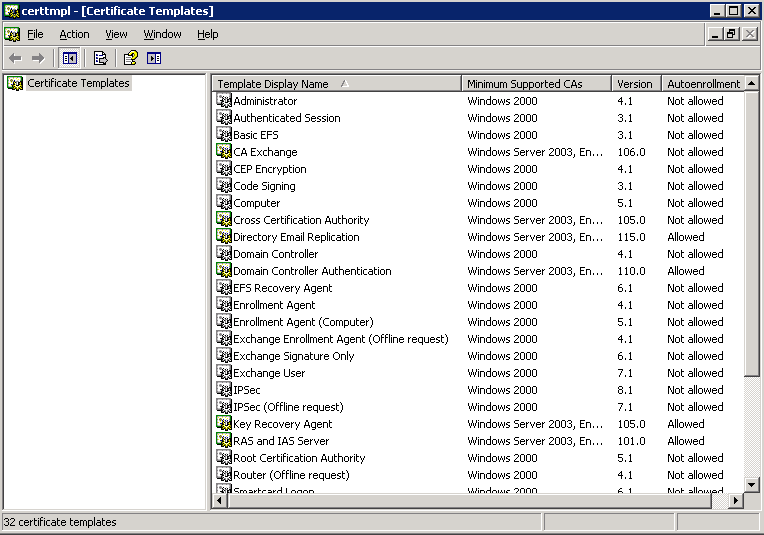
#### Providing IPsec certificates to non domain joined computers

If you wish to enroll non domain joined machines for computer certificates you can perform the following steps. Some of these steps may be difficult for non-technical users and may require utilities not present in older, or locked down operating systems. If that is the case, you need to consider during the planning stages of the deployment how you will enroll these machines for certificates. The machine that will be accessing the IPsec secured service must be used to perform the client side actions, to assure security. If you change the certificate template to allow certificates to be exported from one machine to another you remove a significant component in the security of the solution.

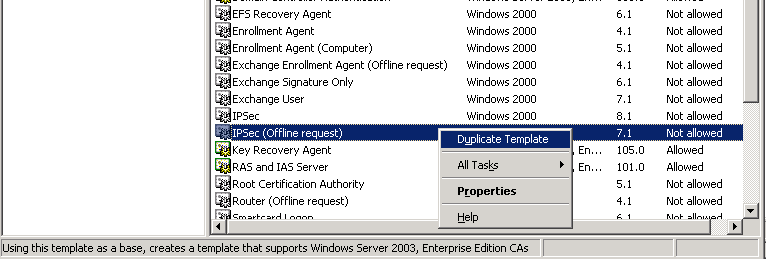
1. On the Windows Server Enterprise Edition that hosts the CA, open the **Certification Authority** management console.



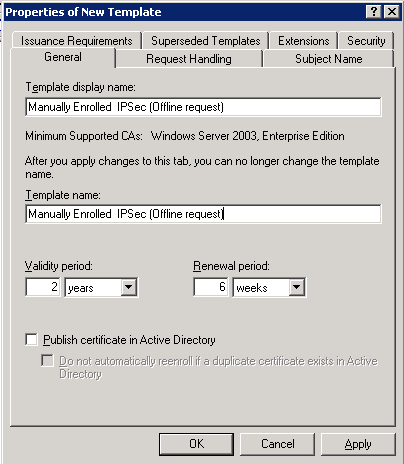
1. Right click the **Certificate Templates** node and choose **Manage**.



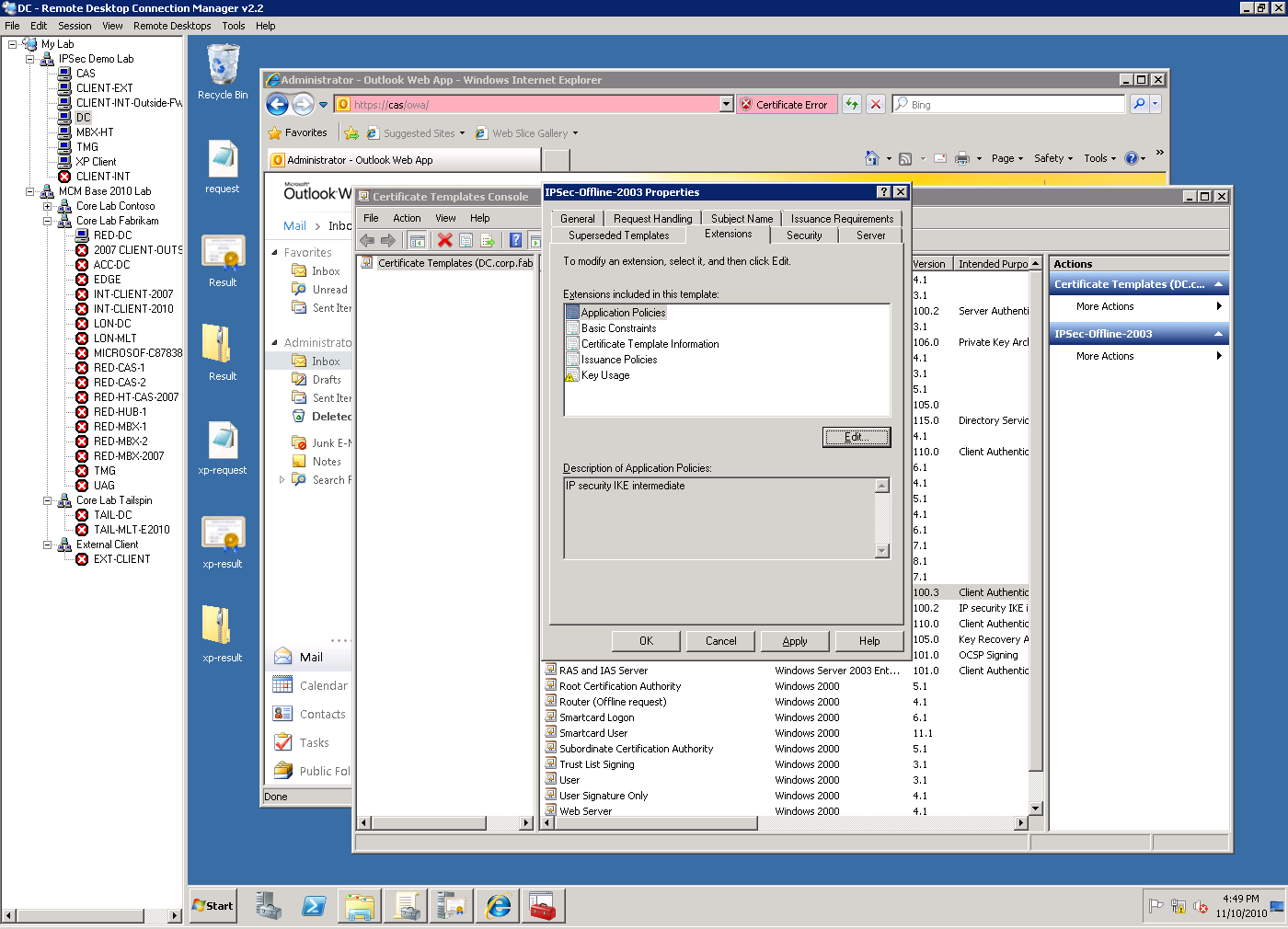
1. Right click the **IPsec (Offline Request)** template and choose **Duplicate Template**.



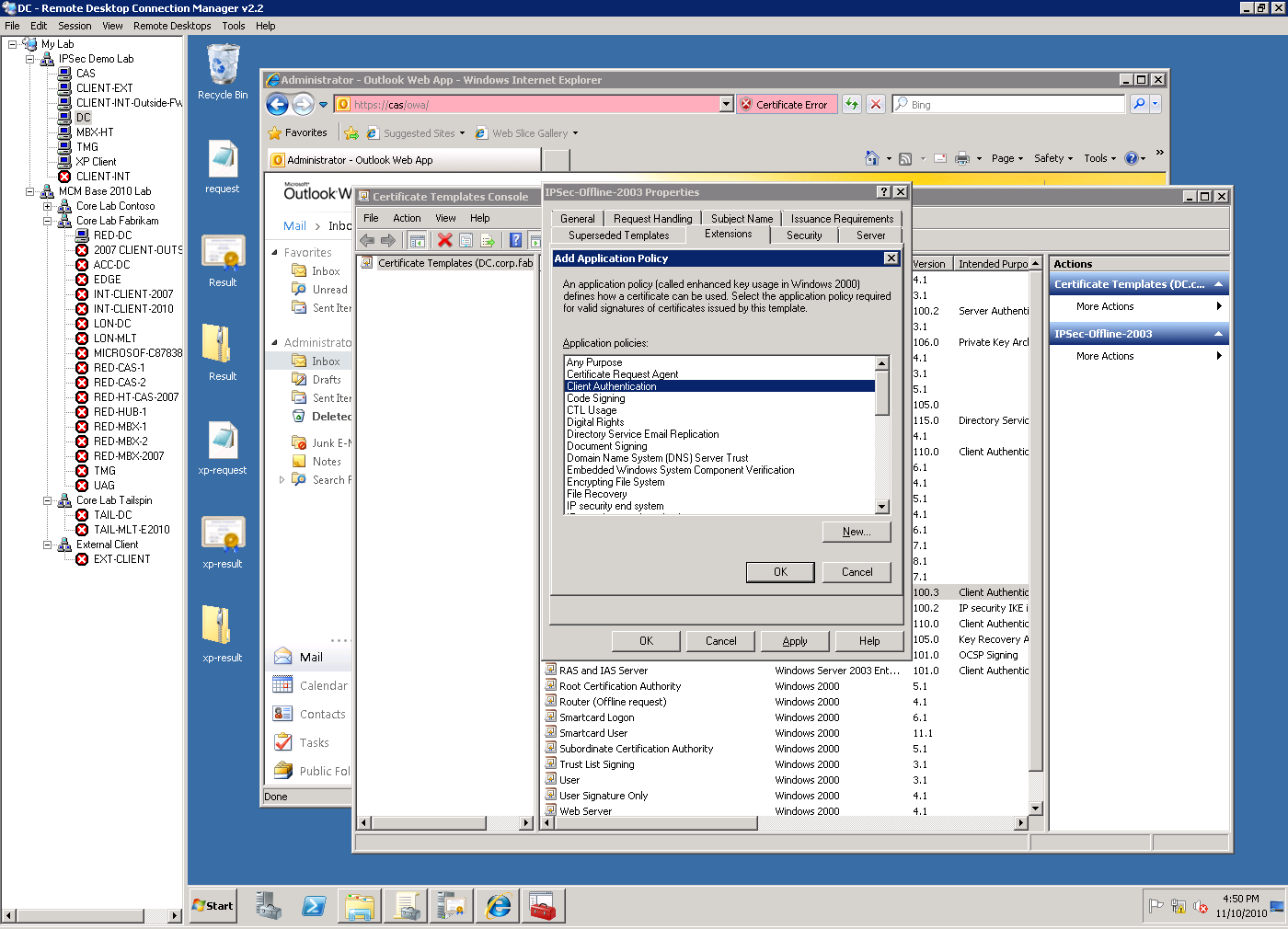
1. Give the new template a meaningful display and template name. If you wish to adjust the validity and renewal settings you can do so here.



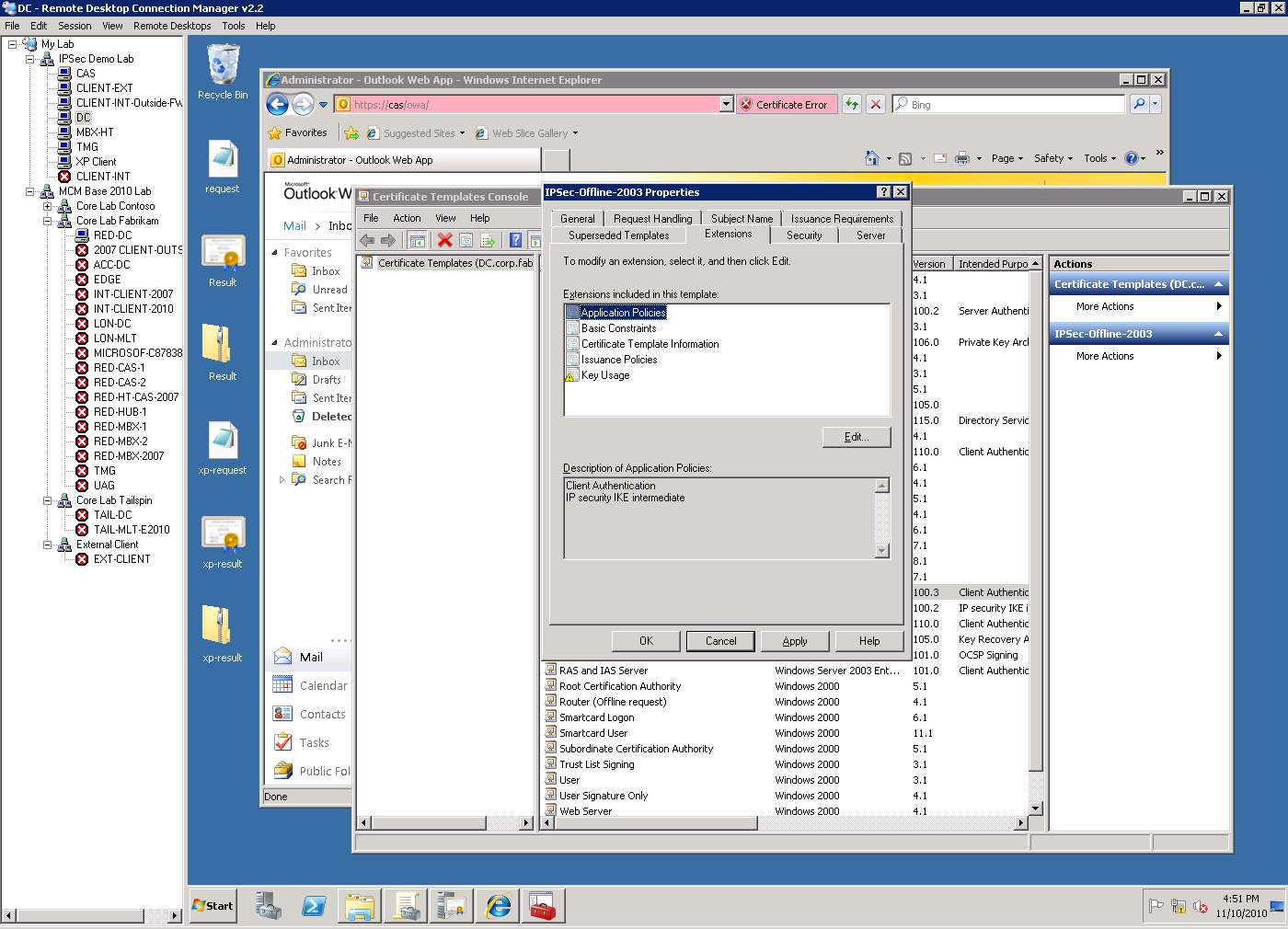
1. Go to the **Extensions** tab, select the **Application Policies** extension and click **Edit**.



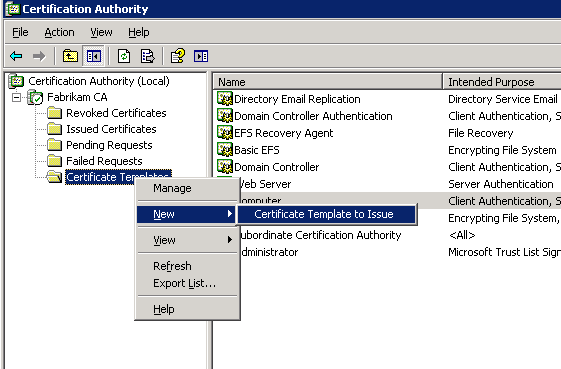
1. Click **Add**, then select **Client Authentication** and click **OK**.



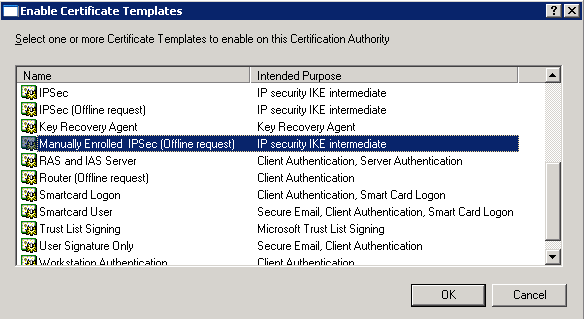
1. Click **OK** again and confirm the certificate template now shows **Client Authentication** as well as **IP security IKE intermediate** when **Application Policies** is selected. This ensures this certificate can be used for both IKE and AuthIP IPsec tunnel negotiation.



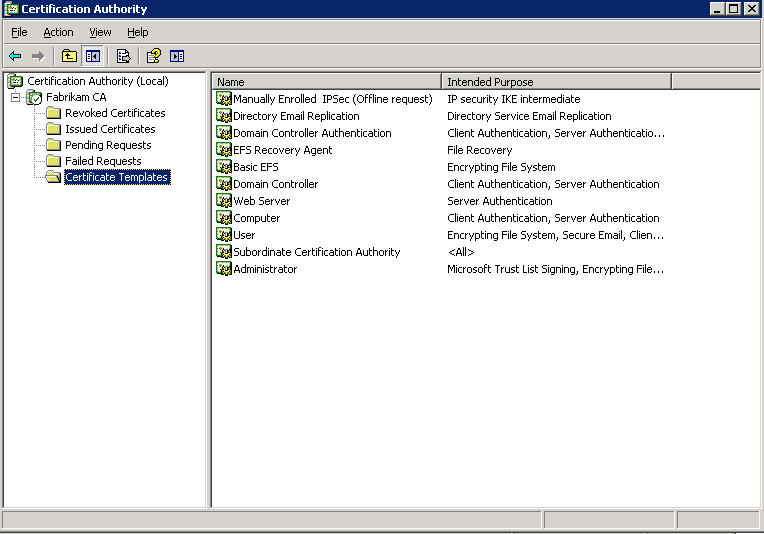
1. If you wish to adjust other properties of the template, such as specify the approval process, you can do so on the other property pages of the template. When finished click **OK**.
2. Close the Certificate Templates management console.
3. In the Certification Authority console, right click the **Certificate Templates** node and choose **New > Certificate template to issue**.



1. Select the previously created template and click **OK**.



1. The new template is now shown in the Certification Authority console.



The next step is to generate a certificate request on the client machine, specifying the necessary parameters that should be contained in the final certificate.

You could write and distribute a script to perform this action, which minimizes user impact, or you can create an .inf file and provide it to the user. You should decide an appropriate method during your planning phase. Either way, the name of both the client machine and the certificate template you created earlier are required for the enrollment.

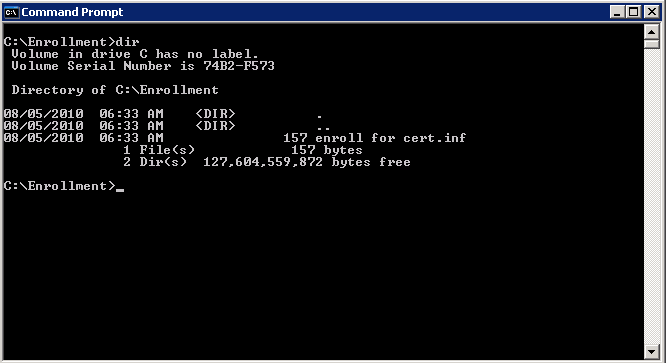
If you decide to use an inf file, and once you have the required pieces of information you can create a text file in this format; (do not include the text shown in red in the actual file you create)

|  |
| --- |
| [NewRequest]  Subject="CN=client-ext.test.com" ; NOTE: The FQDN you use here is that of the client machine, provided by the user  MachinekeySet=TRUE  KeyLength=2048 ; NOTE: This value minimum varies by version of CA so check what Key Lengths are supported.  [RequestAttributes]  CertificateTemplate="Manually Enrolled IPsec (Offline Request)" ; NOTE: This is the name of the template you created earlier |

Either send the body of the file as a text file to the user with instructions on how to save the file with an .inf file extension, or distribute the file using some other approved method. Note that distributing a file with an .inf extension via e-mail may result in the file being blocked or stripped.

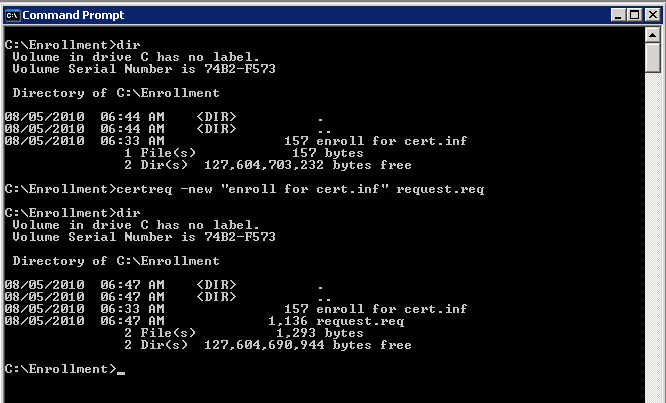
Once the user is in possession of the file, and is using the machine they wish to enroll, ask the user to perform the following steps;

1. Open a command prompt and navigate to the folder or location containing the inf file.



1. At a command prompt run the following command: **Certreq –new <pathtoinf> <outputfile> substituting parameters as required. For example, the following command: Certreq –new –enroll for cert.inf request.req results in the request file being created in the same location as the inf file if the current directory contains the inf file being used.**

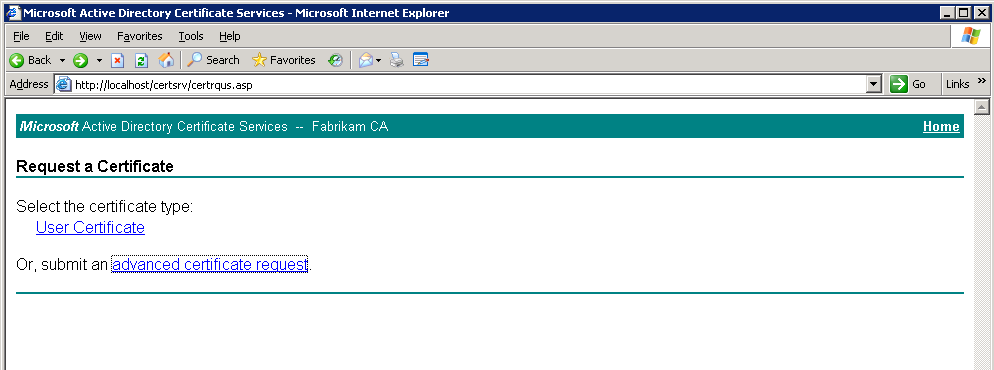
**Note: If the machine running this command does not recognize the Certreq command (Windows XP clients typically do not have the utility available unless the Windows Server Administration Tools have been installed) you may need to investigate alternative ways to generate certificate requests.**



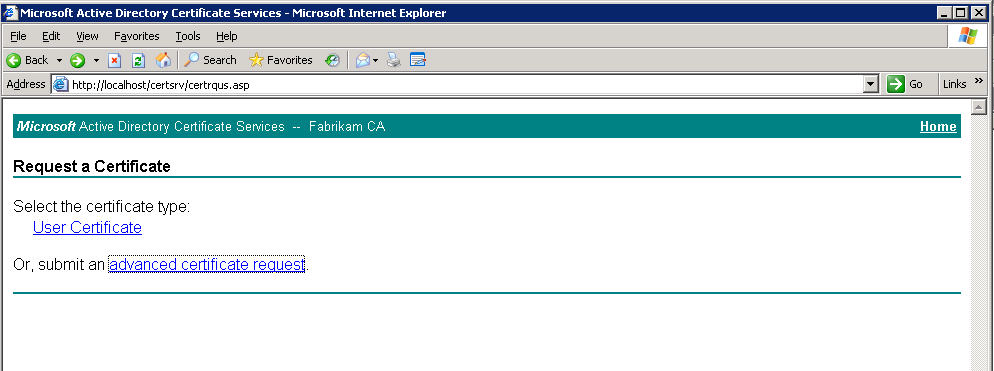
1. The user should then return the resulting req file to the CA administrator. Note this file type can usually be sent via e-mail without being stripped or blocked.

The administrator must then complete the enrollment on behalf of the user.

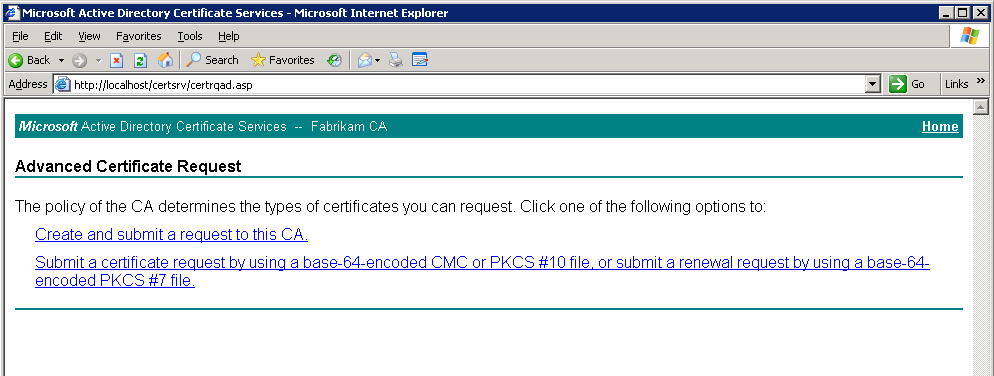
1. If the CA is based on a Windows Server 2003 machine, the CA administrator can fulfill the request by using the Certificate Services web enrollment service (see the next section for a procedure required for a Windows Server 2008 or later CA). The CA administrator first browses to the web enrollment page of the Certificate Authority.



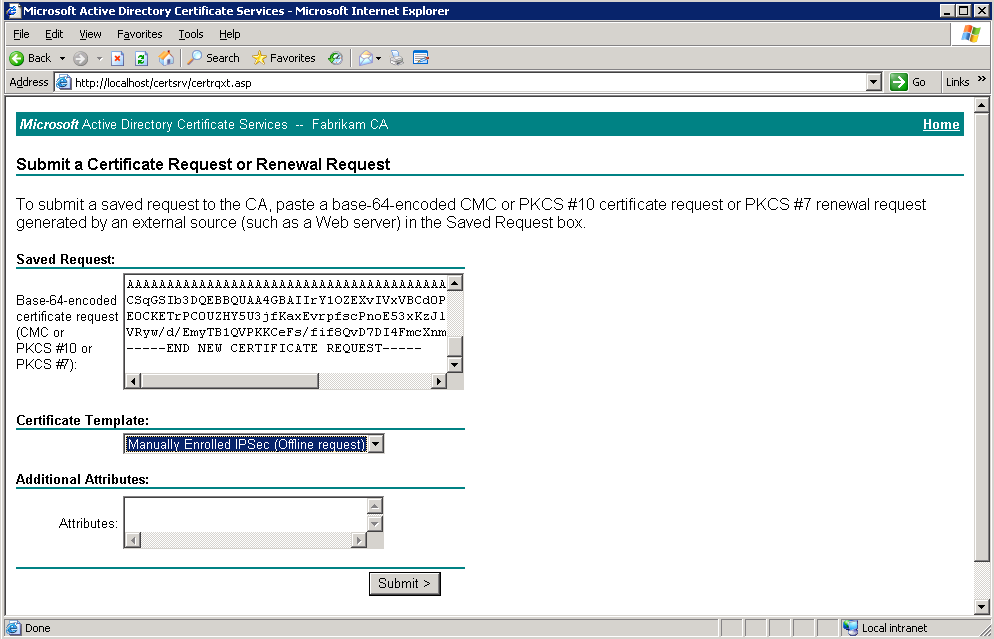
1. The CA administrator clicks the **advanced certificate request** link.



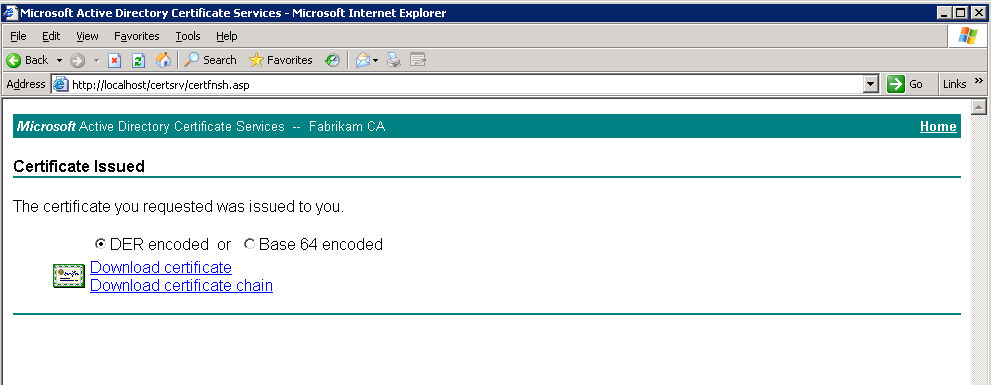
1. The CA administrator then clicks the **Submit a certificate request by using**… link.



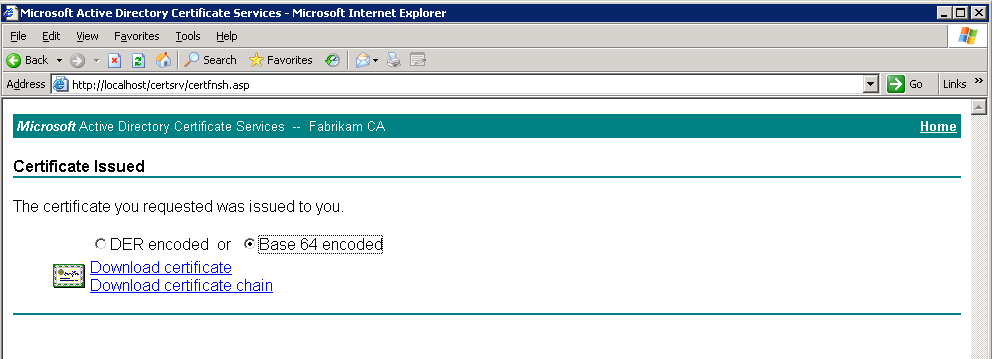
1. The CA administrator pastes the contents of the req file (which can be easily opened using Notepad) into the **Saved Request** field of the page. The CA administrator then chooses the IPsec offline request template created earlier from the **Certificate Template** drop down list.

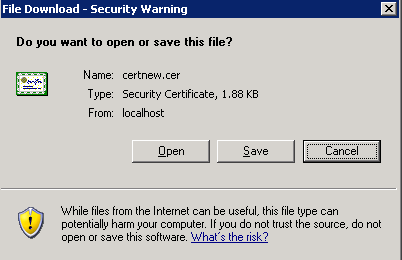


1. The CA administrator then clicks **Submit**, and once any approval process is complete (if one was enabled for the template being used) the certificate is made available.



1. The CA administrator checks the radio button next to **Base 64 encoded**, and clicks the **Download certificate** link to download a copy of the certificate.

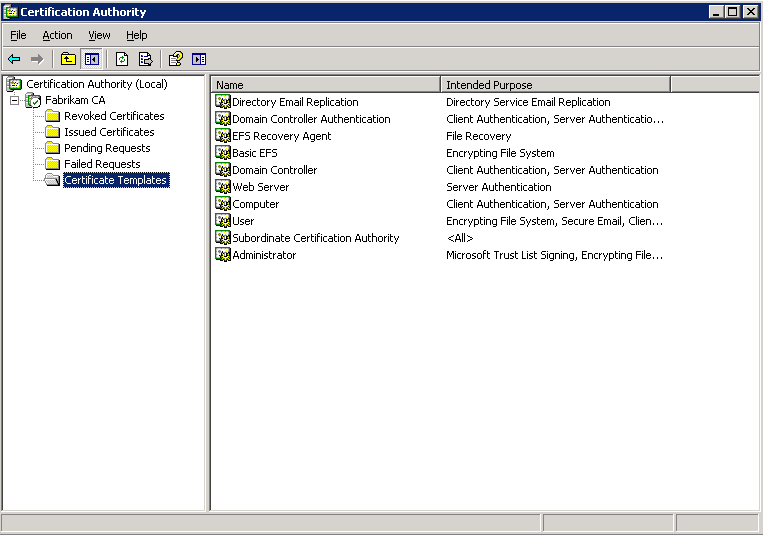




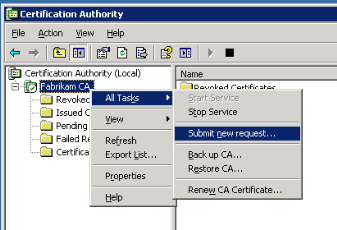
1. The CA administrator then provides the file back to the user using an appropriate distribution method. Note: e-mail is unsuitable for this action as the file will likely be blocked or stripped though if the file is contained within a compressed folder it may be possible to send via e-mail. It is important to note this file is not the certificate itself, and can only be imported on the same machine that made the request.

If the CA is installed on Windows Server 2008 or later, the administrator must use the Certificate Authority MMC snap-in rather than the web enrollment.

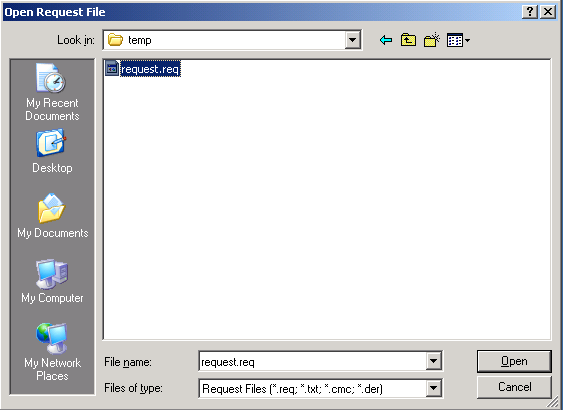
1. On the Windows Server Enterprise Edition that hosts the CA, open the **Certification Authority** management console.



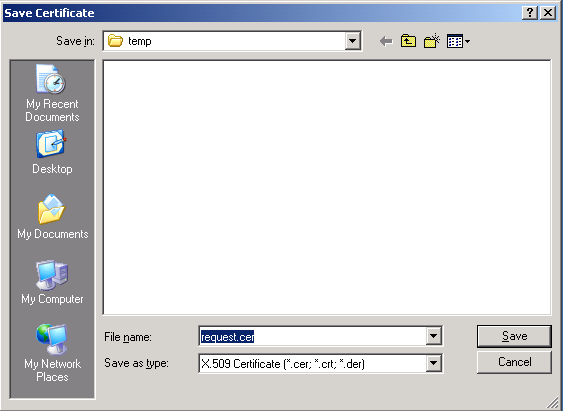
1. Right click the CA object itself and choose **All Tasks**, **Submit New Request** from the pop-up menu.



1. Browse to the location of the file sent by the user and select it.



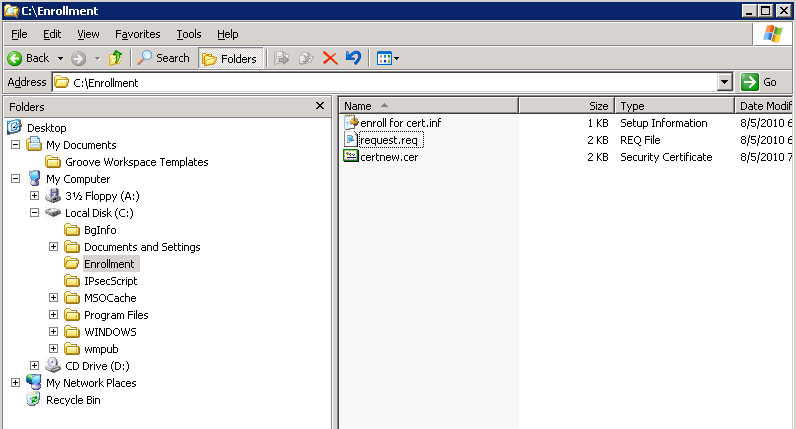
1. The console will then prompt for the location you wish you save the completed request file to.



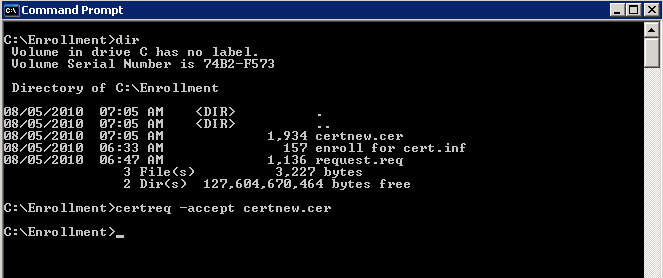
1. The CA administrator then provides the file back to the user using an appropriate distribution method. Note: e-mail is unsuitable for this action as the file will likely be blocked or stripped though if the file is contained within a compressed folder it may be possible to send via e-mail. It is important to note this file is not the certificate itself, and can only be imported on the same machine that made the request.

Once the client is in possession of the .cer file they must import it to their machine to complete the pending certificate request.

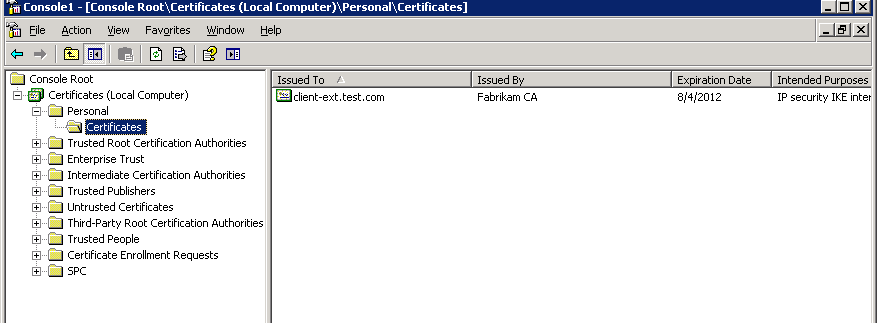
1. The user first places the file in a location they can access from a command prompt.



1. The user then runs the following command, certreq –accept <path to the cer file>, for example; **certreq –accept certnew.cer**



1. A successful enrollment will result in no errors. If the user wishes to check that the certificate is correctly installed they can open the certificates MMC, focusing on the **Certificates (Local computer, Personal, Certificates** node, and look for the certificate itself.



1. Double clicking the certificate will show the private key is in place, and checking the **Certification Path** tab will ensure the certificate can chain successfully to the root certificate. Any errors at this stage should be resolved before continuing.

|  |  |
| --- | --- |
|  |  |

### Configuring IPsec Policies and Connection Security Rules

IPsec policies (used by Windows XP and Windows Server 2003) and Connection Security Rules (used by Windows Vista, Windows 7, and Windows Server 2008 and Windows Server 2008 R2) define the security settings that trigger the use of IPsec, determine the authentication and encryption that will be used, and assign any other security settings that will be applied. A policy or rule must be created on both the client machine, and on the server, the machine with Forefront TMG or UAG installed.

The client policy applies to outbound connections, to the specific IP address and port of the Forefront TMG/UAG server publishing Exchange, and the server policy applies to the corresponding inbound connections.

Connection Security Rules are built in to the Windows Firewall with Advanced Security tool in Windows Vista, Server 2008 and later, so configuration and tight integration with Windows Firewall is implicit. Ordinarily when configuring Connection Security Rules on a client or server you must additionally configure Inbound or Outbound Rules within the Firewall itself, but this scenario walkthrough does not require this for two reasons;

* By default outbound connections are allowed – the client will be making an outbound connection to TCP 443 and this will therefore be allowed unless the administrator has chosen to control outbound connections.
* On the server side of the connection in this solution, Forefront TMG is installed onto Windows Server 2008 SP2 or Windows 2008 R2 (required for UAG). In either case, TMG registers with Windows firewall as an “all protocols” traffic handler. For this reason any primary traffic control policies (as opposed to connection security policies) should be created using the TMG or UAG management consoles; not in the Windows Firewall console. Manually creating Windows Firewall policies on a TMG server is not supported and will result in traffic misbehavior that is very difficult to troubleshoot.

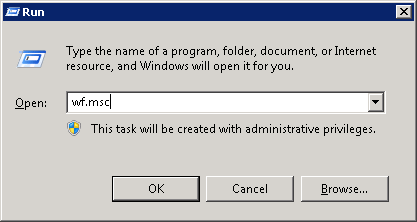
It is critical to make sure these policies have consistent settings, or negotiation of IPsec will very likely fail. Generally the client and server policies will be identical in terms of authentication and encryption, but mirror images of each other in terms of network configuration.

#### Configuring Connection Security Rules on a Windows Vista or Windows 7 Based Client Computer

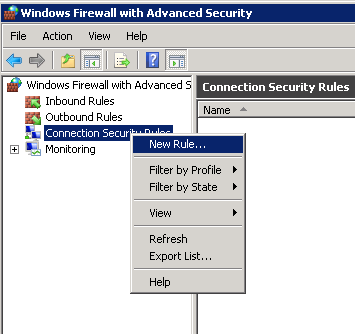
Configuring Connection Security Rules can be done either directly on each client machine, either using the user interface, a script, or a policy can be created within a Group Policy Object and be distributed to all applicable client machines. The policy conditions in either case are the same, the difference is only is how and where the objects are created.

This walkthrough will show how to create a rule using the Windows Firewall with Advanced Security user interface, and how to use a scripted command to achieve the same result.

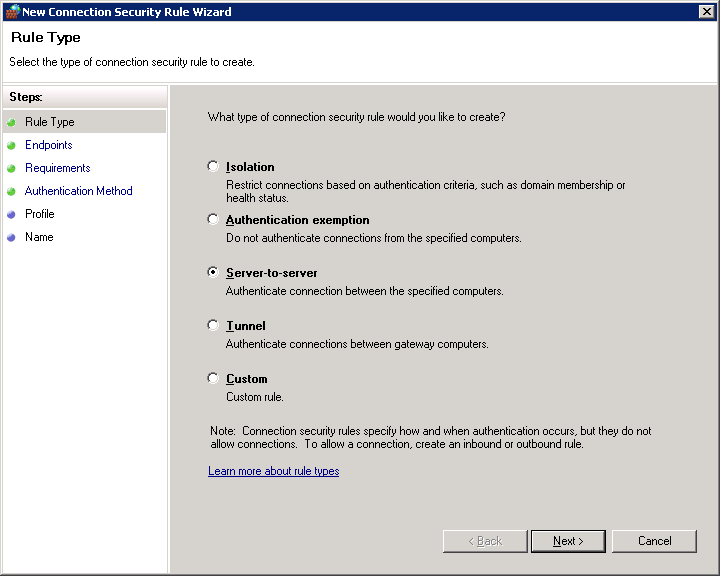
1. Click **Start, Run** and type **wf.msc** in the **Open** field, then click **OK**.



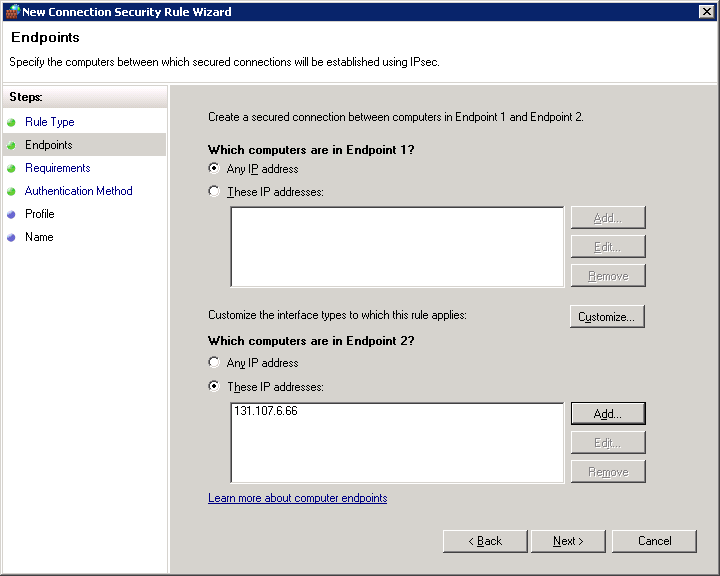
1. Right click the **Connection Security Rules** object in the task pane and choose **New Rule.**



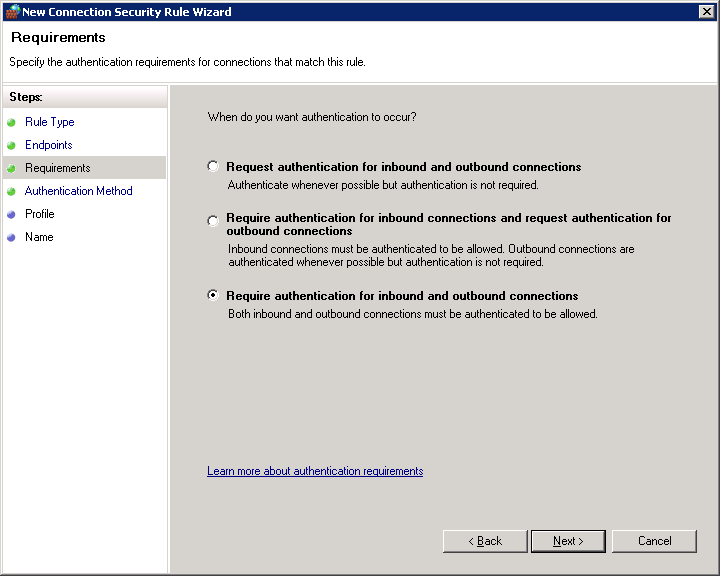
1. Click to select **Server-to-server** and then click **Next**.



1. On the **Endpoints** page of the wizard, In the **Endpoint 2** section of the page, click **These IP Addresses**, click the **Add** button and specify the external IP address used by the listener on TMG and receiving the inbound IPsec connections –131.107.6.66 in this example. Technically it does not matter whether you specify this as Endpoint 1 or 2, as long as you are consistent on both client and server policies. We have chosen endpoint 2 for this walkthrough to represent the TMG server and Endpoint 1 to represent the client.



1. Click **Next** and at the **Requirements** stage of the wizard select **Require authentication for inbound and outbound connections**. Then click **Next**.

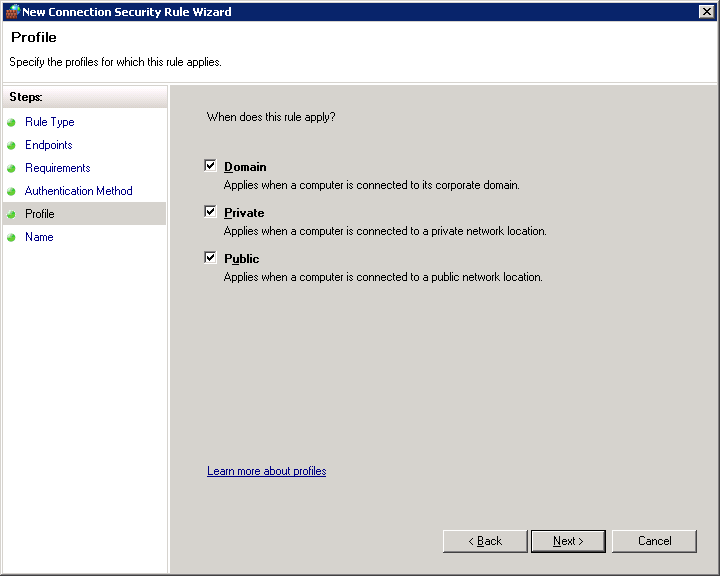


1. At the **Authentication Method** page, **Computer certificate** is enabled by default. Click the **Browse** button and then select the Certificate Authority from which the computer certificates will be issued.

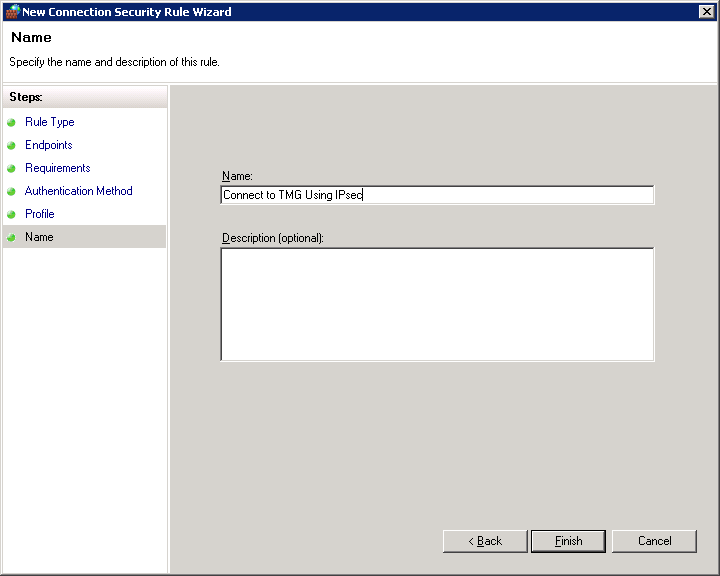
|  |  |
| --- | --- |
|  |  |

**Note:** The CA that issued this certificate must be trusted by the remote endpoint or certificate-based IPsec will fail between these two hosts.

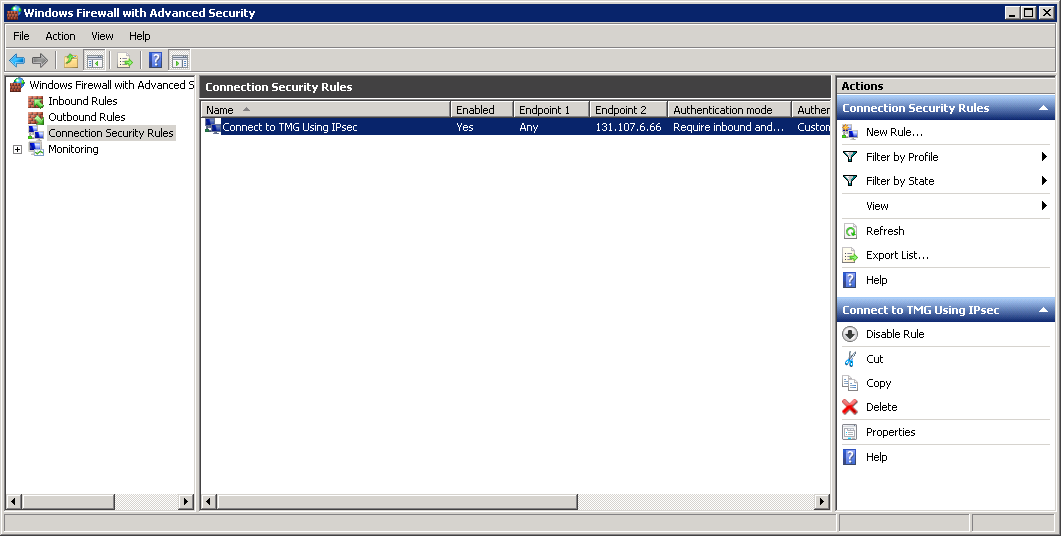
1. Click **Next** to display the Profile page, where you are able to select which network locations the rule will apply to. You may elect to leave all locations selected here, as the rule will apply to a specific IP address, and so will only be triggered in specific scenarios, or you may choose to use Windows Network Location Awareness features and have more control. For this walkthrough, and to ease initial configuration, we will leave all locations selected, meaning that the security rule will apply no matter what network the client detects it is using.



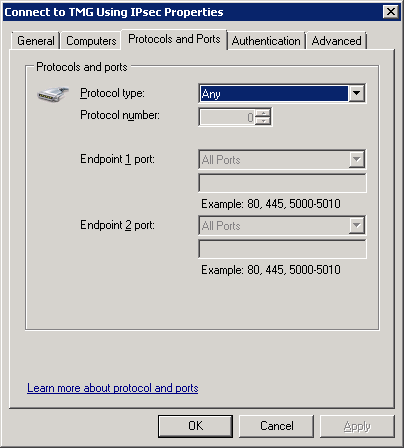
1. Click **Next** and at the **Name** page of the wizard, use a descriptive name before completing the wizard by clicking **Finish**.



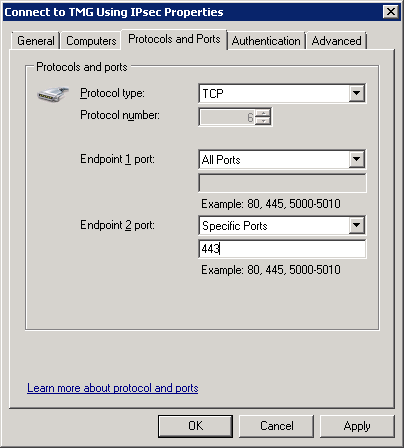
1. The wizard closes and the rule is shown in the results pane of the console. Note that the rule is already shown as **Enabled**.



1. Next we need to scope the connection to just the port being used to connect to Exchange, TCP 443 in this case. Right click the new rule you created and choose **Properties**, then select the **Protocols and Ports** tab.



1. Click the **Protocol type** drop down list to select **TCP**, then next to **Endpoint 2** (as we are using Endpoint 2 to represent TMG in these examples), choose **Specific Ports** from the list and enter **443** in the box just below.



1. The rule is set to only apply to connections made to the external IP address of TMG, and specifically only when the connection is to TCP port 443. Click **OK** and the rule will be active.

###### Scripting the Creation of Rules

It is also possible to use the Netsh utility to script the creation of the previous rule. Netsh can be used to create Connection Security Rules in this way on Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2.

The following example will create exactly the same rule as in the previous walkthrough.

**C:\> netsh advfirewall consec add rule name="Connect to TMG Using IPsec" endpoint1=any endpoint2=131.107.6.66 protocol=tcp port2=443 action=RequireInRequireOut Auth1=ComputerCert Auth1CA="DC=COM, DC=FABRIKAM, CN=Fabrikam CA"**

Using a script to deploy your initial settings is recommended, though using the management console to examine the results is also advised, and is useful in helping understand the various parameters available.

During testing, you might create your rules, or modify rules through the console, and then decide to script the actual deployment. If you wish to easily view the parameters of the rules you create, to help you in scripting their deployment, you can use the following simple command to view both the rules and their settings.

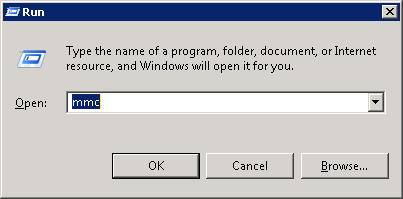
**C:\> netsh advfirewall consec show rule name=all**

#### Configuring IPsec Policies on a Windows XP or Windows Server 2003 Based Client Computer

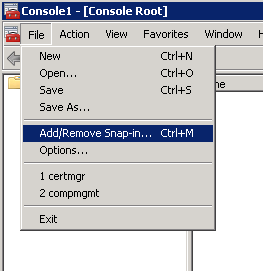
Configuring IPsec policies can be done either directly on each client machine, or the policy can be created within a Group Policy Object and be distributed to all applicable client machines. The policy conditions in either case are the same, the difference is only is how and where the objects are created.

In this section we will configure the policy object on the machine itself, which is ideal if you are simply testing this configuration, as it only applies to the machine it is configured on. Once you have the policy settings for your environment configured and validated, you can then configure the same policy settings as part of a GPO and distribute them automatically to all client machines.

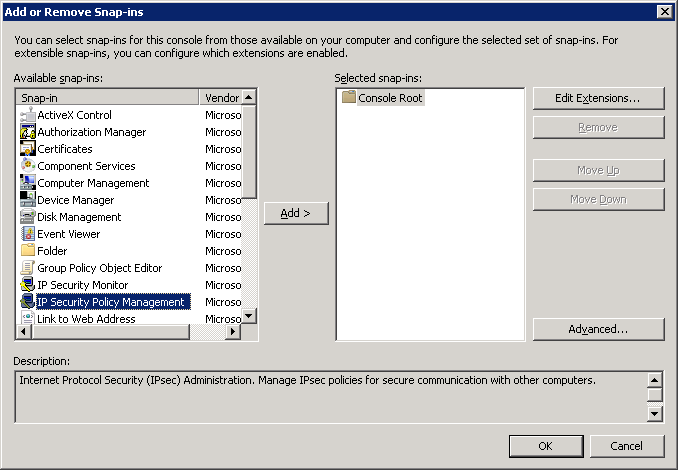
1. Click **Start, Run** and type **mmc** in the **Open** field, then click **OK**.



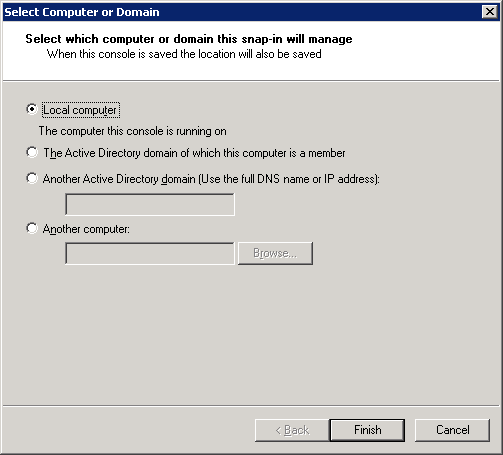
1. Click **File, Add/Remove Snap-in**



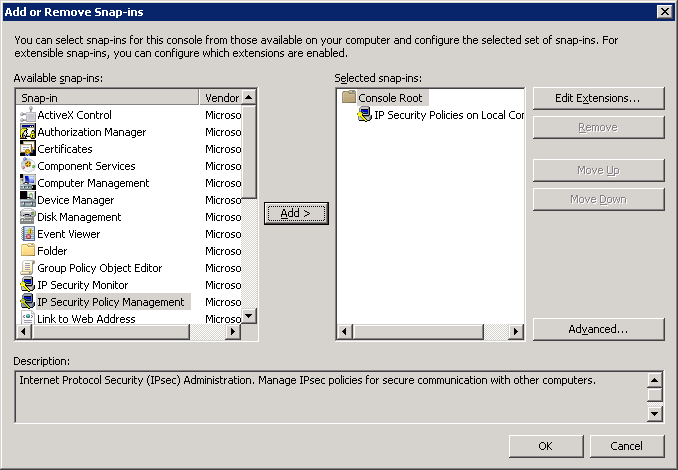
1. From the **Available Snap-ins** list choose **IP Security Policy Management**, click **Add** to start the process of adding the snap-in to the **Selected snap-ins** column.



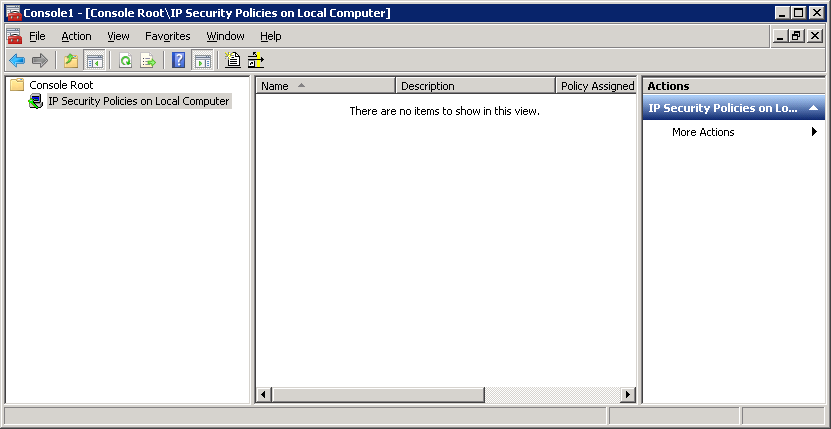
1. Leave the default selection of **Local Computer** selected and click **Finish.**



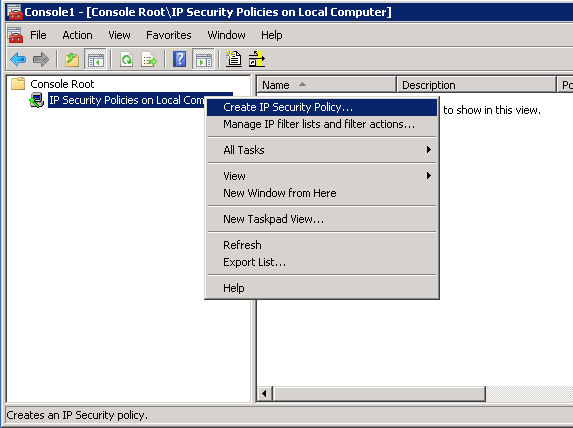
1. Click **OK** once the snap-in is selected and the scope is defined.



1. The IP Security Policies console will display the selected snap-in.



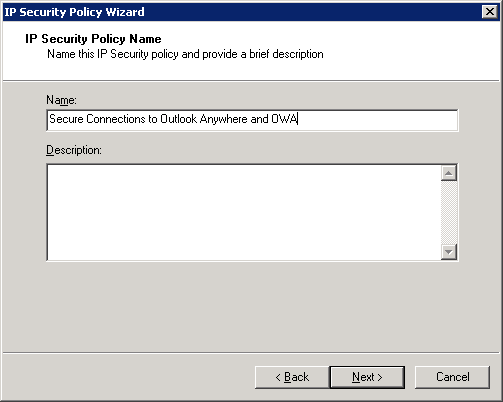
1. Right click the **IP Security Policies on Local Computer** Node and from the pop up menu choose **Create IP Security Policy**



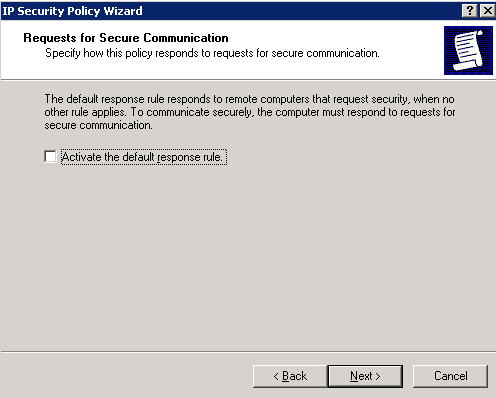
1. At the Welcome screen click **Next**



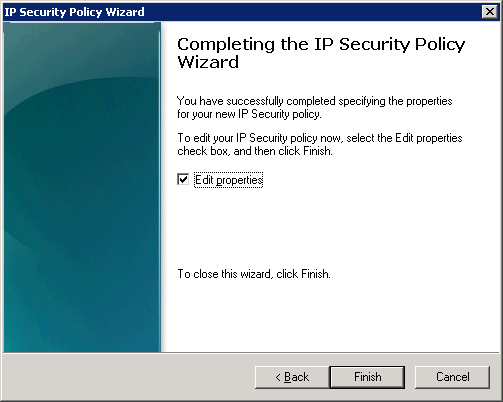
1. Give the policy a descriptive name then click **Next**



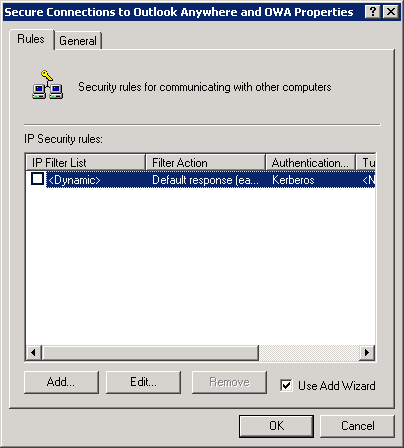
1. At the **Requests for Secure Communication** page of the wizard, there is no need for the **Activate the default response rule** to be checked in this scenario so just click **Next**.



1. At the Completing the **IP Security Policy Wizard** screen leave the Edit properties checkbox selected and click **Finish**



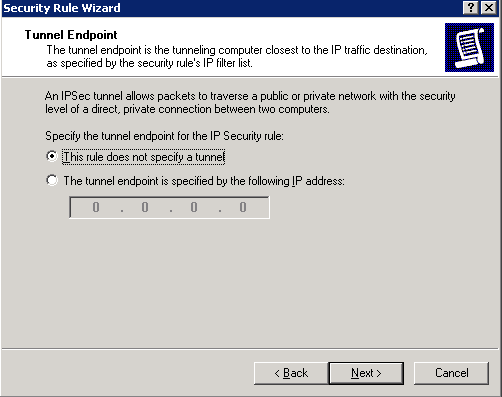
1. The properties page for the policy opens.



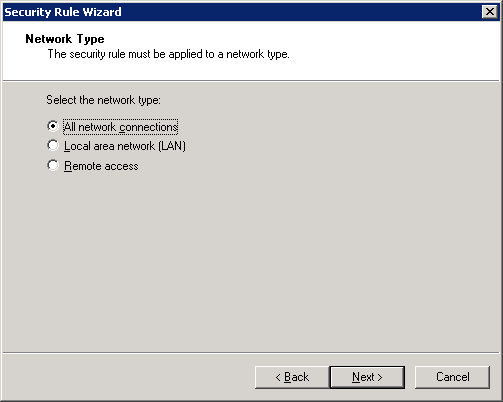
1. Click the **Add** button to start the **Welcome to the Create IP Security Rule Wizard**



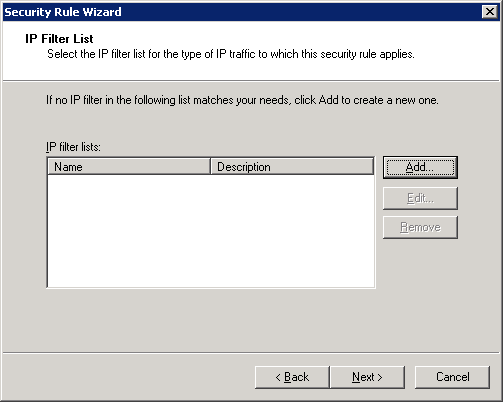
1. At the **Tunnel Endpoint** page of the wizard leave the default option of **This rule does not specify a tunnel** and then click **Next**.



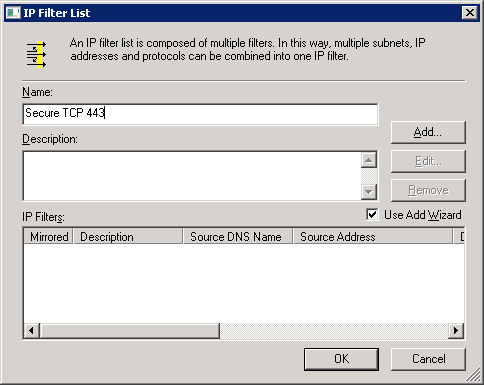
1. At the **Network Type** page of the wizard leave the default of **All network connections** and click **Next**.



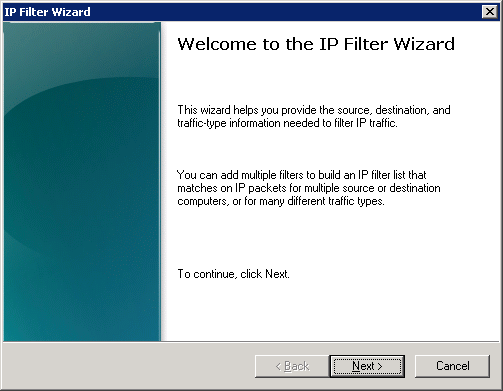
1. At the **IP Filter List** page click **Add** to create a new IP filter list.



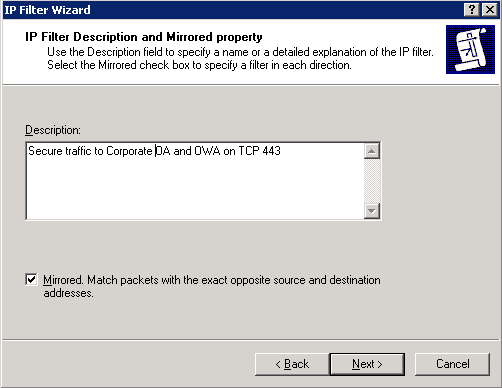
1. Give the new IP Filter List a meaningful and descriptive name.



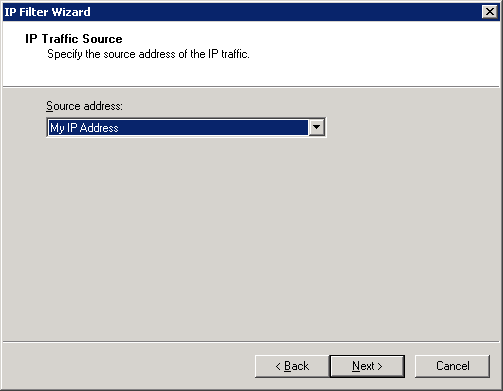
1. Click **Add** to launch the **IP Filter Wizard**.



1. Click **Next** and then provide a meaningful description, then click **Next**.

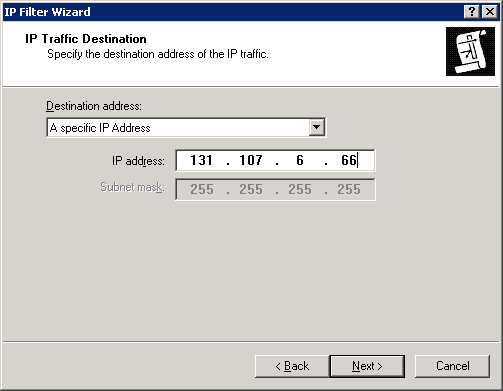


1. On the **IP Traffic Source** page, use the drop down box to choose **My IP Address**, then click **Next**.

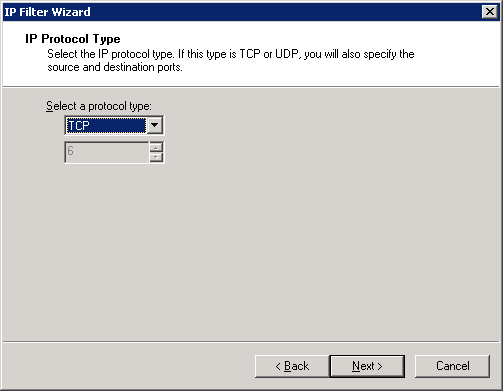


**Note**: IPSec “source” selections refer to the host that initiates the connection. These policies automatically allow response traffic on a given connection, so there is no need to create a reciprocal IPsec policy for response traffic.

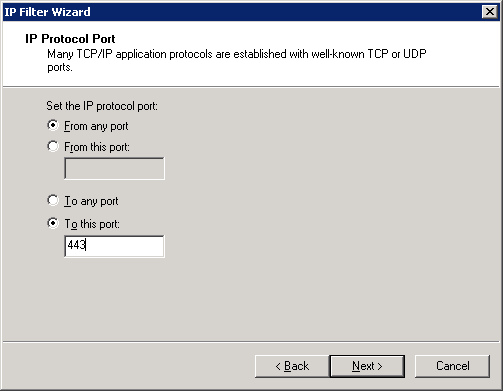
1. On the **IP Traffic Destination** page of the wizard, choose **A specific IP Address or Subnet** from the dropdown list and enter the IP address used by the external interface of Forefront TMG or Forefront UAG. If you have multiple IP addresses associated with TMG or UAG, you can simply run the IP Filter List wizard as many times as needed, adding each IP address individually.



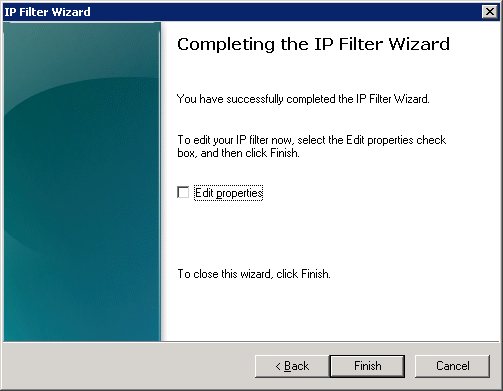
1. Click **Next** and choose **TCP** as the protocol type on the **IP Protocol Type** page of the wizard. Then click **Next**.



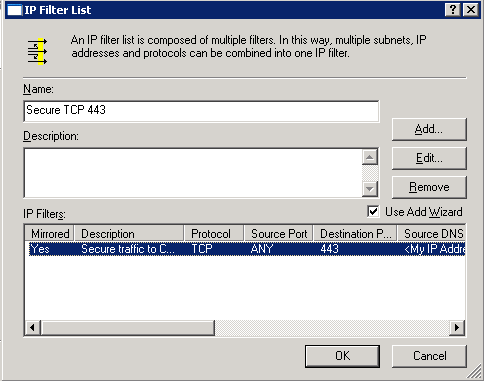
1. Click the radio button next to **To this port** and enter 443. All connections to Exchange are being made to TCP 443, the port commonly used by the HTTPS protocol.



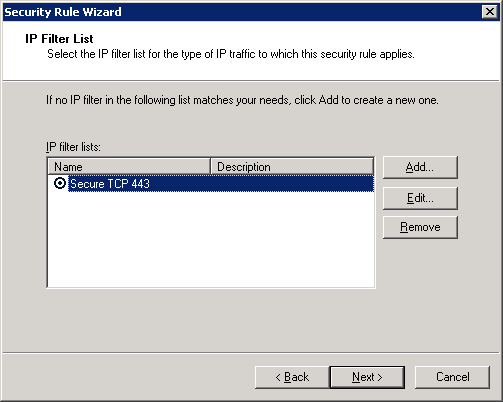
1. Click **Next**, then click **Finish**.



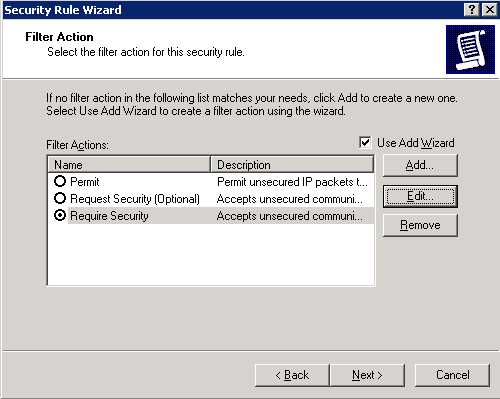
1. Click **OK** to close the IP Filter List wizard.



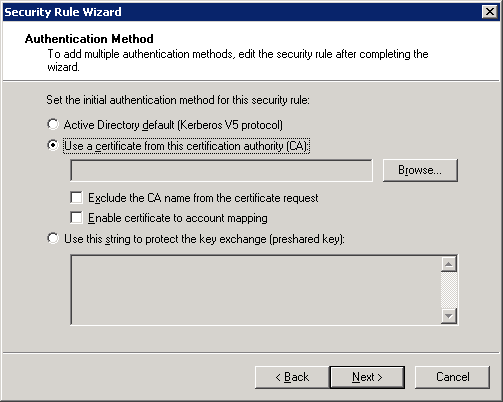
1. Check the radio button next to the IP filter list you just created, then click **Next**.



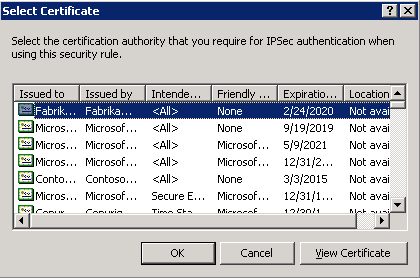
1. The default Filter Action will vary based on operating system. For newer versions of Windows, the **Nego** Filter Action uses data integrity, not encryption as its defaults, and uses the SHA1 algorithm for integrity. On earlier versions of Windows the **Require Security** Filter Action provides the same settings. If these settings are acceptable, click the radio button next to the filter action name and click **Next**. If you wish to add encryption to the configuration (remember that Exchange traffic is SSL encrypted already) or change the algorithm used, you can just edit the existing Filter Action or create a new one. It is important that any changes made here are reflected in the server policy.



1. At the Authentication Method page of the wizard, check the radio button next to **Use a certificate from this certification authority (CA)**. You can alternatively choose the preshared key option at the bottom of the dialog to use a text passphrase, remembering that this is less secure and not practical for mass deployment.

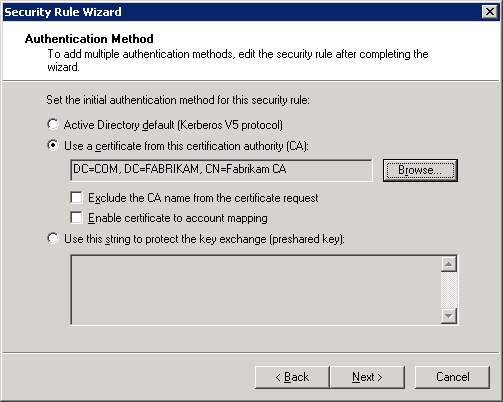


1. Click the **Browse** button to bring up a list of all installed CA’s. Select your root CA from this list and click **OK**.



**Note:** the CA certificate you select must be trusted by the TMG/UAG server or certificate-based IPsec negotiations will fail.

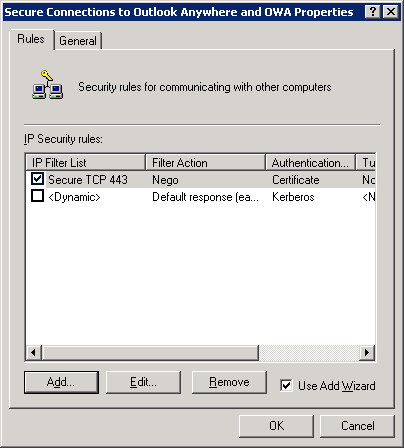
1. The CA is added to the Authentication Method page of the wizard. You can additionally choose to further secure the certificate authentication method by selecting the **Exclude the CA name from the certificate request** checkbox, which prevents the client from exposing the CA name during negotiation. When your selections are made, click **Next**.



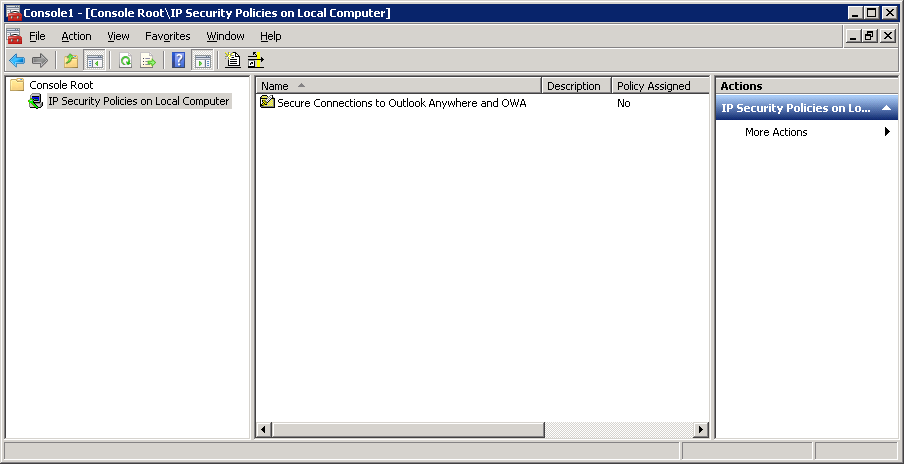
1. Click **Finish** to complete the wizard.



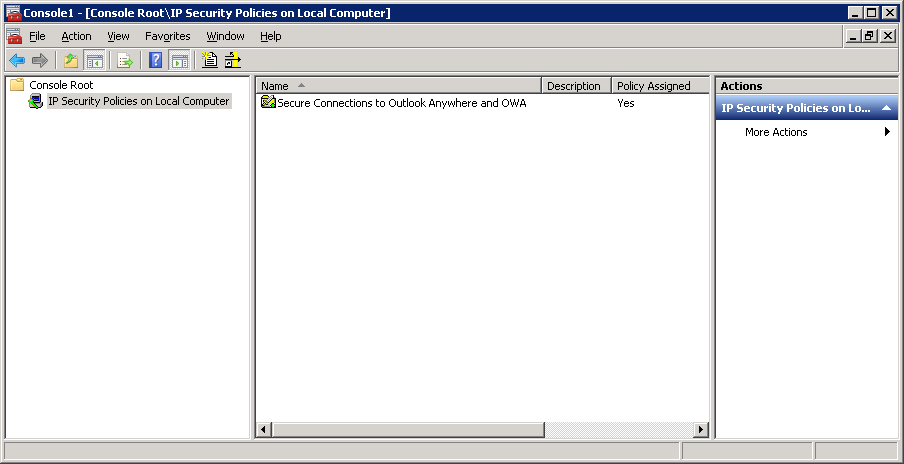
1. Click **OK** to complete the creation of the policy.



1. The IP Security Policies MMC shows the policy as created, but not assigned.



1. To assign the policy to the client simply right click the policy object and choose **Assign**.



1. All outbound connections now made from the client, to the specified IP address, when using TCP 443 will negotiate IPsec integrity only, using a certificate from the chosen CA. Close the IP Security Policies console.

#### Configuring Policies or Connection Security Rules on the Server

In this section we will configure the policy object or connection security rules on the server itself, which is ideal if you’re simply testing this configuration, as they only apply to the machine they are configured on. Once you have the policy settings for your environment configured and validated, you can then configure the same policy settings as part of a GPO and distribute them automatically to all machines or distribute them via script.

As discussed previously, if the AutoDiscover service is being published and used by clients that cannot support IPsec, such as mobile clients, then it must use a different IP address on Forefront TMG or Forefront UAG than that used for Outlook Anywhere or OWA, when requiring IPsec for those clients. This is to ensure that non IPsec aware clients can make a connection to the AutoDiscover service. If you have no requirement for remote access by mobile devices, and only want to provide AutoDiscover to Outlook Anywhere clients, then the AutoDiscover service can use the same IP address externally as Outlook Anywhere or OWA. That way an IPsec SA must be established before the client can use the AutoDiscover service.

Also note that if you are using UAG to publish Exchange you must use the TMG management tools to create the rules detailed in this section. The support boundaries specifying what features you can use in TMG when using UAG are detailed in <http://technet.microsoft.com/en-us/library/ee522953.aspx> and configuring IPsec inbound is listed as one of the supported scenarios. Creating the Exchange publishing rules when using UAG is done in the UAG management console in the usual way, only the changes necessary to allow IPsec are performed in the TMG console.

As with the client settings, the method you use will vary based upon the operating system version of the server. Forefront TMG requires a minimum of Windows Server 2008 SP2, and Forefront UAG requires Windows Server 2008 R2. Both of these require rule creation using the Windows Firewall with Advanced Security console or by using NETSH.

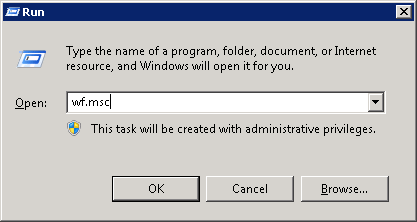
If you have chosen to configure this scenario using ISA server which can only be installed on Windows Server 2003, you must use IPsec polices. The steps necessary for Windows Server 2003 are provided in the Appendix of this document.

##### Configuring Connection Security Rules on a Windows Server 2008 or later Computer

Configuring Connection Security Rules can be done either directly on each client machine, either using the user interface, a script, or a policy can be created within a Group Policy Object and be distributed to all applicable machines. The policy conditions in either case are the same, the difference is only is how and where the objects are created.

This walkthrough will show how to create a rule using the Windows Firewall with Advanced Security user interface, and how to use a scripted command to achieve the same result.

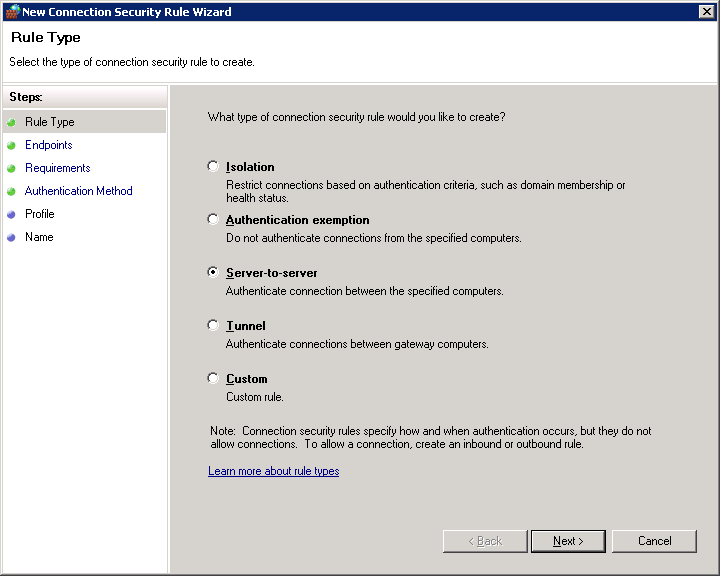
1. Click **Start, Run** and type **wf.msc** in the **Open** field, then click **OK**.



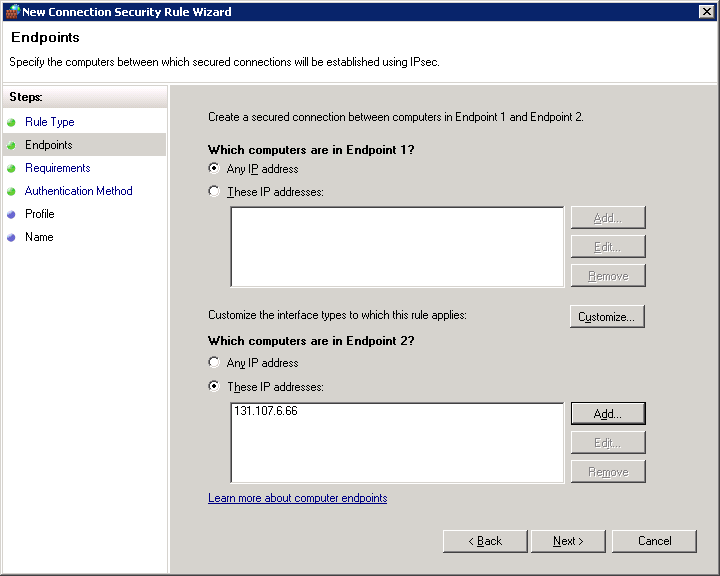
1. Right click the **Connection Security Rules** object in the task pane and choose **New Rule**



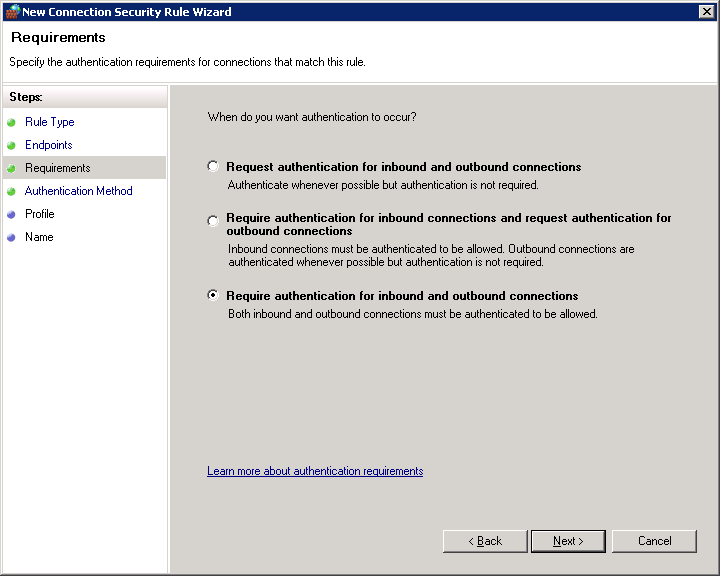
1. Click to select **Server-to-server** and then click **Next**.



1. On the **Endpoints** page of the wizard, In the **Endpoint 2** section of the page, click **These IP Addresses**, click the **Add** button and specify the external IP address used by the listener on TMG and receiving the inbound IPsec connections – 131.107.6.66 in this example. Technically it does not matter whether you specify this as Endpoint 1 or 2, as long as you are consistent on both client and server policies. We have chosen endpoint 2 for this walkthrough to represent the TMG server and Endpoint 1 to represent the client.



1. Click Next and at the **Requirements** stage of the wizard select **Require authentication for inbound and outbound connections**. The click **Next**.

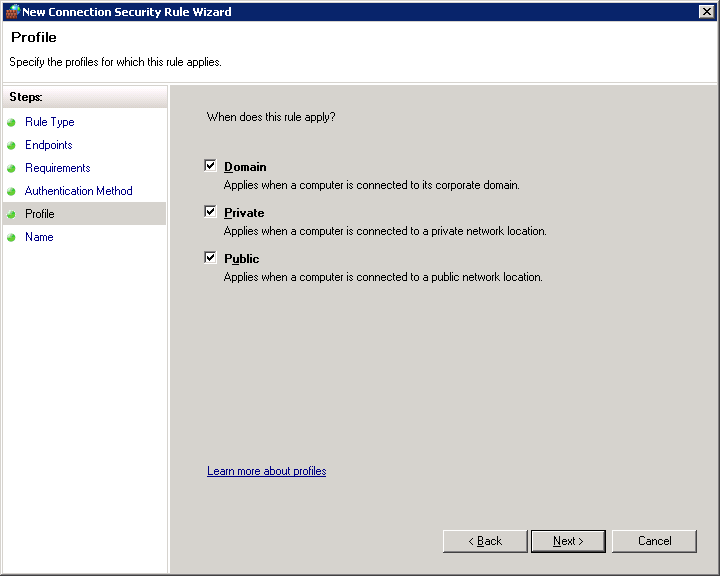


1. At the **Authentication Method** page, **Computer certificate** is enabled by default. Click the **Browse** button and then select the Certificate Authority from which the computer certificates will be issued.

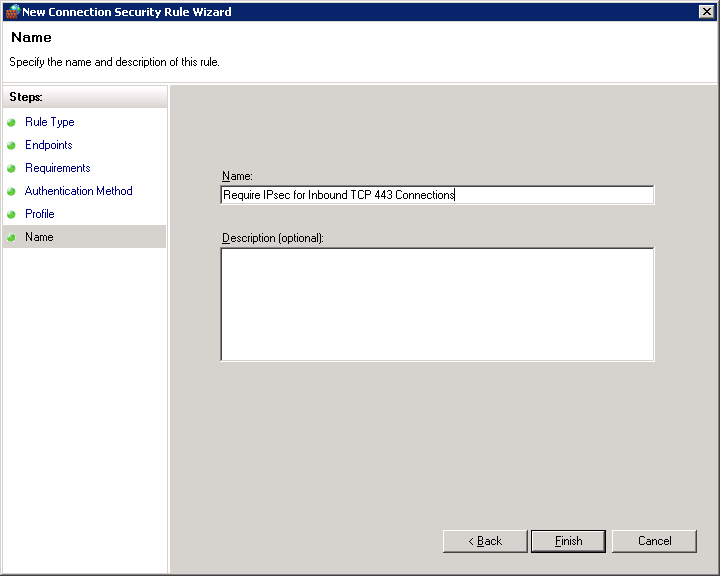
|  |  |
| --- | --- |
|  |  |

**Note:** the issuing CA certificate must be trusted by the remote client or IPsec negotiation will fail.

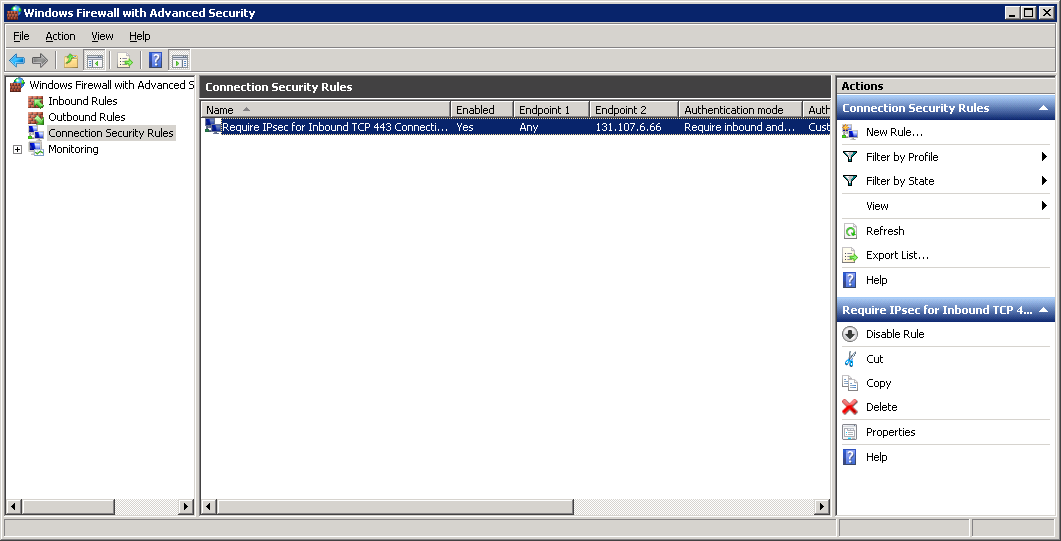
1. Click **Next** and at the profile page you are able to select which network locations the rule will apply to. You may elect to leave all locations selected here, as the rule will apply to a specific IP address, and so will only be triggered in specific scenarios, or you may choose to use Windows Network Location Awareness features and have more control. For this walkthrough, and to ease initial configuration, we’ll leave all locations selected, meaning that the policy will apply no matter what network the client detects it is using.



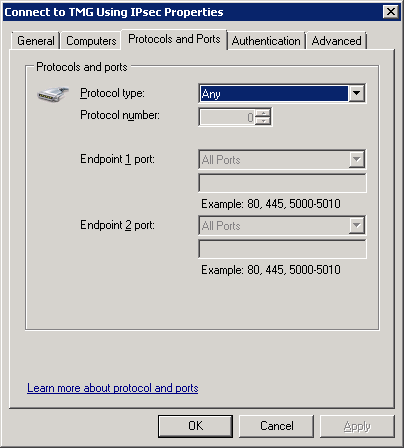
1. Click **Next** and at the **Name** page of the wizard, use a descriptive name before ending the wizard by clicking **Finish**.



1. The wizard closes and the rule is shown in the results pane of the console. Note that the rule is already shown as Enabled.

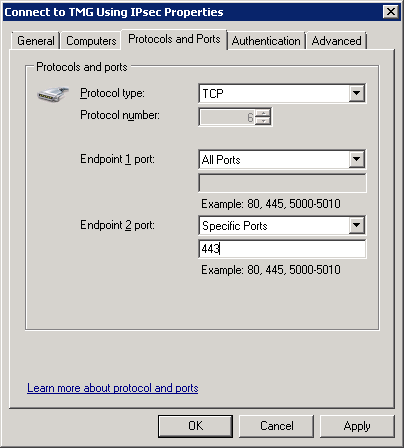


1. Next we need to scope the connection to just the port being used to connect to Exchange, TCP 443 in this case. Right click the new Rule you created and choose **Properties**, then select the **Protocols and Ports** tab.



**Note:** You could opt to leave this at “Any” if you want to limit all traffic from trusted hosts to the specified local IP address.

1. Click the **Protocol type** drop down list and select **TCP**, then next to **Endpoint 2** (as we are using Endpoint 2 to represent TMG in this example), choose **Specific Ports** from the list and enter **443** in the box just below.



1. Now that the Rule is set to only apply to connections made to the external IP address of TMG, and specifically only when the connection is to TCP 443, click **OK** and the rule will be active.

###### Scripting the Creation of Rules

It is also possible to use the Netsh utility to script the creation of the previous rule. Netsh can be used to create Connection Security Rules in this way on Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2.

The following example will create exactly the same rule as in the previous walkthrough.

**C:\> netsh advfirewall consec add rule name="Require IPsec for Inbound TCP 443 Connections" endpoint1=any endpoint2=131.107.6.66 protocol=tcp port2=443 action=RequireInRequireOut Auth1=ComputerCert Auth1CA="DC=COM, DC=FABRIKAM, CN=Fabrikam CA"**

Using a script to deploy your initial settings is recommended, though using the interface to examine the output is also advised, and is useful in helping understand the various parameters available.

During testing you might create your rules, or modify rules through the console, and then decide to script the actual deployment. If you wish to easily view the parameters of the rules you create, to help you in scripting their deployment, you can use the following simple command to view both the rules and their settings.

**C:\> netsh advfirewall consec show rule name=all**

### Configure Forefront TMG/UAG To Allow IPsec Traffic

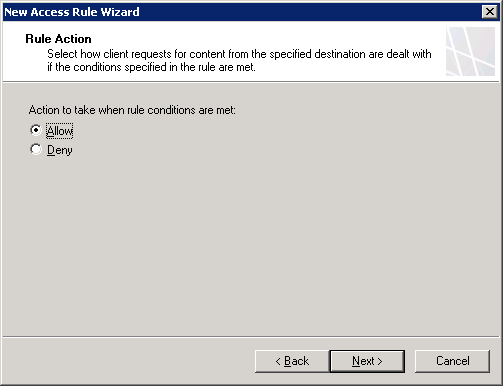
There are two steps to complete on Forefront TMG or UAG to allow incoming IPsec sessions.

#### Creating an Access Rule

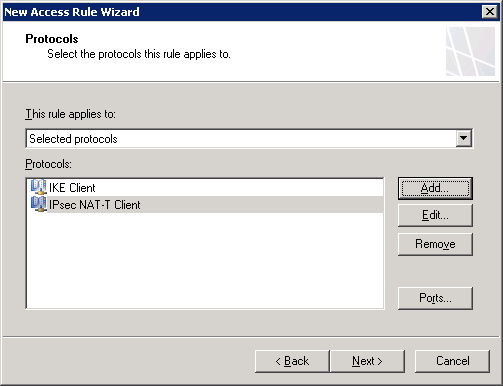
1. Open the Forefront TMG management console and navigate to the **Firewall Policy Node**.
2. Right click the **Firewall Policy** node object and choose **New > Access Rule**. Give the rule a meaningful name, then click **Next**.



1. On the **Rule Action** page of the wizard click the radio button next to **Allow**, then click **Next**.



1. On the **Protocols** page of the wizard click Add and choose **IKE Client** and **IPsec NAT-T Client** from the VPN and IPsec section of the dropdown list. Then click **Next**.

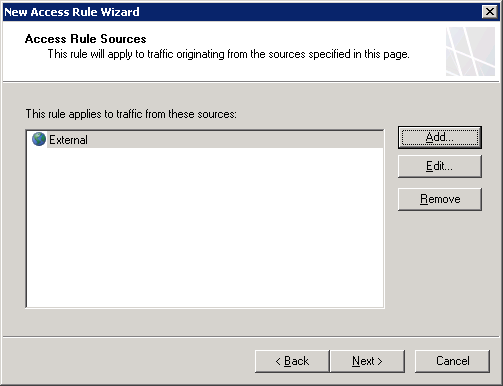


**Note**: If you have chosen to use encryption as well as integrity for IPsec you may additionally have to add IPsec ESP and IPsec AH to the Access Rule. Remember that Outlook Anywhere and OWA traffic is already encrypted in SSL, and that IPsec ESP is incompatible with NAT so by enforcing encryption in IPsec you are encrypting already encrypted pieces of traffic and potentially causing issues for clients utilizing NAT.

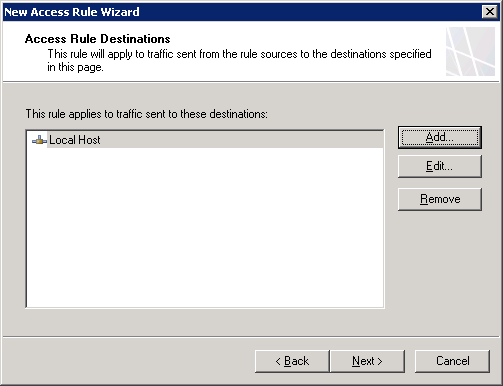
IPsec AH must be defined as a custom protocol using the following parameters:

* Name: IPsec AH
* Protocol Type: IP-level
* Protocol Number: 51
* Direction: Send-Receive

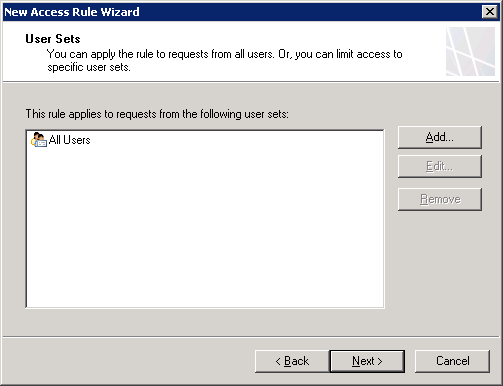
1. On the Access Rule Sources page of the wizard select the network that represents the network clients will be using, External in this example as client connections are inbound from the Internet. Then click **Next**.



1. Click the Add button to select an object that refers to the external IP address of the Forefront TMG server, the IP used by the OWA and OA listener. **Localhost** includes all IP address on TMG. Click **Next**.



1. Leave the default selection of All Users in the User Sets page of the wizard, then click **Next**.



1. Click **Finish** to complete the wizard, then click the **Apply** button in the console to activate the new configuration.



#### Disabling TCP Checksum for IPsec Packets

The final step in configuring Forefront TMG/UAG is to run a script on the server to allow TMG to ignore the mismatch between the TCP checksum of incoming packets and the calculated checksum, which happens as a result of the NAT-T IPsec process from dropping TCP packets. More information about this process and the script itself is provided in <http://support.microsoft.com/kb/911554>.

**NOTE**: This step should only be used if you notice the problem discussed in the knowledgebase article. There is no need to complete the following steps if you do not experience the issue described.

The original script used in the KB article is as follows;

|  |
| --- |
| ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''  '  ' Copyright (c) Microsoft Corporation. All rights reserved.  ' THIS CODE IS MADE AVAILABLE AS IS, WITHOUT WARRANTY OF ANY KIND. THE ENTIRE  ' RISK OF THE USE OR THE RESULTS FROM THE USE OF THIS CODE REMAINS WITH THE  ' USER. USE AND REDISTRIBUTION OF THIS CODE, WITH OR WITHOUT MODIFICATION, IS  ' HEREBY PERMITTED.  ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''  ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''  ' This script adds a new VendorParametersSets under the array root.  ' Used to added new parameters that are required for hotfixes or service packs.  ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''  Sub AddIPsecXsumBypass()  ' Create the root object.  Dim root ' The FPCLib.FPC root object  Set root = CreateObject("FPC.Root")  'Declare the other objects needed.  Dim array ' An FPCArray object  Dim VendorSets ' An FPCVendorParametersSets collection  Dim VendorSet ' An FPCVendorParametersSet object  ' Get references to the array object  ' and the network rules collection.  Set array = root.GetContainingArray  Set VendorSets = array.VendorParametersSets  On Error Resume Next  Set VendorSet = VendorSets.Item( "{143F5698-103B-12D4-FF34-1F34767DEabc}" )  If Err.Number <> 0 Then  Err.Clear  ' Add the item  Set VendorSet = VendorSets.Add( "{143F5698-103B-12D4-FF34-1F34767DEabc}" )  CheckError  WScript.Echo "New VendorSet added... " & VendorSet.Name  Else  WScript.Echo "Existing VendorSet found... value- " & VendorSet.Value("IpAddrToBypassIPsecXsum")  End If  WScript.Echo "Initial IpAddrToBypassIPsecXsum- " & VendorSet.Value("IpAddrToBypassIPsecXsum")  Err.Clear  '  ' The format for setting an exception is: sourceip:sourceport>destinationip:destinationport  ' Any field (entire ip or port) which is 0 is ignored.  ' For example- 12.0.0.0:0>14.15.16.17:80;  ' means that traffic from 12.0.0.0, any source port, to 14.15.16.17  ' port 80 is not subject to validation of tcp checksum. The ';' character  ' must end each address pair, even if there is only one pair.  ''  '  ' THIS FOLLOWING LINE IS THE ONE THAT YOU NEED TO CHANGE  '  VendorSet.Value("IpAddrToBypassIPsecXsum") = "12.34.55.66:45587>54.127.232.0:80;"  '  ' Use the following value to reset the exception list.  '  ' VendorSet.Value("IpAddrToBypassIPsecXsum") = ""  If Err.Number <> 0 Then  CheckError  Else  VendorSets.Save false, true  CheckError  If Err.Number = 0 Then  WScript.Echo "Done with IpAddrToBypassIPsecXsum, saved!"  End If  End If  WScript.Echo "Final IpAddrToBypassIPsecXsum- " & VendorSet.Value("IpAddrToBypassIPsecXsum")  End Sub  Sub CheckError()  If Err.Number <> 0 Then  WScript.Echo "An error occurred: 0x" & Hex(Err.Number) & " " & Err.Description  Err.Clear  End If  End Sub  AddIPsecXsumBypass  'End of Script |

You must amend the line in the script that starts with “VendorSet.Value("IpAddrToBypassIPsecXsum")” to include the exception list. Use the following format:

SourceIp:SourcePort>DestinationIp:DestinationPort

We will assume that traffic from anywhere external to the corporate network will be accepted, inbound to TCP443, so we will change the line to read as follows:

"0.0.0.0:0><*the IP address of your TMG/UAG server*>:443”

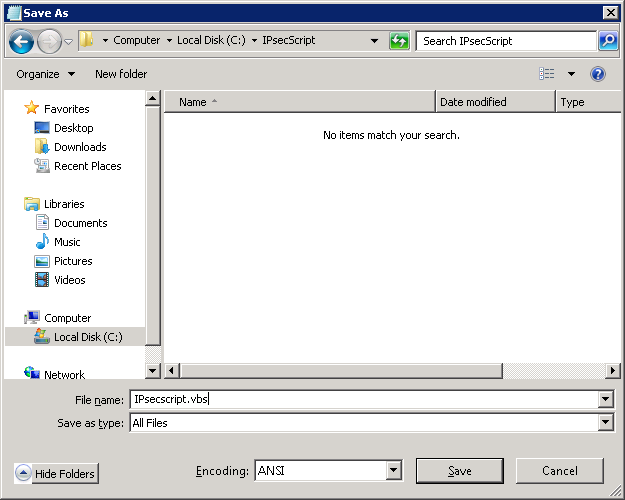
**Note**: Multiple entries are supported if you wish to narrow the scope allowed inbound. Each entry must end by using a colon (;). For example, the following address and port notation is supported:

"12.0.0.0:0>14.15.16.17:443;12.0.0.0:1>14.15.16.17:443;"

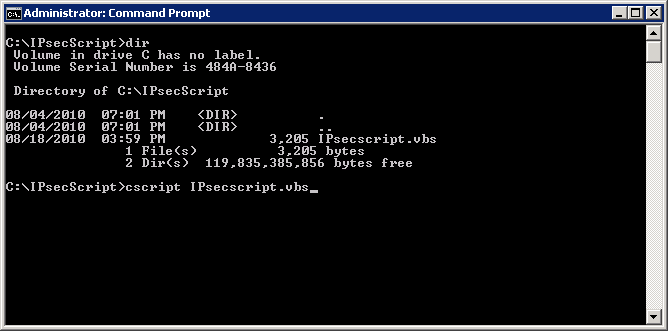
If you wish to allow traffic from any destination to bypass the TCP checksum, the following script can be used, simply changing the 131.107.6.66 (the external IP of the TMG server used in this lab walkthrough) value shown in red in the sample script below to the external IP address value of your TMG/UAG server.

|  |
| --- |
| ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''  '  ' Copyright (c) Microsoft Corporation. All rights reserved.  ' THIS CODE IS MADE AVAILABLE AS IS, WITHOUT WARRANTY OF ANY KIND. THE ENTIRE  ' RISK OF THE USE OR THE RESULTS FROM THE USE OF THIS CODE REMAINS WITH THE  ' USER. USE AND REDISTRIBUTION OF THIS CODE, WITH OR WITHOUT MODIFICATION, IS  ' HEREBY PERMITTED.  ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''  ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''  ' This script adds a new VendorParametersSets under the array root.  ' Used to added new parameters that are required for hotfixes or service packs.  ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''  Sub AddIPsecXsumBypass()  ' Create the root object.  Dim root ' The FPCLib.FPC root object  Set root = CreateObject("FPC.Root")  'Declare the other objects needed.  Dim array ' An FPCArray object  Dim VendorSets ' An FPCVendorParametersSets collection  Dim VendorSet ' An FPCVendorParametersSet object  ' Get references to the array object  ' and the network rules collection.  Set array = root.GetContainingArray  Set VendorSets = array.VendorParametersSets  On Error Resume Next  Set VendorSet = VendorSets.Item( "{143F5698-103B-12D4-FF34-1F34767DEabc}" )  If Err.Number <> 0 Then  Err.Clear  ' Add the item  Set VendorSet = VendorSets.Add( "{143F5698-103B-12D4-FF34-1F34767DEabc}" )  CheckError  WScript.Echo "New VendorSet added... " & VendorSet.Name  Else  WScript.Echo "Existing VendorSet found... value- " & VendorSet.Value("IpAddrToBypassIPsecXsum")  End If  WScript.Echo "Initial IpAddrToBypassIPsecXsum- " & VendorSet.Value("IpAddrToBypassIPsecXsum")  Err.Clear  '  ' The format for setting an exception is: sourceip:sourceport>destinationip:destinationport  ' Any field (entire ip or port) which is 0 is ignored.  ' For example- 12.0.0.0:0>14.15.16.17:80;  ' means that traffic from 12.0.0.0, any source port, to 14.15.16.17  ' port 80 is not subject to validation of tcp checksum. The ';' character  ' must end each address pair, even if there is only one pair.  ''  '  **' THIS FOLLOWING LINE IS THE ONE THAT YOU NEED TO CHANGE**  '  **VendorSet.Value("IpAddrToBypassIPsecXsum") = "0.0.0.0:0>131.107.6.66:443;"**  '  ' Use the following value to reset the exception list.  '  ' VendorSet.Value("IpAddrToBypassIPsecXsum") = ""  If Err.Number <> 0 Then  CheckError  Else  VendorSets.Save false, true  CheckError  If Err.Number = 0 Then  WScript.Echo "Done with IpAddrToBypassIPsecXsum, saved!"  End If  End If  WScript.Echo "Final IpAddrToBypassIPsecXsum- " & VendorSet.Value("IpAddrToBypassIPsecXsum")  End Sub  Sub CheckError()  If Err.Number <> 0 Then  WScript.Echo "An error occurred: 0x" & Hex(Err.Number) & " " & Err.Description  Err.Clear  End If  End Sub  AddIPsecXsumBypass  'End of Script |

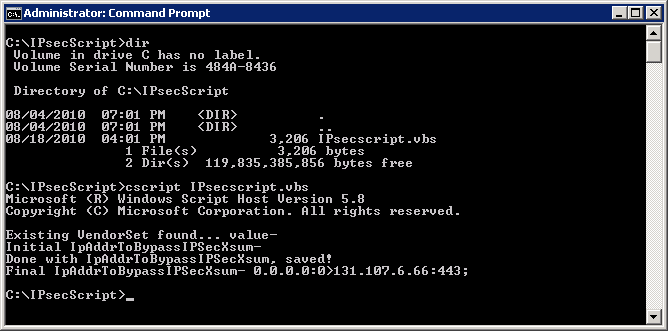
1. Copy the amended text into Notepad and save the file to the TMG/UAG server with a .vbs file extension.



1. Open a command prompt, navigate to the folder in which you saved the VBS script and run the script by entering the name of the file preceded by ‘cscript’, e.g. **cscript IPsecscript.vbs**.



1. You will receive output similar to that shown here.



1. Restart the firewall service on the TMG/UAG server.

### Test Your Configuration

Configuring IPsec as described in this guide involves making many configuration settings and mistakes are inevitable even if you are familiar with the process. You are strongly encouraged to follow this guide precisely the first time you use it, and once you have it working successfully, go back and make any customizations you require.

Testing this configuration is as simple as attempting to use OWA or Outlook Anywhere against the Forefront TMG or UAG server, and it working as expected. You can monitor the IPsec SA’s as described in the troubleshooting section of this document, and confirm IPsec SA’s have been successfully negotiated.

If a client does not have the required certificate, and Forefront TMG or UAG are configured to require IPsec, then the user does not even see the Forms Based Authentication page (in the case of OWA), or is simply unable to connect, in the case of Outlook Anywhere.

#### Troubleshooting IPsec

Troubleshooting IPsec can be challenging because by its very nature the traffic is protected from close inspection. There are several key tools you should consider using when troubleshooting;

* **Event Log** – the security log built into Windows provides information explaining why an SA failed to be established, and often provides clues as to how to solve the problem.
* **IPsec Security Monitor** – the IPsec Security Monitor mmc snap-in shows the policy assigned to the client, and the details of the established SA’s.
* **Using IPsec logging** - You can have IPsec log the IKE exchanges to a log file on the hard drive for troubleshooting or monitoring needs.

Regardless of the type of problem you are experiencing, you should first make sure that the necessary services are started and set to automatic on both IPsec peers. On computers running Windows Server 2003, the IPsec Services service must be started. Sometimes, especially after making significant changes, you might be able to resolve a problem by restarting IPsec services. This completely clears the IKE negotiation state. You can restart IPsec services from a command prompt by running the following commands:

* **net stop policyagent**
* **net start policyagent**

This is simply a quick way to restart IPsec without restarting the computer. After restarting the IPsec services on both computers, attempt to establish a secure connection. If the problem persists, restart the operating systems on both IPsec peers and try again.

Next, verify that the correct policy has been assigned to each of the IPsec peers by using the IP Security Monitor snap-in, which is discussed later in this section. Remember, creating a new policy does not automatically assign it to a computer. Additionally, if you deploy a policy by using a GPO, the settings do not propagate instantly. If the policy is different from the one you were expecting, identify the responsible GPO by using the Resultant Set Of Policy snap-in or the command **Netsh IPsec Static Show Gpoassignedpolicy** on Windows Server 2003, or **Netsh avdfirewall consec show rule name=all** if you are troubleshooting Windows Vista, Windows 7, Windows Server 2008 or Windows Server 2008 R2.

Verify that IKE negotiation is succeeding by enabling auditing and checking the Security event log. If IKE negotiation is not succeeding, verify that authentication, encryption, and key change settings are the same on both IPsec peers. If there is no indication that negotiations are succeeding, use Network Monitor to verify that packets are reaching the correct computer.

If using Windows 7 or Windows Server 2008 or later you should also look for events in the Applications and Services Logs/Microsoft/Windows/Windows Firewall with Advanced Security section. You may see events here that are helpful.

If IKE negotiation is succeeding but IPsec communications are still failing, verify that Quick Mode is succeeding by checking the Security event log and the IKE tracing log. If Quick Mode is not succeeding, check to see that all Quick Mode encryption, integrity, key strength, and key change settings are the same on both IPsec peers. If IPsec negotiations simply do not occur, or if the type of negotiations are different from what you expected, double-check the IPsec filters. If you are specifying source and destination IP addresses in the filter, verify that the filters on each of the IPsec peers are mirrors of each other.

Certificates can also be a common cause for failure. If you are experiencing problems with IPsec and want to verify that the problem is related to authentication, temporarily change the IPsec authentication method on both IPsec peers to Preshared Key. If IPsec communications succeed with Preshared Key but fail with certificates, the problem is almost certainly related to certificates.

If you have multiple rules in a policy, double-check that those rules will use the same authentication method consistently for any single remote computer.

Another potential cause of authentication problems is incorrectly obtained certificates. Incorrectly obtained certificates can result in a condition in which the certificate exists and is chosen to be used for IKE authentication, but fails to work because the private key corresponding to the certificate’s public key is not present on the local computer.

Depending upon how the certificate was requested and populated into the host’s local certificate store, this private key value might not exist, or it might not be available to be used during the IKE negotiation. If the certificate in the personal folder does not have a corresponding private key, certificate enrollment has failed.

If a certificate was obtained from Certificate Services with the option set for Strong Private Key Protection, the user must enter a PIN number to access the private key each time that the private key is used to sign data in the IKE negotiation. Because the IKE negotiation is being done in the background by a system service, there is no window available to the service to prompt the user. So certificates obtained with this option will not work for IKE authentication.

##### Network Address Translation Problems

Early implementations of IPsec were not compatible with NAT. NAT’s purpose is to modify the source or destination IP address in a packet without the client or server being aware, and part of IPsec’s purpose is to discard packets that have been modified in transit. IPsec NAT Traversal (NAT-T) allows IPsec traffic to pass through compatible NAT servers. However, both the IPsec hosts and the NAT server must support NAT-T, and the NAT server must be configured to allow traffic on UDP port 4500. Windows Server 2003, Windows XP Professional, and all newer Windows operating systems support NAT-T.

Windows 2003 and Windows 2008 fully support the use of NAT-T. If you are having problems establishing an IPsec connection across a NAT server, first verify that both IPsec clients and the NAT servers support NAT-T. You cannot use IPsec AH across a NAT server, because AH is not compatible with NAT-T.

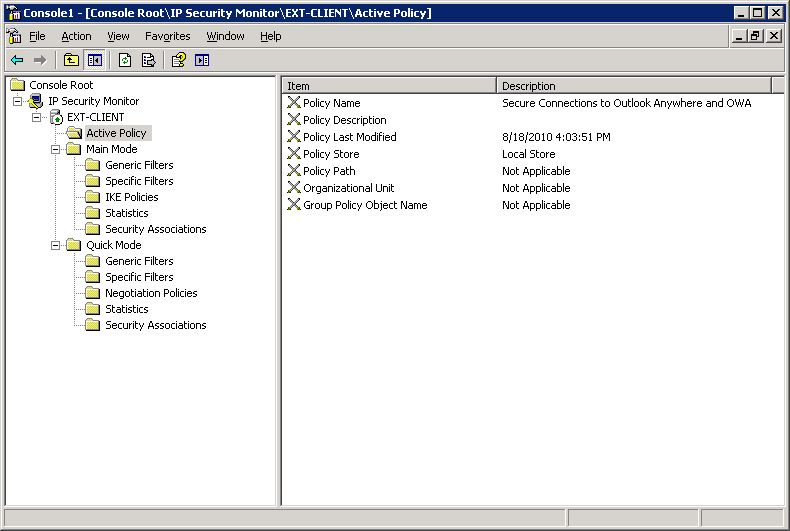
Windows Server 2003 and 2008 support IPsec NAT-T as described by version 2 of the IPsec NAT-T Internet drafts, but some applications might not work when their traffic is first protected with IPsec and then passed through a network address translator. Test how your planned implementation of IPsec interacts with network address translators in a lab before deploying IPsec in your environment.

If possible, verify that IPsec works properly between two computers on the same side of the NAT server. If problems persist, the problem might not be related to NAT-T and verify that the NAT server is not filtering packets required by IPsec.

##### IPsec Security Monitor

IP Security Monitor is a Windows snap-in used to monitor and troubleshoot IPsec. If an IPsec policy is active, you can use this console to examine the policy and its operations. Information in the IP Security Monitor snap-in is divided into three nodes: Active Policy, Main Mode, and Quick Mode. The Active Policy node, as shown below, displays information about the currently assigned policy. This information includes the policy’s name, last modified date, and origin. If you are unsure about how a particular policy was applied to a computer, check this node to identify the GPO that assigned the policy.

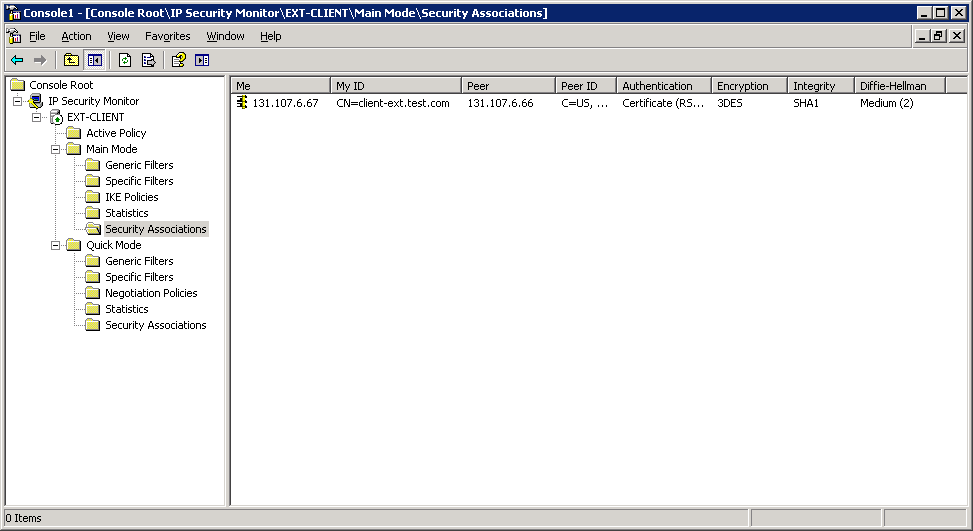
The same features are also available at the command line in newer Windows systems by using the **Netsh advfirewall consec** command set and within the Windows Firewall with Advanced Security management console.



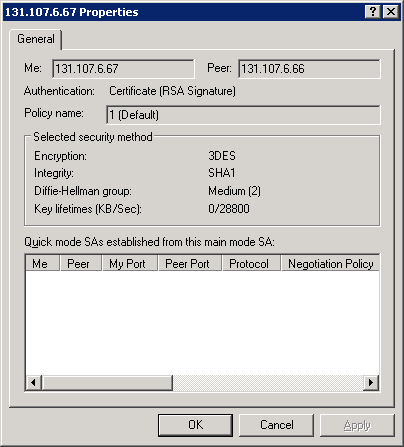
###### Main Mode

Main Mode negotiation is the first phase of establishing an IPsec connection. Main Mode establishes common security protocols shared by the two hosts, determines master key keying material that will be used for encrypting communications, and authenticates the computers themselves.

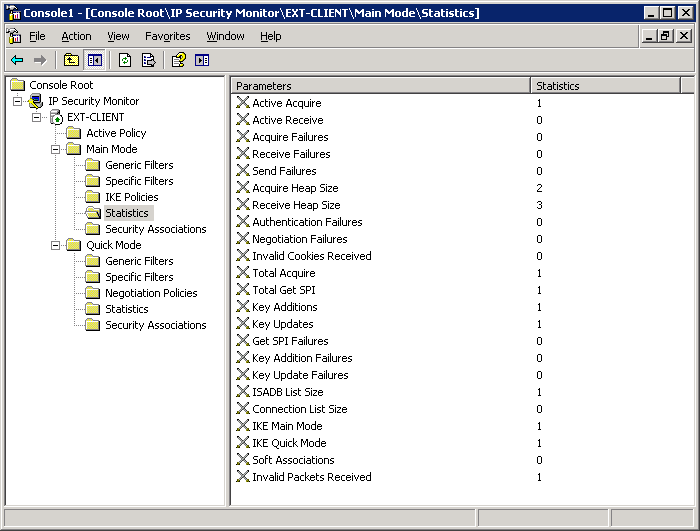
One of the most useful features of the IP Security Monitor snap-in is its ability to quickly view active SAs. To do this, expand Main Mode, and then click Security Associations. The right pane displays a list of active SAs, including the IP address of the IPsec peer.



Double-click any SA to view the properties of the SA, as shown below. The SA properties dialog box shows you the IP addresses of the two peers, the protocols used for encryption and integrity, the key lifetimes, and a list of Quick Mode SAs that were established from that Main Mode SA. The listing of Quick Mode SAs, in turn, reveals the negotiation policy used to establish each Quick Mode SA.

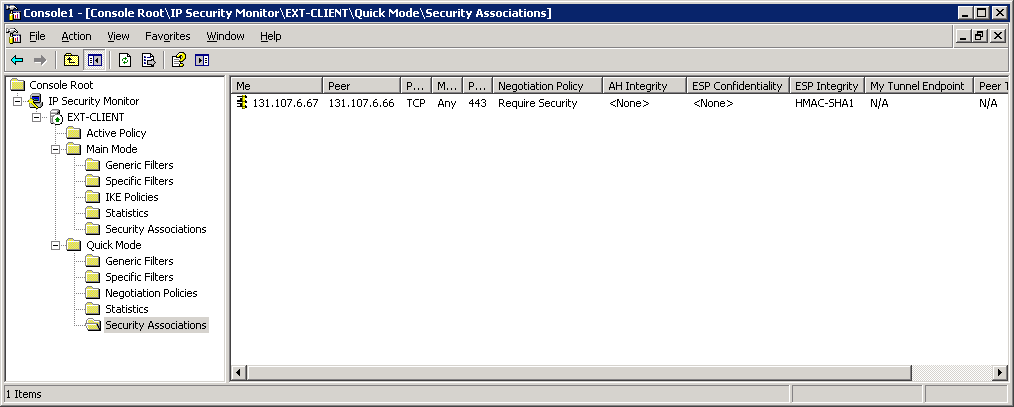


The most important node within the Main Mode node of the IP Security Monitor is the Statistics node. The Statistics node will be your primary tool for monitoring IPsec, because it contains statistics about Phase 1 of the IPsec negotiations, including the number of active IKE negotiations and the total number of successful and unsuccessful negotiations and authentications.

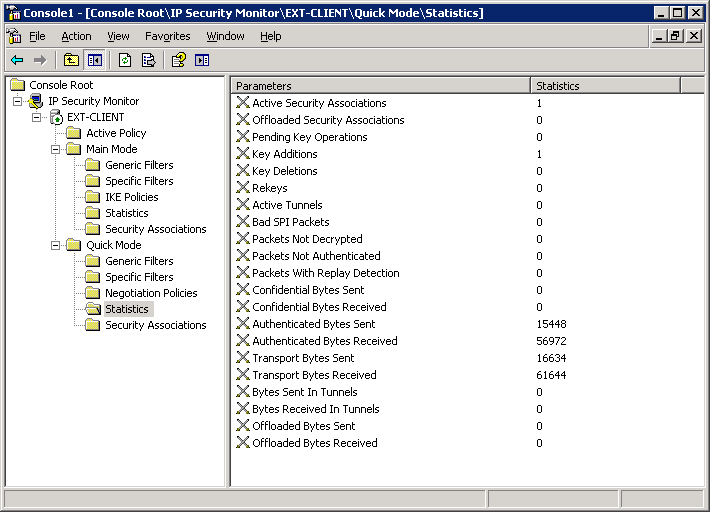


###### Quick Mode

Quick Mode, also known as Phase 2 of IPsec negotiations, occurs after Main Mode and regularly while an IPsec connection is in use. The IP Security Monitor tool has a Quick Mode node that you can use to view current information about Quick Mode negotiations. The information contained in the Quick Mode node is similar to that of Main Mode, including the listing of active Quick Mode SAs.



The most useful information can be viewed from within the Quick Mode Statistics node. Quick Mode statistics provide more granular information than is available in Main Mode, including the total number of encrypted and authenticated bytes.



##### Using IPsec logging

To have your computer log IKE exchanges, you must create a registry value named EnableLogging in the registry key HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent\Oakley. To enable logging, set the value to 1 and restart the IPsec services. The log file will be written to the file %systemroot% \debug\oakley.log. Note that if you use preshared keys for authentication, the key will appear in the log file in plaintext.

The IKE tracing log appears as the %systemroot%\Debug\Oakley.log file. A new Oakley.log file is created each time the IPsec service is started, and the previous version of the Oakley.log file is saved with the file name Oakley.log.sav. The log is limited to 50,000 lines. When the Oakley.log file becomes full, the current file is saved as Oakley.log.bak, and a new Oakley.log file is created. Because many IKE negotiations can occur simultaneously, you should minimize the number of negotiations and enable the IKE tracing log for as briefly as possible to capture a more easily interpreted log. Use the IP addresses, SPI, timestamps, and SA identifiers to identify messages related to one security negotiation or IPsec SA processing session.

You can also enable tracing on newer Windows system through the **Netsh** command line utility and on Windows 7 you might need to enable IPsec Audit logging using the following two commands;

auditpol.exe /set /SubCategory:"IPsec Main Mode" /success:enable /failure:enable

auditpol.exe /set /SubCategory:"IPsec Extended Mode" /success:enable /failure:enable

## Appendix

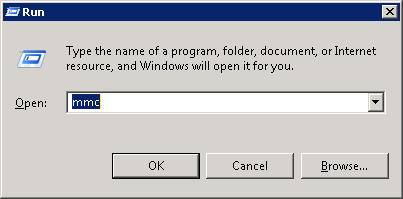
### Configuring IPsec Policies on a Windows Server 2003 Computer

**Note**: These steps only apply if you have chosen to use ISA 2006 to publish Exchange, not Forefront TMG or UAG.

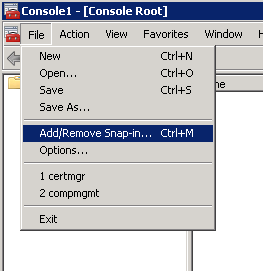
Configuring IPsec policies can be done either directly on each server, or the policy can be created within a Group Policy Object and be distributed to all applicable machines. The policy conditions in either case are the same, the difference is only is how and where the objects are created.

In this section we will configure the policy object on the server itself, which is ideal if you are simply testing this configuration, as it only applies to the machine it is configured on. Once you have the policy settings for your environment configured and validated, you can then configure the same policy settings as part of a GPO or script and distribute them automatically to all client machines.

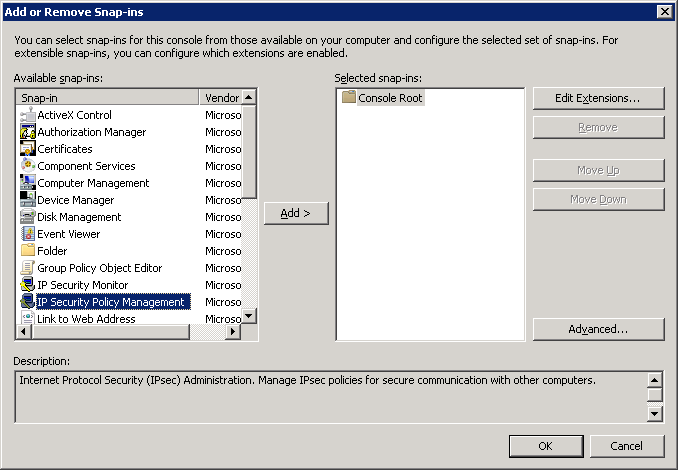
1. Click **Start, Run** and type **mmc** in the **Open** field, then click **OK**.



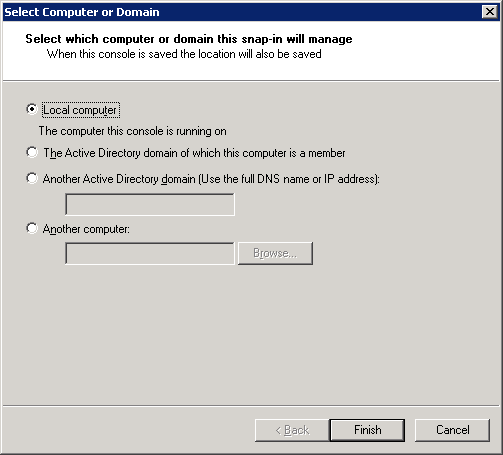
1. Click **File, Add/Remove** Snap-in



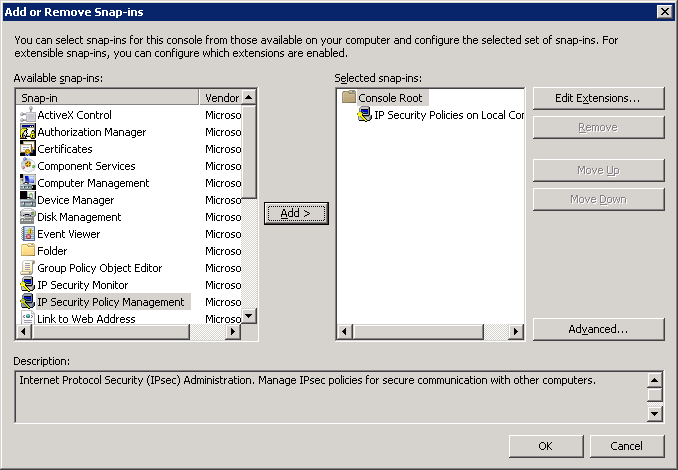
1. From the Available Snap-ins list choose IP Security Policy Management, click **Add** to move the snap-in to the Selected snap-ins column.



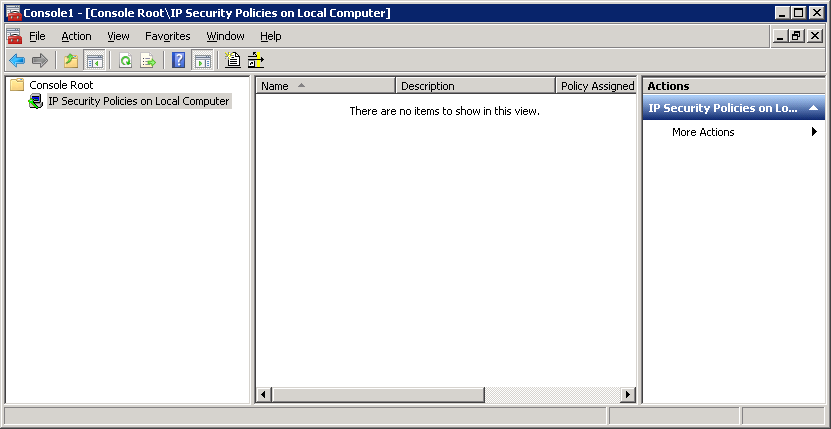
1. Leave the default selection of **Local Computer** selected and click **Finish**



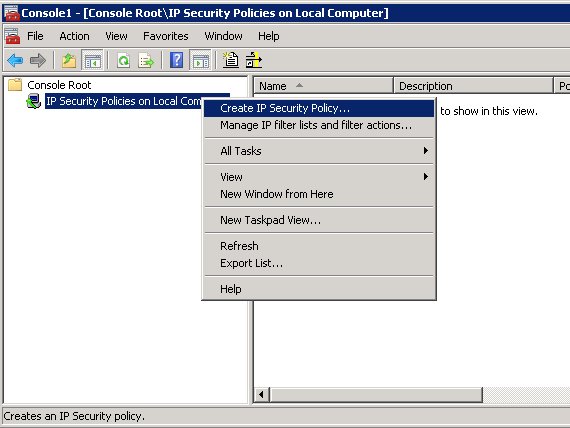
1. Click **OK** once the snap-in is selected and the scope is defined.



1. The IP Security Policies console will open.



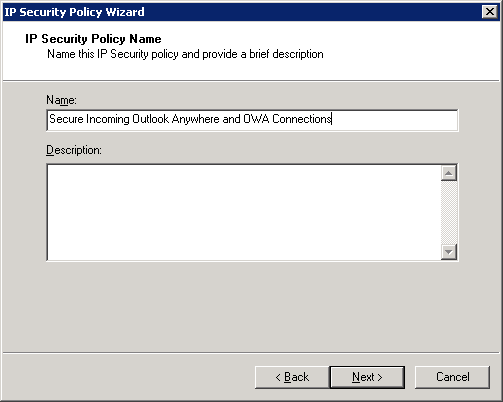
1. Right click the **IP Security Policies on Local Computer Node** and from the pop up menu choose **Create IP Security Policy**



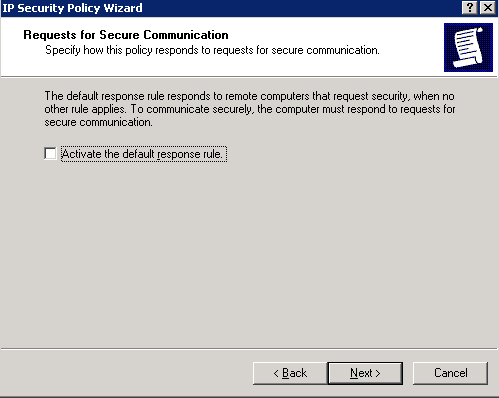
1. At the Welcome screen click **Next**



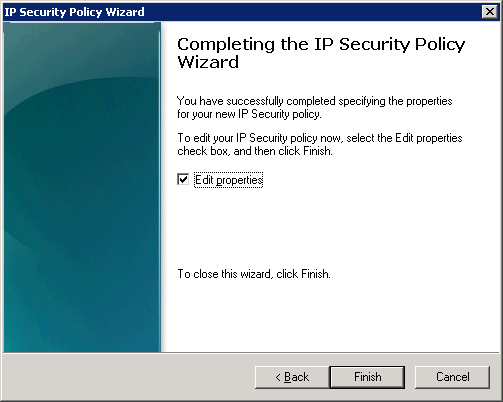
1. Give the policy a descriptive name then click **Next**



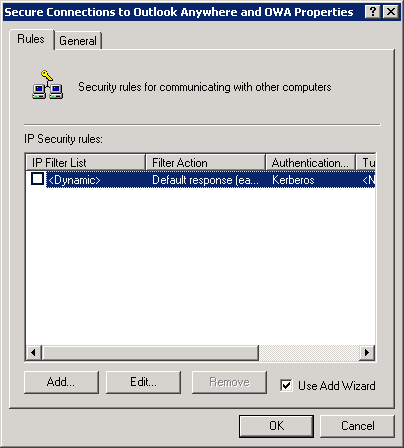
1. At the **Requests for Secure Communication** page of the wizard, uncheck the **Activate the default response rule** for this scenario and click **Next**.



1. At the **Completing the IP Security Policy Wizard** screen leave the Edit properties checkbox selected and click **Finish**



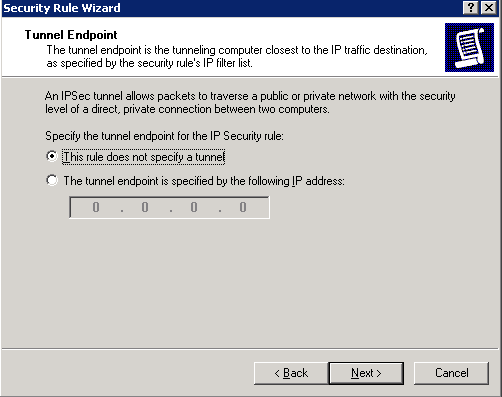
1. The properties page for the policy opens.



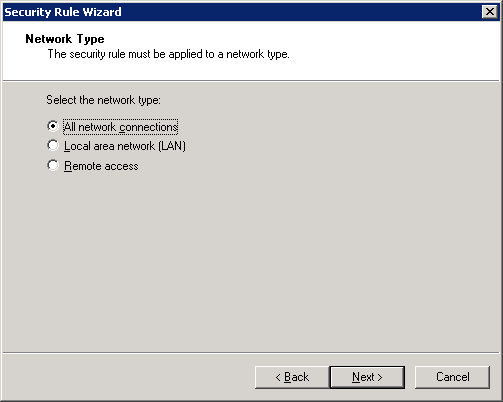
1. Click the **Add** button to start the **Welcome to the Create IP Security Rule Wizard**



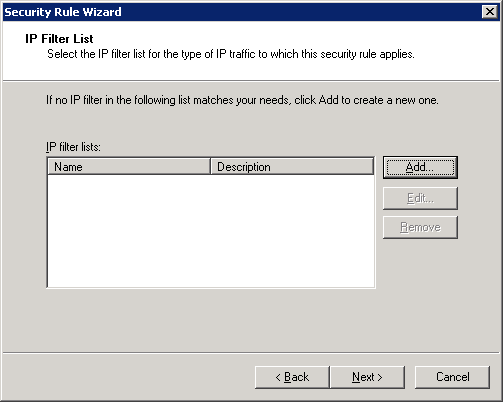
1. At the **Tunnel Endpoint** page of the wizard leave the default option of **This rule does not specify a tunnel** and then click **Next**.



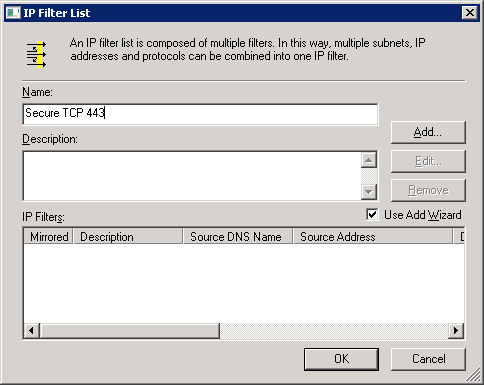
1. At the **Network Type** page of the wizard leave the default of **All network connections** and click **Next**.



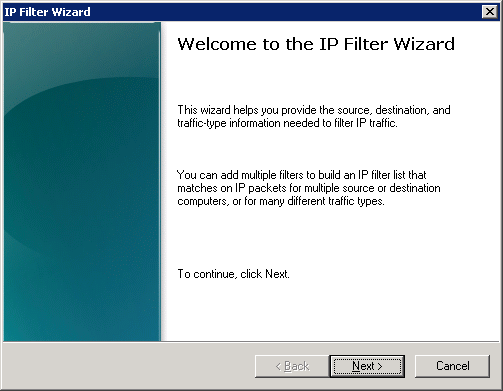
1. At the **IP Filter List** page click **Add** to create a new IP filter list.



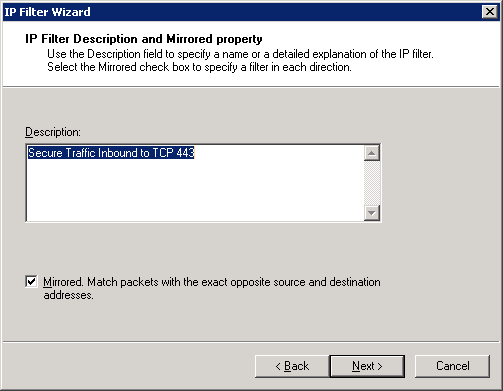
1. Give the new IP Filter List a meaningful and descriptive name.



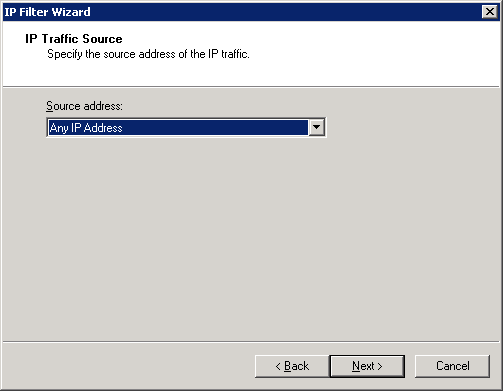
1. Click **Add** to launch the **IP Filter Wizard**.



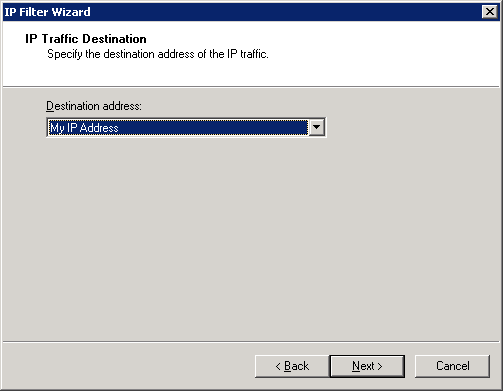
1. Click **Next** and then provide a meaningful description, then click **Next**.



1. On the **IP Traffic Source** page, use the drop down box to choose **Any IP Address**, then click **Next**.

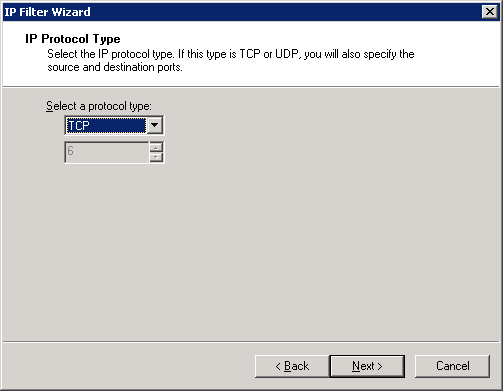


1. On the **IP Traffic Destination** page of the wizard, choose **My IP Address**. If you have multiple external IP addresses on your Forefront TMG or UAG system and you only wish to secure connections using TCP 443 to just one of those IP address, choose A specific IP address or subnet from the dropdown list and enter the external IP used by TMG or UAG for the traffic.

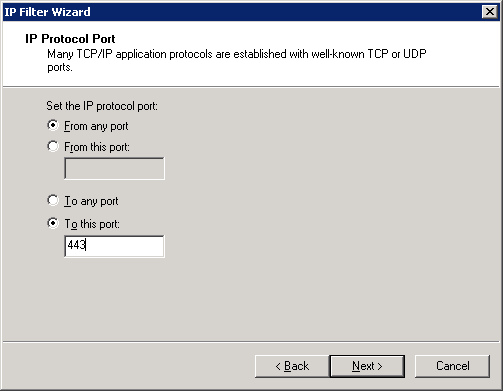


**Note**: IPSec “destination” selections refer to the host that accepts the connection. These policies automatically allow response traffic on a given connection, so there is no need to create a reciprocal IPsec policy for response traffic to the connecting client.

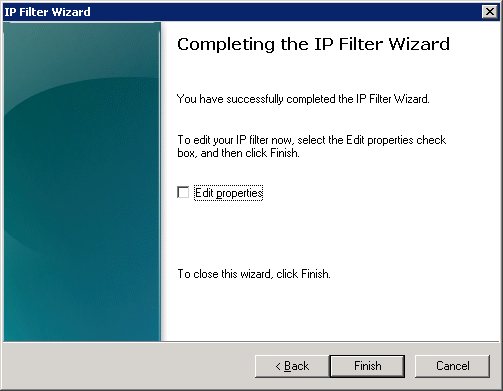
1. Click **Next** and choose **TCP** as the protocol type on the **IP Protocol Type** page of the wizard. Then click **Next**.



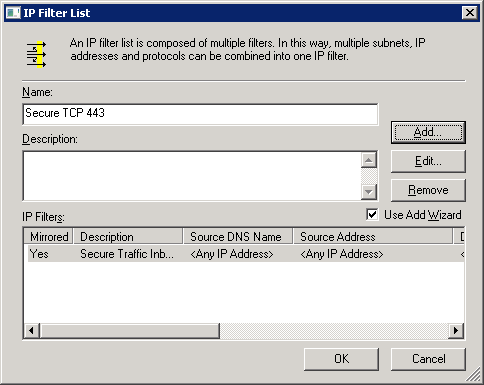
1. Click the radio button next to **To this port** and enter 443. All connections to Exchange are being made to TCP 443, the port commonly used by the HTTPS protocol.



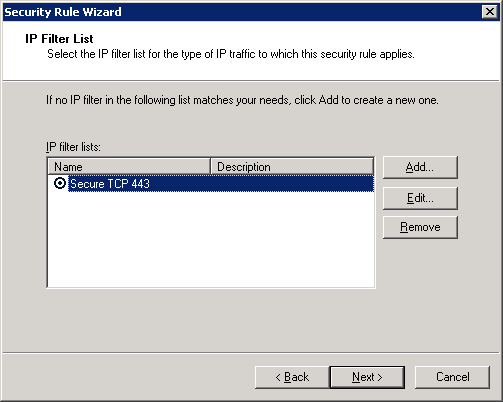
1. Click **Next**, then click **Finish**.



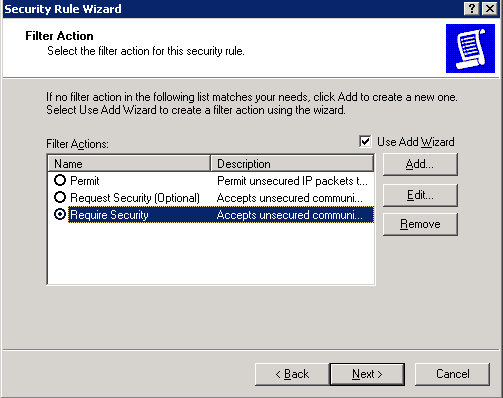
1. Click **OK** to close the IP Filter List wizard.



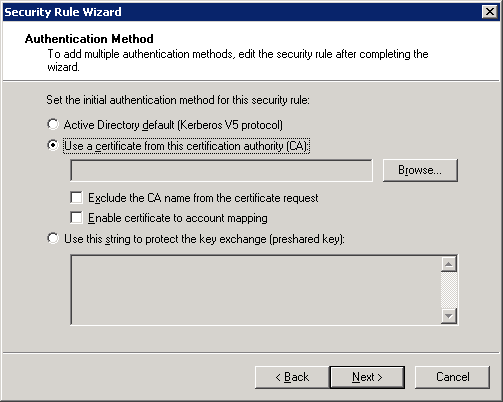
1. Check the radio button next to the IP filter list you just created, then click **Next**.



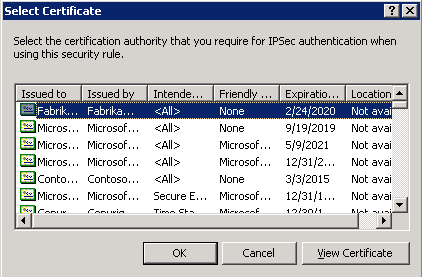
1. The default Filter Action will vary based on operating system. For newer versions of Windows, the **Nego** Filter Action uses data integrity, not encryption as its defaults, and uses the SHA1 algorithm for integrity. On earlier versions of Windows the **Require Security** Filter Action provides the same settings. If these settings are acceptable, click the radio button next to the filter action name and click **Next**. If you wish to add encryption to the configuration (remember that Exchange traffic is SSL encrypted already) or change the algorithm used, you can just edit the existing Filter Action or create a new one. It is important that any changes made here are reflected in the client policy.



1. At the **Authentication Method** page of the wizard, check the radio button next to **Use a certificate from this certification authority (CA)**. You can alternatively choose the preshared key option at the bottom of the dialog to use a text passphrase, remembering that this is less secure and not practical for mass deployment.

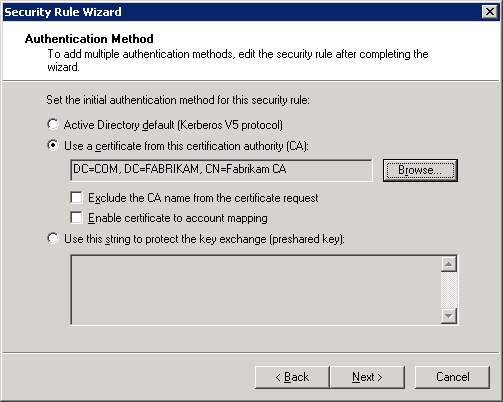


1. Click the **Browse** button to bring up a list of all installed CA’s. Select your root CA from this list and click **OK**.



**Note:** the issuing CA certificate must be trusted by the remote host or certificate-based IPsec negotiations will fail.

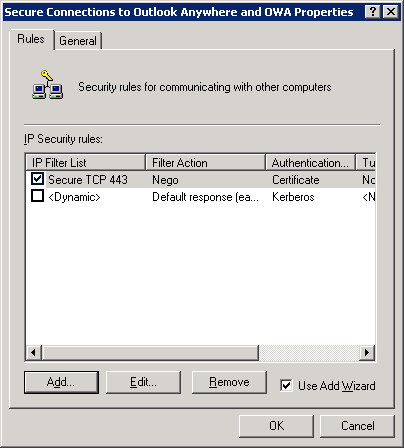
1. The CA is added to the Authentication Method page of the wizard. You can additionally choose to further secure the certificate authentication method by selecting the Exclude the CA name from the certificate request checkbox, which prevents the client from exposing the CA name during negotiation. When your selections are made, click **Next**.



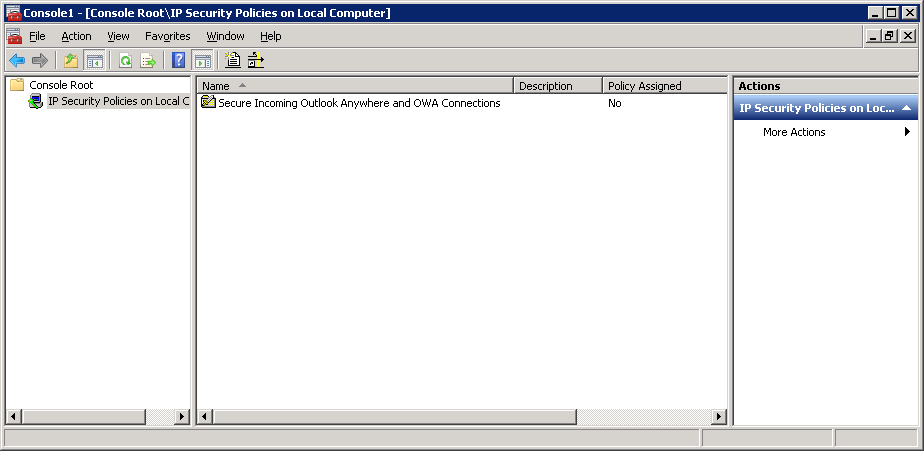
1. Click **Finish** to complete the wizard.



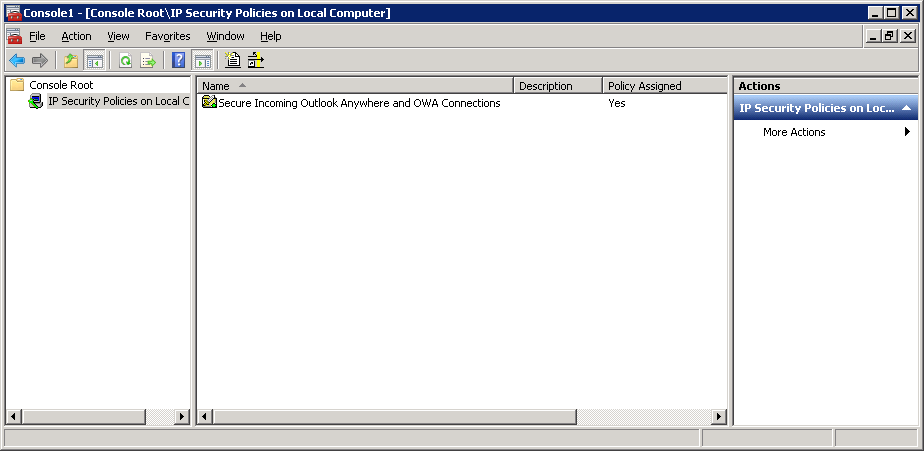
1. Click **OK** to complete the creation of the policy.



1. The IP Security Policies MMC shows the policy as created, but not assigned.



1. To assign the policy to the client simply right click the policy object and choose **Assign**.



1. All incoming connections now made from a client, to the specified IP address, when using TCP 443 will negotiate IPsec integrity only, using a certificate from the chosen CA. Close the IP Security Policies MMC.

## References

TechNet IPSEC Start Page - <http://technet.microsoft.com/en-us/library/cc783420(WS.10).aspx>

The IPSEC Process - <http://technet.microsoft.com/en-us/library/cc776080(WS.10).aspx>

IPSEC and NAT-T - <http://blogs.msdn.com/b/james_morey/archive/2005/04/29/413572.aspx>

Windows Firewall and IPsec Policy Deployment - <http://technet.microsoft.com/en-us/library/cc732400(WS.10).aspx>

AuthIP in Windows Vista - <http://technet.microsoft.com/en-us/library/bb878097.aspx>

What's New in Windows Firewall with Advanced Security - <http://technet.microsoft.com/en-us/library/cc755158(WS.10).aspx>

Public Key Infrastructure for Windows Server 2003 - <http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx>

IPsec troubleshooting section based upon the material available in the Microsoft Press title MCSA/MCSE Training Kit (Exam 70-299): Implementing And Administering Security In A Microsoft Windows Server 2003 Network (ISBN: 0-7356-2061-X)

For more information about Exchange Server, see the following resources:

* [Microsoft Exchange Server 2010](http://go.microsoft.com/fwlink/?LinkID=21573)
* [Exchange Server 2010: Exchange 210 Help](http://go.microsoft.com/fwlink/?LinkID=135761)
* [Unified Communications Certificate Partners for Exchange Server and for Communications Server](http://go.microsoft.com/fwlink/?linkid=3052&kbid=929395)

For more information about Forefront UAG, see the following resources:

* [Forefront Unified Access Gateway (UAG) 2010](http://go.microsoft.com/fwlink/?LinkId=196383)
* [Forefront Unified Access Gateway (UAG)](http://go.microsoft.com/fwlink/?LinkId=196384) 2010 on TechNet

For more information about Forefront TMG, see the following resources:

* [Forefront Threat Management Gateway (TMG) 2010](http://go.microsoft.com/fwlink/?LinkId=196382)
* [Forefront Threat Management Gateway (TMG) 2010](http://go.microsoft.com/fwlink/?LinkId=196385) on TechNet

## Legal Notice

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Mobile, Windows Server, Active Directory, ActiveSync, Forefront, Outlook, and SharePoint are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.