



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Enabling Windows 2000 IPSec Using Certificates

By Mark Ellister

Introduction –

IPSec provides a transparent method of providing secure authentication and encryption of network traffic over Tcp/Ip. The Microsoft implementation of IPSec was jointly developed by Cisco¹ and Microsoft based upon the IP security protocol working group of the Internet Engineering Task Force (IETF) ². IPSec provides end-to-end protection that compliments the perimeter, access control, and physical levels of security that may already exist in your networking environment.

IPSec provides 3 primary functions –

- Authenticity – non-repudiation of the sender of the data
- Integrity – Ensures no in transit modifications have been made to the data
- Confidentiality – Encrypts the data in transit and can hide the originating IP address

The Microsoft implementation of IPSec can also provide a secondary function of Packet or IP filtering. This provides some Firewall-like functions at a lower level of the protocol stack than the Tcp/Ip filtering options found in the advanced section of the protocol properties. IPSec filtering operates independently from the authentication and encryption functions and can be used for added security in situations where you cannot use the encryption and authentication functionality because of compatibility reasons, like communications with foreign systems where you have no control over that particular system.

This document will not cover advanced features of IPSec or a Public Key Infrastructure (PKI), but will rather provide a background of what is necessary to enable default IPSec policies using Certificates. The goal of this document is to educate to a point of allowing the reader to easily setup a pilot or test environment in which to explore the more advanced features of IPSec and allow fine-tuning for your particular organization or network. IPSec can be configured to use Certificates either inside or outside of Active Directory but the primary focus of this document will be configuration outside of Active Directory, the main difference being that many of the same things in this document configured locally may be achieved using Group Policy inside Active Directory.

Authentication methods –

Microsoft provides three methods of authentication for enabling IPSec-Kerberos, pre-shared key and certificates.

¹ http://www.cisco.com/warp/public/cc/techno/protocol/ipsecur/ipsec/tech/ipsec_wp.htm

² <http://www.ietf.org/html.charters/ipsec-charter.html>

1. Kerberos – is the authentication policy set by default and will only function inside an Active Directory environment. Because of Active Directory's ability to manage computer settings with Group policy and because of the strength of the Kerberos authentication method, this is the best choice inside an AD environment. Group policy overrides local policy in an AD setting, ensuring that the setting on any machine controlled by group policy have not been altered, adding to the security of your environment. When using Kerberos authentication the client machine will be automatically configured to support this option when it joins an AD enabled Domain. It is possible to use a combination of Kerberos and Certificates in an advanced IPSec setup if needed for compatibility with outside systems.
2. Pre-shared Secret – “Microsoft does not recommend frequent use of pre-shared key authentication, because the authentication key is stored unprotected, in the IPSec policy. Pre-shared key methodology is provided ONLY for interoperability purposes and to adhere to the IPSec standards set forth by the IETF³.”

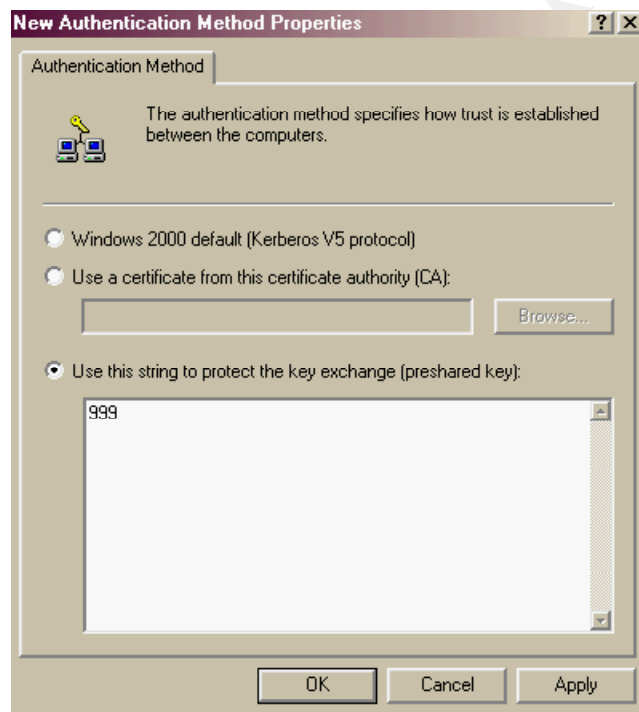


Figure 1- setting the pre-shared password in IPSec policy

Setting the IPSec policy to pre-shared and placing 999 as the password, we can easily navigate to the corresponding IPSec policy in the registry and find that password. The password, is always preceded and followed by the same hex values in the key named "IPSec Data" and thus figuring

³ Microsoft Windows 2000 resource kit - TCP/IP Core Networking Guide pg. 610

out the actual password is an easy task. Knowing this password would allow anyone with that knowledge to possibly view or compromise transmitted data.

Example 1- IPSec policy registry entry exposing the pre-shared Key password.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local\ipsecNFA{E404D08E-A1A1-4148-A224-10B8D31E1BD4}]
"ClassName"="ipsecNFA"
"ipsecID"="{E404D08E-A1A1-4148-A224-10B8D31E1BD4}"
"ipsecNegotiationPolicyReference"="SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local\ipsecNegotiationPolicy{1B04FEC2-300F-4DA0-9695-0177D20D6A9D}"
"ipsecName"="SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local\ipsecNegotiationPolicy{1B04FEC2-300F-4DA0-9695-0177D20D6A9D}"
"ipsecDataType"=dword:00000100
"description"="• "
"ipsecData"=hex:00,ac,bb,11,8d,49,d1,11,86,39,00,a0,24,8d,30,21,30,00,00,00,01,\
00,00,00,01,00,00,00,08,00,00,00,39,00,39,00,39,00,00,00,fd,ff,ff,ff,02,00,\
00,00,00,00,00,00,00,00,00,00,00,00,01,00,00,00,02,00,00,00,00,00,00,00,\
"whenChanged"=dword:3b2fd724
"name"="ipsecNFA{E404D08E-A1A1-4148-A224-10B8D31E1BD4}"
"ipsecOwnersReference"=hex(7):53,00,4f,00,46,00,54,00,57,00,41,00,52,00,45,00,\
5c,00,50,00,6f,00,6c,00,69,00,63,00,69,00,65,00,73,00,5c,00,4d,00,69,00,\
63,\
00,72,00,6f,00,73,00,6f,00,66,00,74,00,5c,00,57,00,69,00,6e,00,64,00,6f,\
00,\
77,00,73,00,5c,00,49,00,50,00,53,00,65,00,63,00,5c,00,50,00,6f,00,6c,00,\
69,\
00,63,00,79,00,5c,00,4c,00,6f,00,63,00,61,00,6c,00,5c,00,69,00,70,00,73,\
00,\
65,00,63,00,50,00,6f,00,6c,00,69,00,63,00,79,00,7b,00,32,00,32,00,32,00,\
43,\
00,43,00,44,00,45,00,37,00,2d,00,38,00,41,00,43,00,30,00,2d,00,34,00,42,\
00,\
45,00,37,00,2d,00,39,00,37,00,32,00,35,00,2d,00,37,00,45,00,30,00,38,00,\
35,\
00,36,00,42,00,32,00,41,00,33,00,31,00,32,00,7d,00,00,00,00,00
```

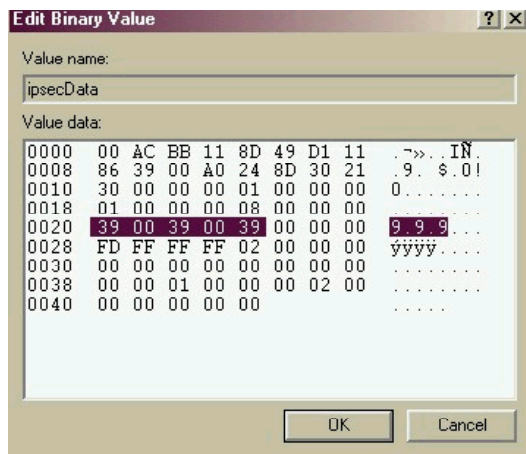


Figure 2 - Displaying the password as stored in the registry

3. Certificates – You can also use certificates generated from 3rd party vendors or from an existing PKI to enable IPsec. If you need to enable IPsec for Windows 2000 outside of Active Directory, this is the preferred method. Certificate Authentication can also be used inside Active Directory taking full advantage of AD's ability to auto-enroll computers for certificates. You can create your own certificate server using Microsoft Certificate Services. Creating your own Root authority can have a small advantage in that you can control the distribution of the root certificate as well as machine certificates. 3rd party vendors also offer many different kinds of solutions such as Baltimore Technologies who offers a W2K integrated solution that is compatible inside or outside of an Active Directory environment ⁴.

Requirements for Using Certificates -

In order to successfully use Certificates to enable IPsec some sort of Public Key Infrastructure (PKI) must be in place. This can be a 3rd party solution or you can use Microsoft Certificate services to create your own PKI. Each machine will need 2 certificates.

- Certificate Authority root certificate – This certificate contains the public key of the Certification Authority you designate to use in the IPsec policy and is also called the root certificate. You can set multiple CA's if required. Most 3rd Party root certificates come installed with Windows 2000 by default, and additional ones may be included with your web browser software. The root certificate identifies the organization or authority you choose to "trust" as having proper private key management and protection as well as the legal responsibility for it's authenticity.

⁴ <http://www.baltimore.com/unicert/unicert/whatsnew.html>

- **Machine or User Certificate** – This certificate contains a public/private key pair created for the local machine or local user by the same Certificate Authority you designated to use for your CA public key. While it is possible to properly obtain and install a Private Key pair for an IPSec Certificate stored in the User Certificate store, IPSec will use the Machine (Local Computer) certificate store.⁵ The implications of this are that you must have administrative access to the local machine to generate the private key pair.

This pair of certificates will be used by IPSec to exchange keys used to authenticate and encrypt the data. The exchange process called Diffie-Hellman is mathematical formula used to agree upon a shared symmetric key without ever exposing that shared key over the network.

Creating a Certificate Server –

If you already have a PKI solution in place you may want to skip this section. This brief walkthrough of setting up Microsoft Certificate Services provides the minimum necessary to enable IPSec and will be used further in this document to show examples of how the PKI interacts with IPSec. This is not meant as a guide for setting up a PKI, which should be researched separately to fit your unique situation or organization.

To set up a CA add certificate services from the windows components area in the ADD/REMOVE icon in the control panel. Simply adding the service will invoke a wizard that will ask you the questions necessary to set up the CA. It is important to note that once the CA has been created the machine cannot be renamed or join or be removed from a domain.

⁵ Microsoft Knowledge Base article Q253498

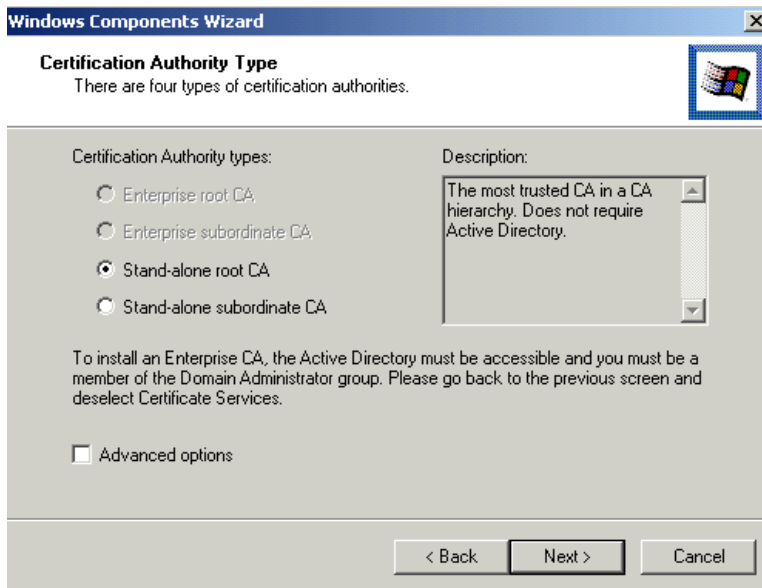


Figure 3 -Step 1 in the wizard is to choose the type of CA you are creating

Step 2 - if the advanced options checkbox was selected you will have the opportunity to choose the cryptographic service provider, hash algorithm, key length or to use an existing key. Be sure whatever CSP you choose is supported by any other 3rd party hardware or software you may be integrating with. If you are unsure or have no 3rd party devices it is safe to choose the Microsoft Base Cryptographic Provider as it will provide good functionality and compatibility with most other systems. Choose SHA-1 as the Hash algorithm. SHA-1 is based upon MD5 and is slightly better, though either SHA-1 or MD5 are good choices. You also have the option to Import a key if you desire. This is available for migration or disaster recovery purposes. You could then use an existing CA key from a 3rd party Certificate Authority if you wished to change to Microsoft Certificate services and retain the same CA private key pair.

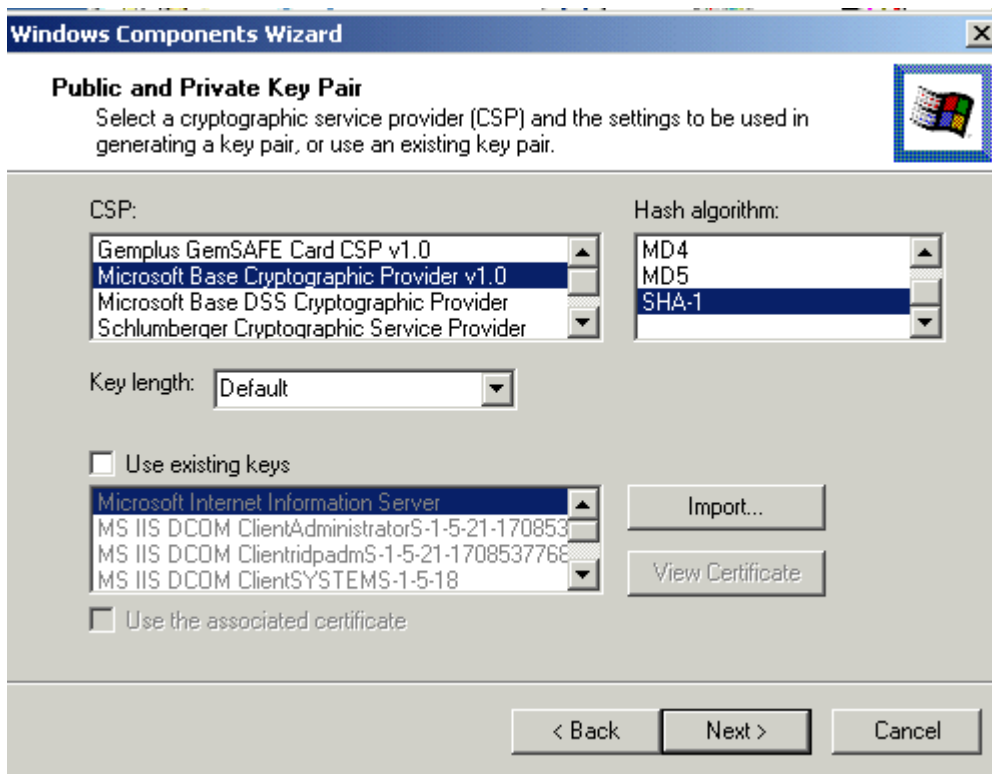


Figure 4 - Step 2 choose the Cryptographic Provider

Name the CA. This cannot be changed later so be sure to choose wisely. For example naming the organizational unit “finance” in some cases can cause problems down the road so be as granular and specific as possible to avoid future conflicts. Creating a new and unique organizational Unit for the CA may be desirable if future growth of your organization is unknown and you want to ensure minimal conflict with other departments. Also try to ensure the CA name is completely unique. Choosing Verisign or even something similar to any existing certificate authority will likely get you into legal trouble.

The screenshot shows the 'CA Identifying Information' dialog box from the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. Below the title bar, the text 'CA Identifying Information' is displayed, followed by the instruction 'Enter information to identify this CA'. The dialog box contains several input fields: 'CA name' (TEST ROOT CA), 'Organization' (TEST COMPANY), 'Organizational unit' (TEST DEPARTMENT), 'City' (ANYTOWN), 'State or province' (OR), 'Country/region' (US), 'E-mail' (emailname@yourdomain.com), 'CA description' (this is a test CA), and 'Valid for' (2 Years). The 'Expires' field shows '6/15/2003 2:16 PM'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

CA name:	TEST ROOT CA		
Organization:	TEST COMPANY		
Organizational unit:	TEST DEPARTMENT		
City:	ANYTOWN		
State or province:	OR	Country/region:	US
E-mail:	emailname@yourdomain.com		
CA description:	this is a test CA		
Valid for:	2	Years	Expires: 6/15/2003 2:16 PM

Figure 5 - name the Certificate Authority

Select the data storage location. This must be an NTFS drive. The option is given to split the database and log file locations. If your CA will have an extremely high volume of traffic you may want to consider placing the database on a RAID 5 partition and the Log files on a RAID 1 partition to increase performance. Follow the same general rules you would for any database server based upon sizing and transactions/second requirements.⁶

⁶ For more information on performance tuning I highly recommend the book "Tuning and Sizing Windows 2000" by Curt Aubley ISBN 0-13-089105-3

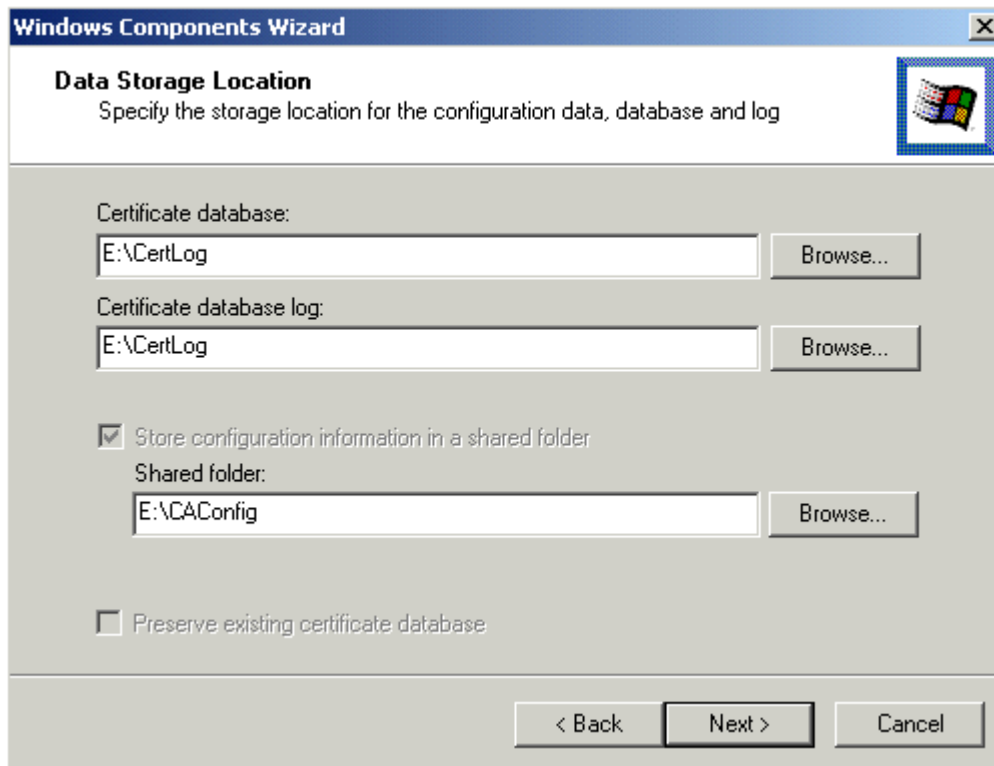


Figure 6 - Select the data storage location

Follow the prompts to finish setup. Once you have a CA and the capability for providing PKI infrastructure you can install the necessary certificates needed to enable IPSec.

Requesting Certificates –

In order for IPSec to function using certificates you need to install and verify both a Root Certificate and a Machine or User certificate. If you are using a 3rd party PKI you probably already have the Root certificate installed as many standard ones are built into Windows 2000 and/or Internet Explorer and other browsers. You should follow the manufacturers method of client, machine or user certificate installation on 3rd party PKI systems. Lets look at an example of certificate installation using the CA we setup in the previous section.

CA Root Certificate Install –

The public key for the CA must be installed as this is the particular selection

made in the IPsec settings that tell the machine which certificates to use. Having machine certificates of a particular CA will do you no good if you do not have the root certificate for the same CA installed. Microsoft Certificate services by default when installed will add a web site where you can conveniently request and retrieve certificates. Browse to <http://yourcertserver/certsrv> and select “retrieve the CA certificate” option and press NEXT.

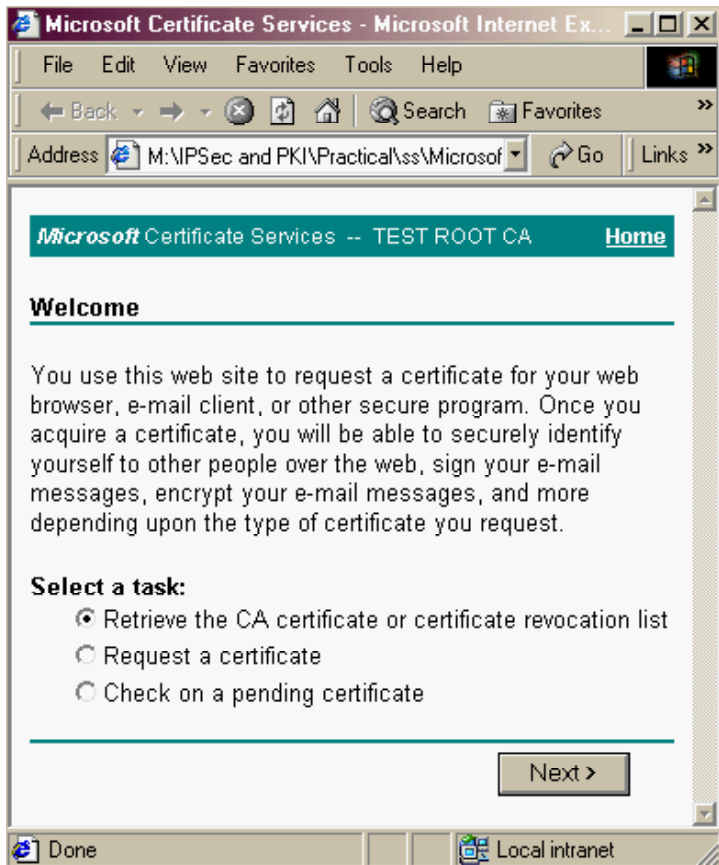


Figure 7 - The MS Certificate Services home page

The CA certificate screen will be displayed. If you click on the first link to automatically install the CA root certificate to the local machine I found in testing it sometimes places the certificate in the Local User Certificate store.

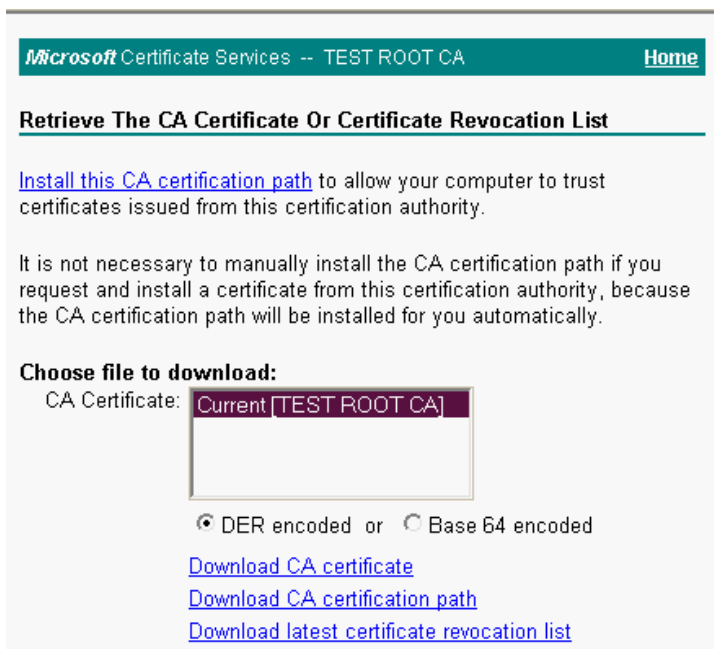


Figure 8 - CA Root Certificate installation page

IPSec requires the root certificate in the Machine (Local Computer) Certificate Store. To ensure the certificate gets placed in the proper store you should first download the certificate. If you have a hierarchical CA you will need to download the CA path. Once the Certificate is downloaded, simply double click on the certificate and choose the “Install Certificate” button. In the Import wizard that is presented to you instead of choosing the default “automatically select the certificate store for this type of certificate”, choose the “place all certificates in the following store” option. Hit the browse button and navigate to the Trusted Root Certification Authorities\Local Computer location and install the certificate at that location. This will ensure IPSec certificate functionality.



Figure 9 - Selecting the Machine Store on Certificate Install

Machine Certificate –

Next you will need a local certificate for the Machine with a public/private key pair. Navigate to the <http://yourcertserver/certsrv> homepage again and select “request a certificate” and press NEXT. On the next screen since IPsec certificates are not displayed select “advanced request” and press NEXT. Then select “submit a certificate to this CA using a form” and press NEXT again. You will use this form to request an IPsec certificate for the machine.

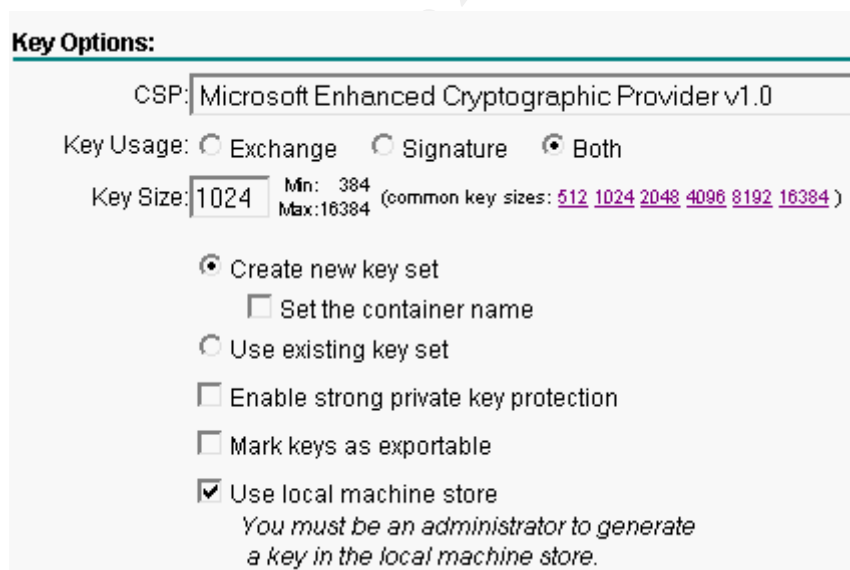
Fill out identifying information in the spaces provided. Make sure you select IPsec certificate on the Intended purpose drop-down.



The screenshot shows a web form section titled "Intended Purpose:". Below the title is a dropdown menu with a purple background and white text. The selected option is "IPSec Certificate".

Figure 10 - Selecting an IPsec certificate

Under Key options select Microsoft Enhanced Cryptographic Provider and set the key size to at least 1024 bits to have a good key strength. Also notice the option “Use local Machine store”. This is where you decide between a User certificate or a Machine certificate. Select the box to create a machine certificate to ensure IPsec functionality. You must have local administrator privileges to generate this key. If you wish to have the ability to move the key to other locations you can select the “mark keys as exportable” option, but this also could possibly allow key compromise, so don’t select that option unless absolutely needed.



The screenshot shows a web form section titled "Key Options:". Below the title, there are several options and settings:

- CSP: Microsoft Enhanced Cryptographic Provider v1.0
- Key Usage: ☐ Exchange ☐ Signature ☒ Both
- Key Size: 1024 (Min: 384 Max: 16384 (common key sizes: 512 1024 2048 4096 8192 16384))
- ☒ Create new key set
 - ☐ Set the container name
- ☐ Use existing key set
- ☐ Enable strong private key protection
- ☐ Mark keys as exportable
- ☒ Use local machine store
 - You must be an administrator to generate a key in the local machine store.*

Figure 11 - Key options

Under additional options on the same form you can select the Hash type. Choose SHA-1 or MD5. SHA-1 is slightly better than MD5, but either are

acceptable and superior to the other choices. Press the submit button and your request will be sent to the CA. You must then wait for the administrator of the CA to approve or reject the certificate before you can complete the install.

Accepting the User's request –

Once a certificate request has been sent to your CA, an administrator must accept or reject that request. This is done using the Certificate Authority MMC snap in, also present in the Administrative tools section on the server running Certificate Services. Under pending requests, right-click on the requested certificate and choose "issue". Unfortunately on a stand-alone Microsoft CA the information you get on the certificate request is somewhat less than complete. The "certificate type" field will be blank as well as many others so you have no information on what type of actual certificate the user has requested other than the basic values entered on the form, which may or may not be valid. You will receive no information on the key strength, hash value or many other settings. There is also no policy settings within the stand-alone CA on which type of certificates are presented as valid selections to the user.

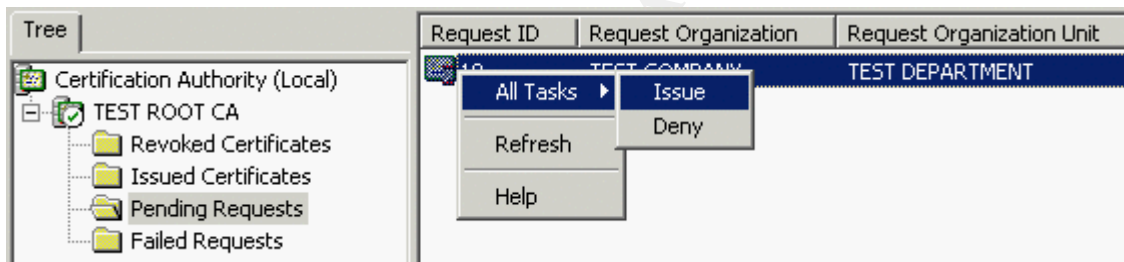


Figure 12 - Issuing a Certificate from the CA

There are steps you can take to help with this however. You can remove anonymous access from the IIS server on the certsrv web site. The logged in user will be displayed in the request and you can dictate who does or does not have access to the folders on the website.. Alternately you can accept or reject based upon that login information as well, letting any user log into the server but only accepting requests from specific accounts if you wish to track users who are trying un-officially or illegally to receive a certificate. The CA itself also has Security ACLs which can be modified to suit who can or cannot enroll or accept/deny a request. Also remember to assign the certsrv website it's own web certificate and enable SSL to ensure that all transactions are kept confidential.

Final Installation of the Machine Certificate –

Once the request has been approved you can go back to the Certificate Server web site and choose “check on a pending certificate”. Any certificates that have been requested will be visible. Select the desired certificate and press NEXT.

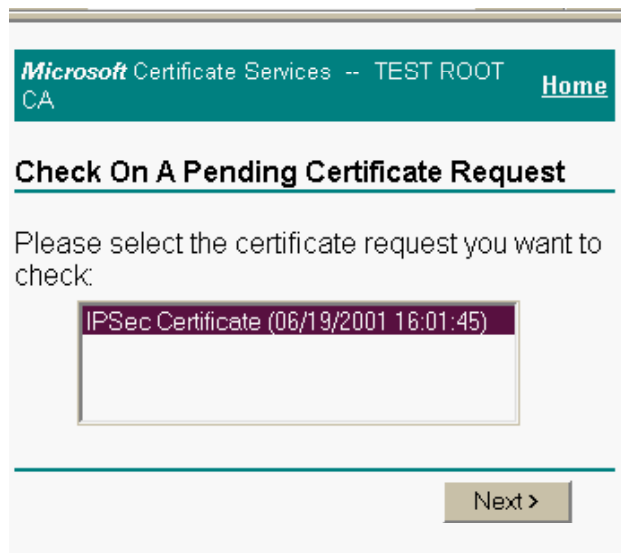


Figure 13 - checking on a pending certificate

Simply click the link on the next page to install the certificate. You must use the same browser that you previously used to request the certificate.

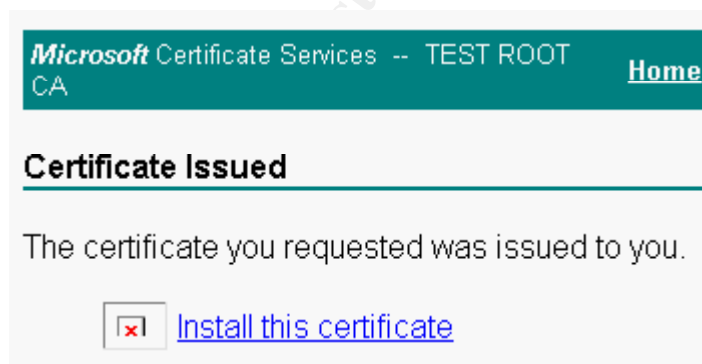


Figure 14 - Install certificate link

Verifying installation of certificates –

To see the certificates installed on your machine you use another MMC snap in. Adding the certificates snap-in you can manage the local user certificates, the machine certificates or a service account certificates. The personal folder will hold machine account certificates or personal user account certificates depending on how you loaded the MMC. You can load multiple certificate snap-ins at once, including multiple machine stores from different computers is necessary. You should be able to find the machine certificate you requested and also the Root Certification Authority certificate of your CA in the Local Computer store. If you cannot find the installed certificates here, check the Current User store as they may have been installed to the wrong location. Review the installation procedures and ensure that both the trusted root public key and the machine private/public key pair in the personal folder are installed in the Local Computer certificates store.

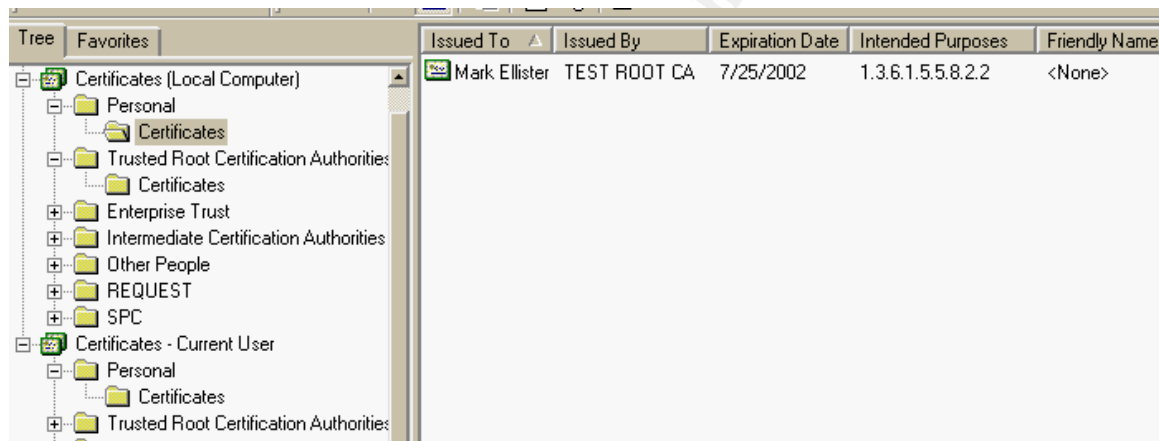


Figure 15 - certificates MMC snap-in showing local machine certificates

Enabling IPSec -

Once the necessary certificates have been installed you use another MMC snap in to configure IPSec. This MMC snap in is also contained in the Local Security Policy Icon in the Administrative tools area. Windows 2000 comes with 3 default IPSec policies. We will be modifying these basic policies to use certificates. You can restore the original policy configuration at any time by selecting “restore default policies” from the “all tasks” menu by right clicking on the IP security policies icon.

There are 3 default IPSec policies -

- Client Respond – used to enable IPSec when connecting to another machine that requests or requires IPSec.
- Server Request – used to request IPSec from incoming connections but does not require it.
- Server Require (Secure Server) – Used to force IPSec on all connections.

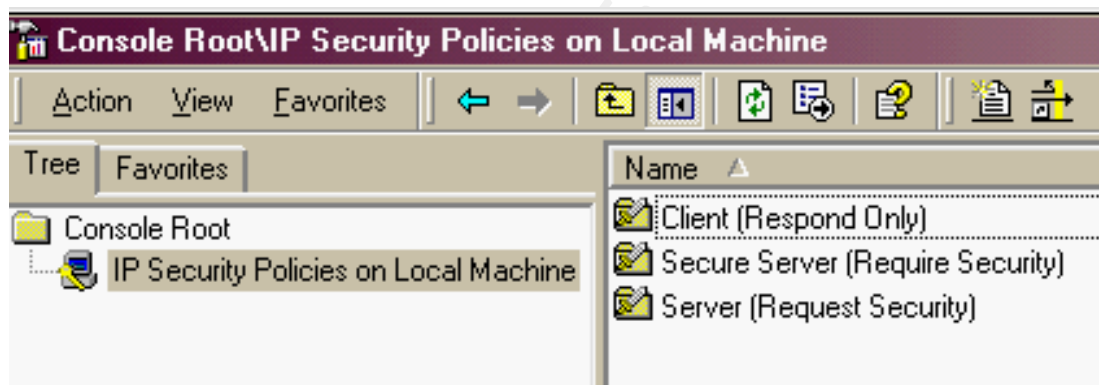


Figure 16 - Default IPSec policies

Generally speaking you, unless you are going to force encryption within your entire organization, you will enable the Client rule on workstations and then either the Server Request or Server Require policy on servers. This allows clients to communicate with other non-IPSec machines while encrypting data to the required locations. Once IPSec set up the connection state is seamless to the user and they can work as normal without knowing or needing to keep track of which connections use IPSec and which do not.

Client Respond Policy –

On a client workstation you wish to take part in IPSec (and also you have already installed both the proper root and machine or user certificate) open the properties on the Client IPSec policy. Select the dynamic filter and press the edit button. The dynamic filter rule will be present in all of the default policies so follow these steps to enable this rule on server policies as well.

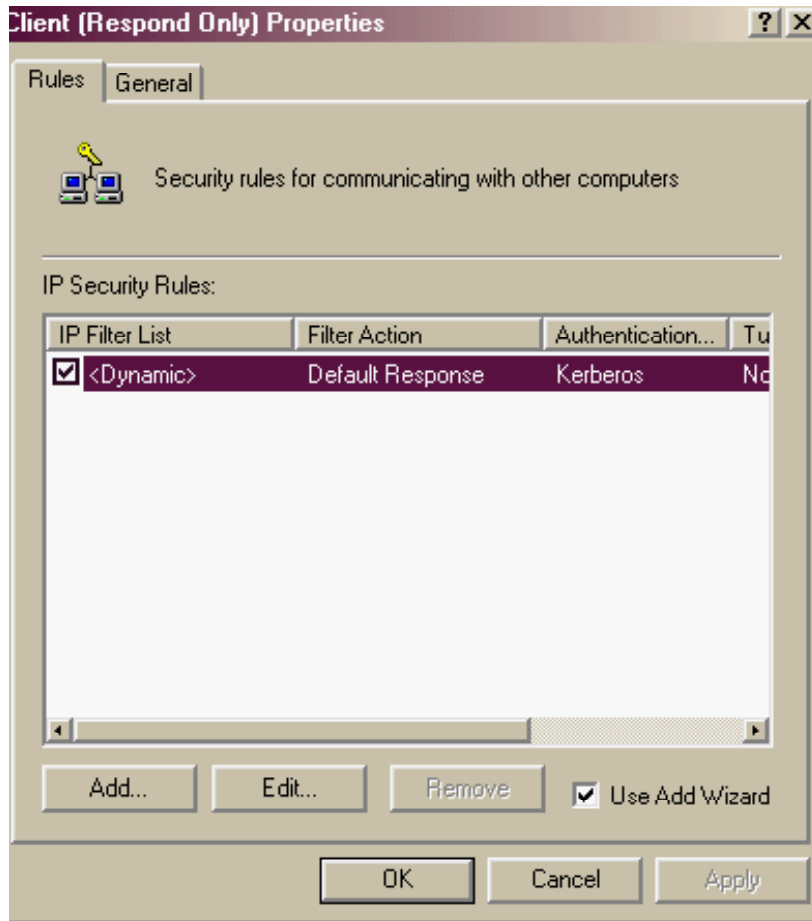


Figure 17 - The Dynamic filter list in the Default Client respond policy

The security methods tab is first displayed. This tab configures AH Integrity column and the ESP encryption methods. Custom modification of this area is beyond the scope of this document, however you may want to remove any encryption methods you know you will not be using. 3DES for ESP and SHA1 for AH are generally the best selections. Remember that to use 3DES you must have the High Encryption pack for IE installed or Windows 2000 SP2. If you wish to force 3DES then definitely remove the other standard DES settings so the authentication will not be accidentally downgraded to a lower encryption level. Do not remove the SHA1 (or the MD5 if you prefer that method) AH setting unless you wish to disable packet integrity. Next click on the Authentication methods tab.

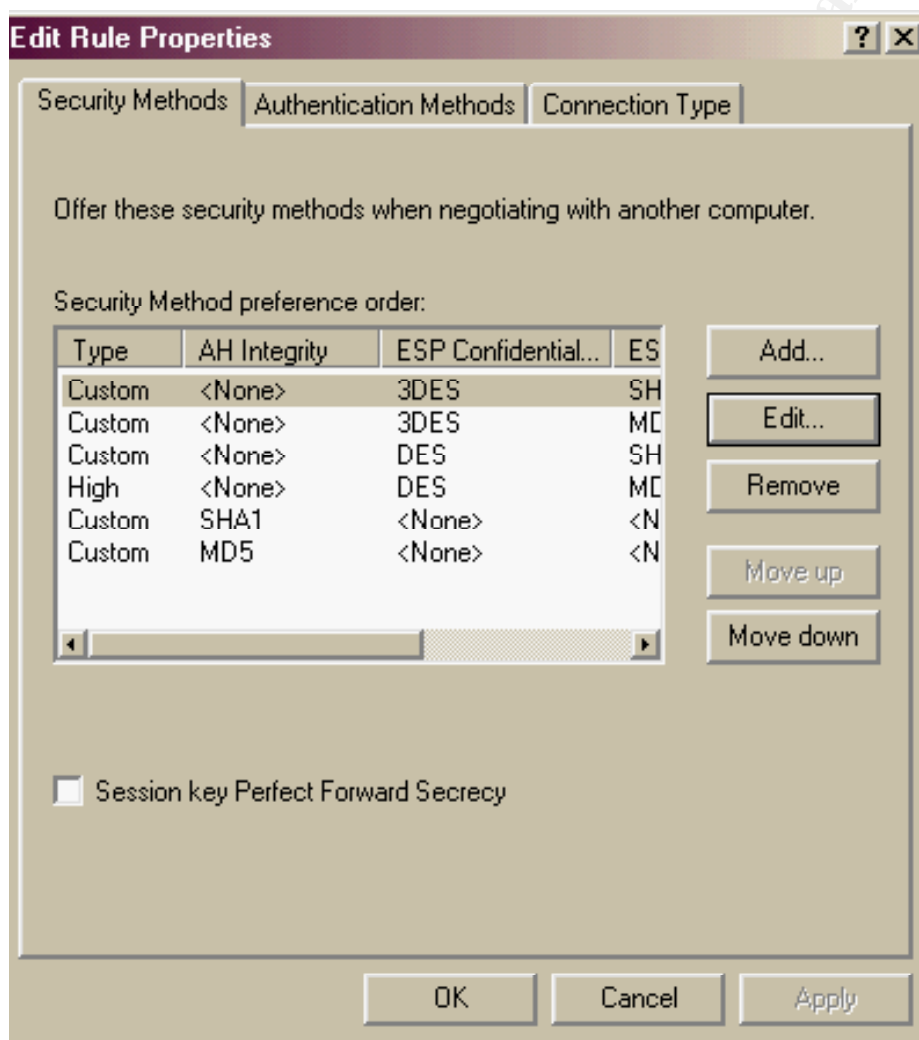


Figure 18 - Security methods tab

The authentication Methods tab will be set to Kerberos by default. Select the Kerberos method and hit the Edit button, or you can add a new authentication method and leave the Kerberos method in place if needed. You can also add several different types of Certificate Authentication from Different Root CA certificates. These methods will be attempted in the order shown. The first successful method will be used for that connection.



Figure 19 - The default Authentication Method setting - Kerberos

On the Authentication method selection tab choose the Certificate Authority selection and browse and find the Root certificate of the CA you wish to use to enable IPSec, in this case the Test CA we created earlier. Close all property windows.

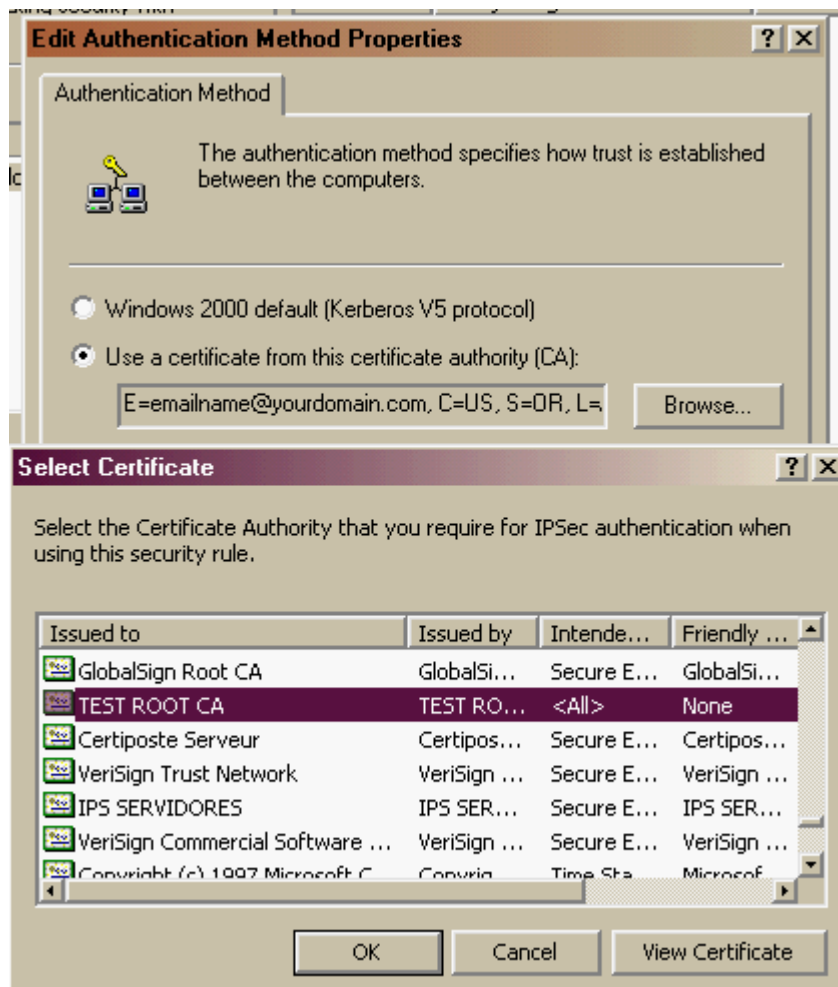
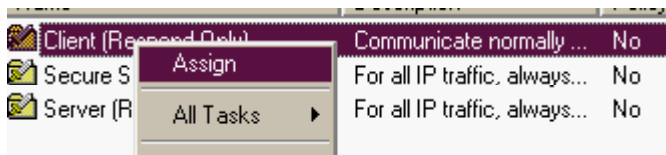


Figure 20 - select the Root Certificate Authority

Navigate back to the policy screen and Right-click on the policy you modified and select "assign". This will enable IPSec for the Client when any other machine using the same Authentication scheme requests encryption.



Server Request and Require Policy –

The Server policies will check for and either request or require IPsec for any incoming connections. The Request policy allows you to have simultaneous IPsec and non-IPsec connections. This can be helpful during migration or when you have a few clients that for some reason cannot participate in IPsec. Most situations, and obviously the most secure is to use the require policy.

By pulling up the properties of one of these policies you see the same <dynamic> response rule we saw in the client respond and also a couple of new ones. If you wish the server to respond to other security requests with IPsec configure the <Dynamic> rule as you did on client respond policy in the previous section.

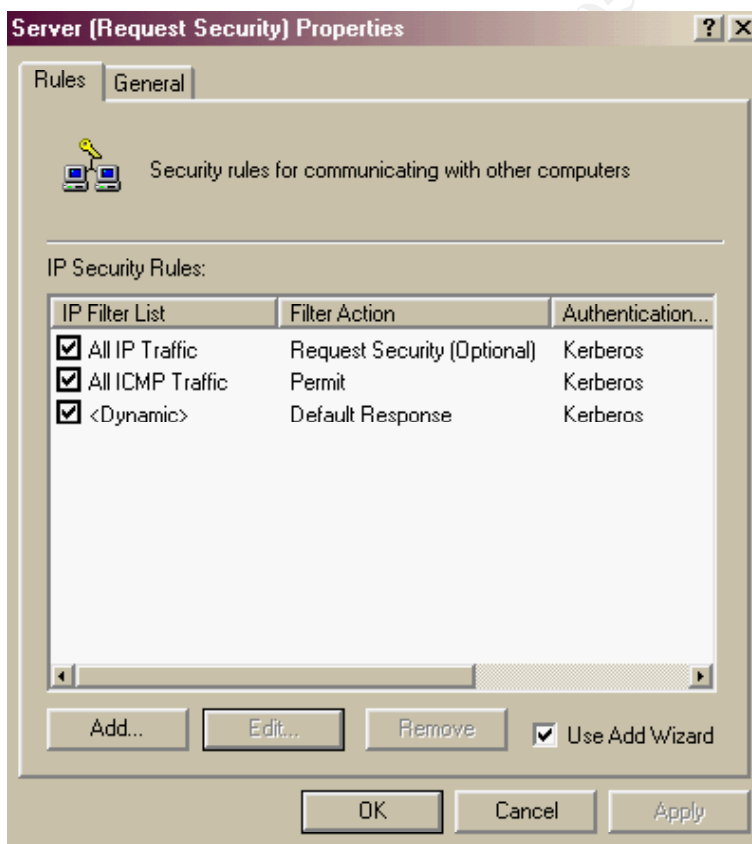


Figure 21 - default server rules

Select each rule and press the edit button, then set the appropriate

Authentication Method. The Authentication tab here is used to choose your CA certificate just like on the <Dynamic> rule. You must select the CA certificate for each rule in the policy you wish to be enabled in IPSec. So do the same in the ICMP rule if you wish that traffic to be enabled for IPSec as well.

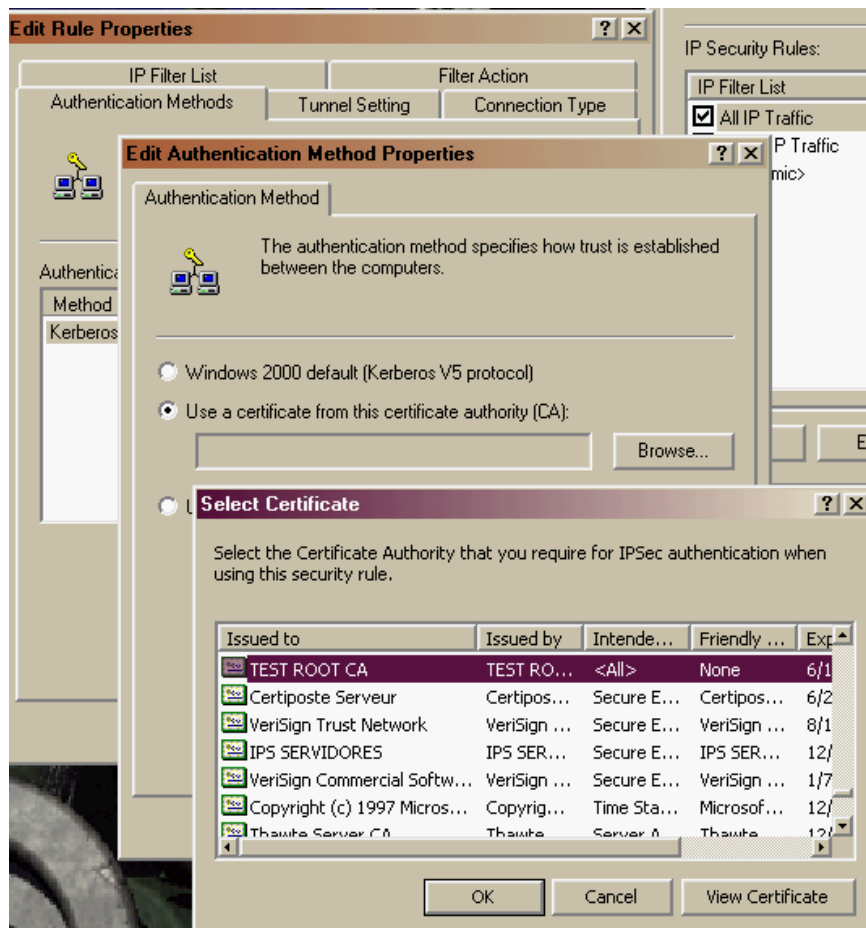


Figure 22 - Authentication tab within the "All IP Traffic" rule

No other changes are needed to these rules for IPSec to function. If you look at the Filter Action tab you will see that the only difference between the Default "server request" policy and the default "server require" policy is set there. After the policy has been configured don't forget to "assign" the desired one to enable it.

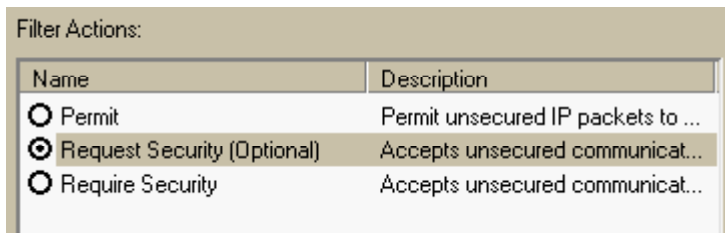


Figure 23 - settings in the "Filter Actions" tab

Verifying IPSec functionality –

To verify IPSec is working properly simply type IPSECMON in the run dialog box. This utility will show all current connections and their security status. If you have used the Request Security policy you can view which connections are using IPSec and which connections are not. A machine must attempt some sort of connection and negotiate security for it to be listed here.

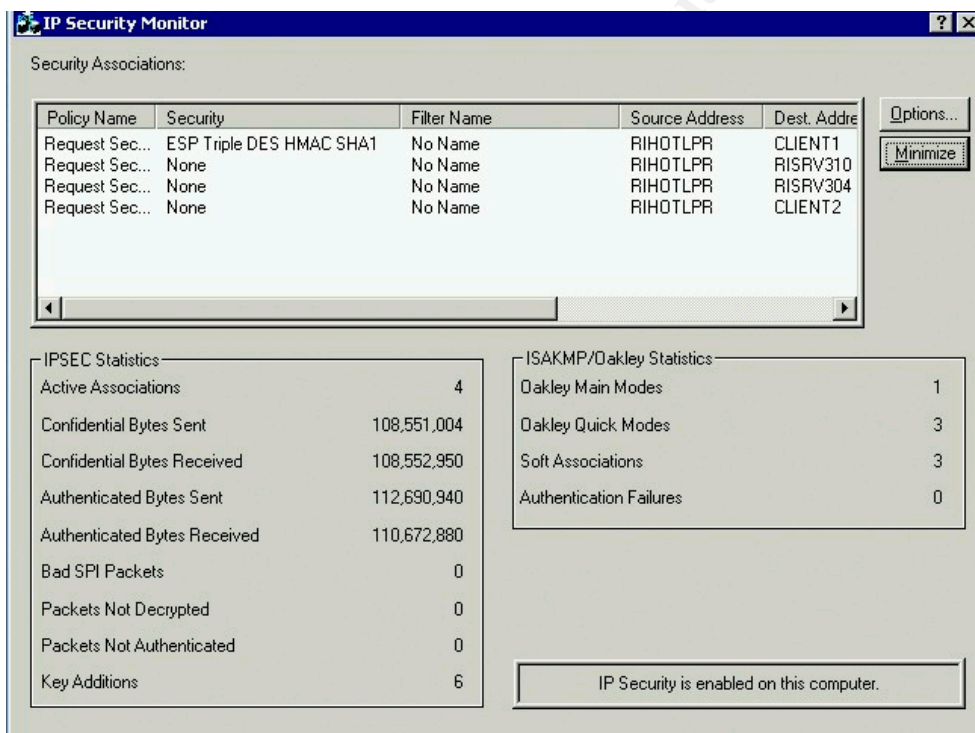


Figure 24 - IPSECMON showing both encrypted and non-encrypted connections

If the client computer makes a connection to the server and no encryption method is shown within IPSECMON then the policy is configured incorrectly. If the client cannot make a connection to the server, then it generally means that the security negotiation has failed. Check the security log file on the machines in question to find out what the failure is. Look for failures that mention the ISAKMP/Oakley or IPSec components and look up the error ID to identify the

problem. Also remember that Broadcast, Multicast, Resource Reservation Pool (RSVP), and Kerberos traffic cannot be secured by IPSec.⁷

Conclusion -

IPSec is designed to protect your IP network traffic and provides an excellent defense against the viewing of transmitted data, but also ensures the authenticity of the data. IPSec is an end-to-end security model, meaning that only the two computers communicating on either end understand the conversation taking place. The path the data takes is inconsequential to the privacy and authenticity of the communication. Other devices that are used in transit to pass, relay, or otherwise route the information to the endpoints do not have to support IPSec in any manner. This provides an extremely flexible platform to add to your existing security infrastructure.

This document provides a basic understanding of what is required to enable IPSec using certificates. This information should be sufficient to set up a pilot environment where you can explore additional functionality available within IPSec to meet your specific needs. It is also recommended that in a production environment new IPSec policies should be created rather than using default ones to avoid GUID duplication and conflict when attempting to Import an IPSec policy from one machine to another.⁸ Setting up a PKI infrastructure is also no small project and regardless of whether you choose to use a Public or Private PKI hierarchy, practicing in a test environment will save time and money down the road. It can be quite costly to change an existing PKI hierarchy once placed into production.

Many companies are migrating to Active Directory and its use of Group Policy to easily control security and configuration of system settings. IPSec using Kerberos can provide a seamless and user-friendly way of providing end-to-end security. However many companies are finding that Active Directory does not solve many of the problems associated with interoperability with foreign systems, and in fact can make things much more difficult in some situations. IPSec using certificates can help provide a secure channel between Windows 2000 systems regardless of Active Directory participation, thus providing an additional avenue for supporting foreign systems or outside business

⁷ Microsoft Knowledgebase Article Q253169

⁸ Microsoft Knowledgebase Article Q232817

connections without disrupting or compromising the existing Active Directory structure.

APPENDIX A: Viewing Packets encrypted with IPSec –

Because IPSec encrypts all data beyond the IP header, this can make troubleshooting problems using sniffers difficult.

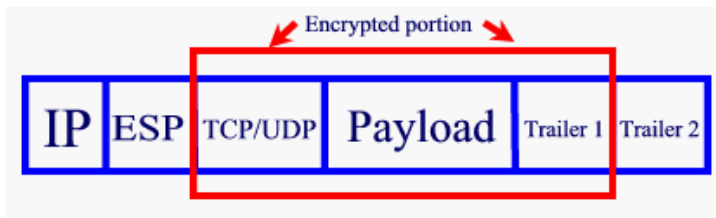


Figure 25 - TCP/IP packet showing encrypted portion

Because even the TCP/UDP portion is encrypted you will see little more than the destination IP address. This is of course by design. If you need to see the data within the ESP packet while sniffing IPSec you can do so at either endpoint using the Windows Network Monitor, as it will automatically convert the encrypted data for you as it is converted for the machine to use. This may not let you place your sniffer in the most desired location however.

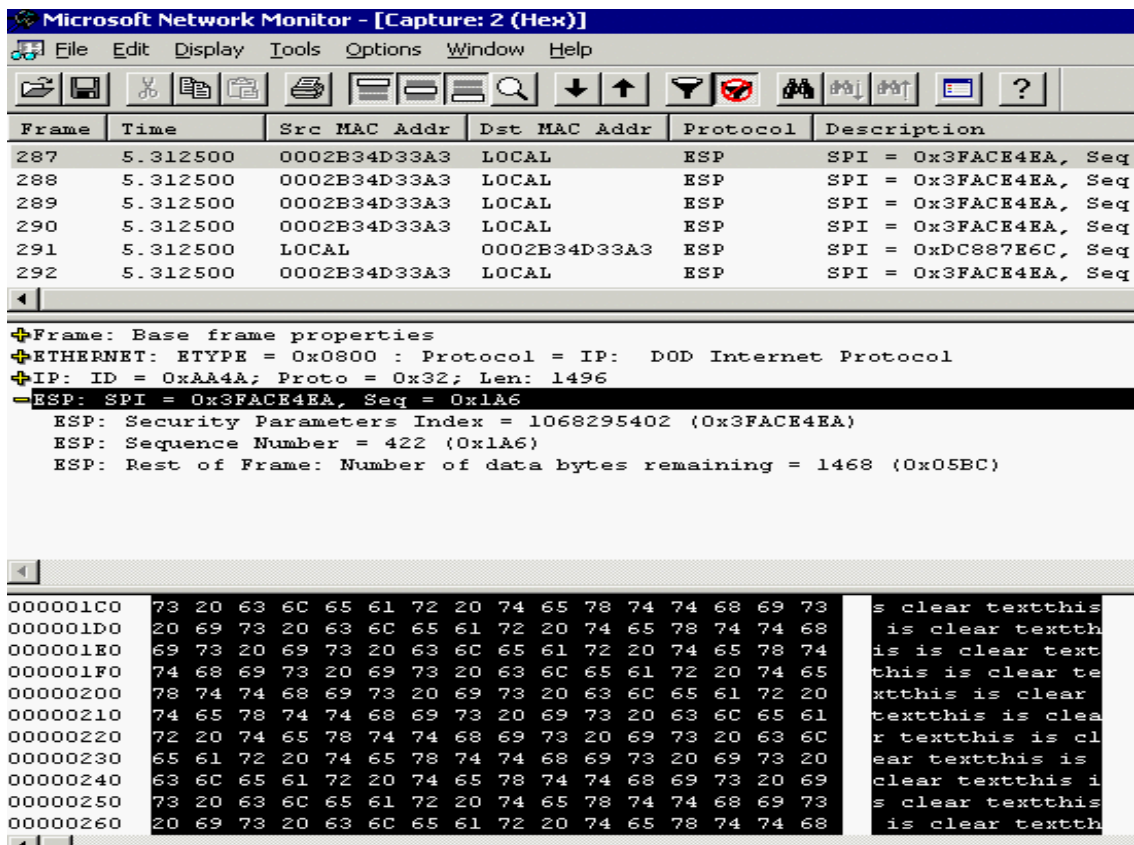


Figure 26 - converted ESP packet at an IPSec endpoint

APPENDIX B: IPSEC enabled NIC's -

Vendors are starting to release IPsec enabled Network Interface Cards. 3COM has separate 168-bit 3DES and 56-bit DES models⁹. Intel has models that will do both 168-bit or 56-bit encryption¹⁰ on the same card. Other Manufacturers are sure to follow suit, as these cards off-load encryption functions from the processor to the NIC. I tested using the Intel Pro 100 /S NIC's and I discovered that at least for these models of Intel cards the offloading of the CPU work happened in both directions and not only outbound as stated in SANS documentation¹¹. However, according to Intel documentation –

- **Double authentication-based** security associations will not be offloaded.
- If you are using an Intel PRO/100 S adapter, note that Windows 2000 doesn't offload **fragmented** IP traffic to the adapter.
- Tunnel mode processing is not off-loaded to the encryption co-

⁹ 3COM part numbers - 3CR990SVR95 and 3CR990SVR97

¹⁰ Intel Part numbers PILA8470C3 and PILA8460C3

¹¹ SANS institute Documentation 5.7 Windows 2000 IPSEC, Rras, and VPN's - page 84

¹² Intel on-line help files for INTEL PRO100 /S NICs

processor.¹²

So be aware that an improperly set up network or testing on a heavily used network may produce inaccurate results. Also various IPsec card manufacturers may handle the encryption offloading in a different manner than the Intel Cards tested here. Try a few different types of cards if possible.

Looking at traffic flow from a large file transfer (the W2K SP2 file to be exact). You can see the effects on bandwidth and CPU usage without IPsec enabled.

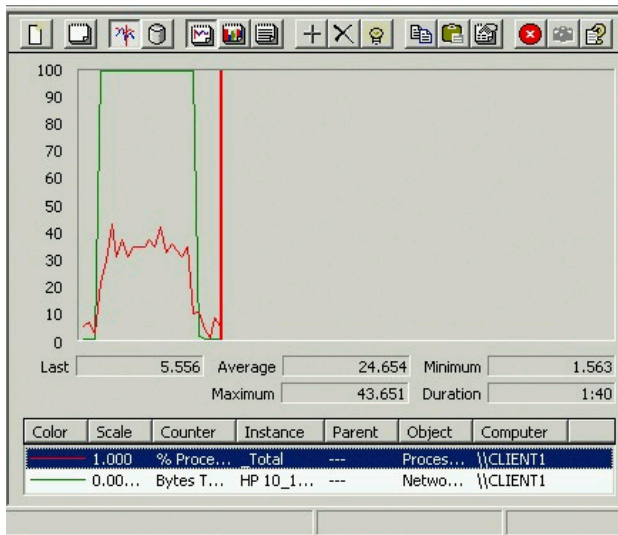


Figure 27 - File transfer with no encryption - Red line=CPU Green line = Bytes/sec

Adding IPsec to the transfer not only increases CPU, but also reduces total output efficiency. Also notice the length of time it took to transfer the same file has increased dramatically. I expected to see a larger CPU crunch on this particular test, but rather throughput was reduced as the computer struggled to keep up on this old Pentium Pro system. The card used was an Intel PRO 100 non-IPsec NIC.

¹² Intel on-line help files for INTEL PRO100 /S NICs

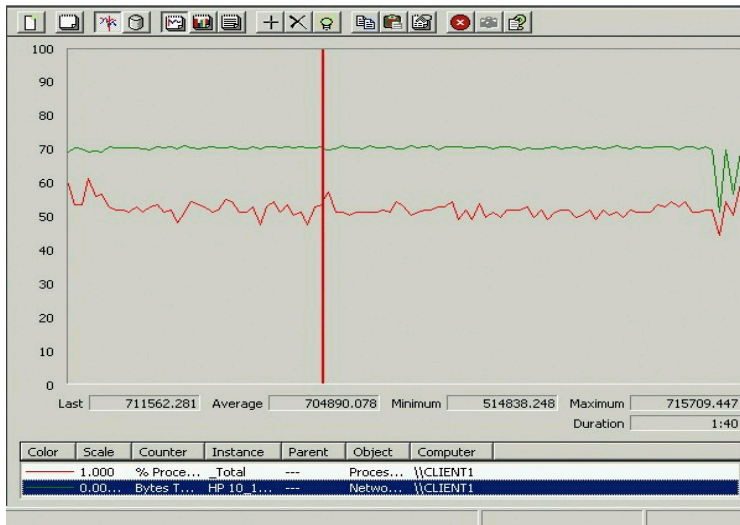


Figure 28 - File transfer with encryption enabled - Red line=CPU Green line = Bytes/sec

Adding an Intel PRO 100 /S NIC with encryption enabled brought the transfer back to near original stats.

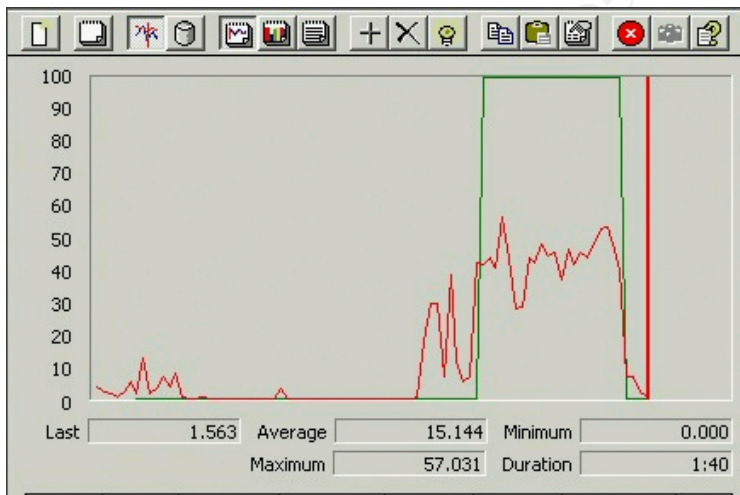


Figure 29 - File transfer with encryption on an IPsec NIC - Red line=CPU Green line = Bytes/sec

All NICs are not the same –

While the previous results give a good general idea of the effects of IPsec on computer resources I found in testing several different machines and non-IPsec NICs that results may vary widely. It is not uncommon to find CPU resources at

90% – 100% without hardware acceleration. Also beware that the Intel S series cards are **PCI version 2.2 compliant only**. I found several older machines that would not work with these cards, and in some cases would not even boot. Be sure to test a few of the cards you choose before making an order for wide distribution.

The best example hardware acceleration benefits I found was when testing a 333Mhz laptop. The non-IPSec NIC was a Xircom Fast Ethernet/Modem combo. This was tested against the Intel Mobil /S IPSec NIC.

Looking at the laptop CPU and bytes per second with the Xircom card and no encryption revealed the computer was working quite hard just to use do a simple file transfer.

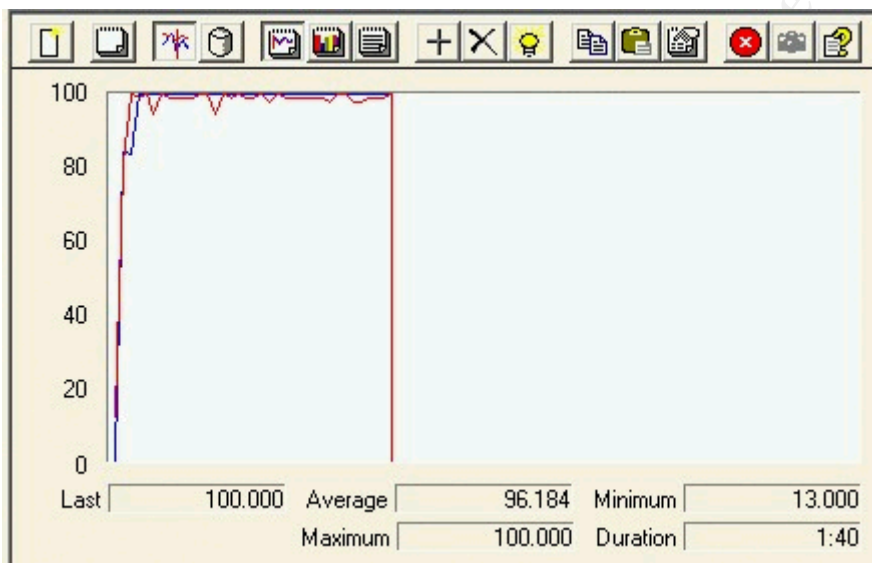


Figure 30 - Laptop file transfer without encryption -- Red line=CPU Green line = Bytes/sec

Adding Encryption really slowed things down on the machine and throughput dropped to about 55% of maximum.



Figure 31 - Laptop file transfer with IPsec enabled - Red line=CPU Green line = Bytes/sec

What was surprising was when the Intel Mobil /S IPsec NIC was added and encryption enabled, performance actually improved drastically. Transfer time was cut to about 1/10th of the original transfer without encryption on the Xircom NIC. Truly a portion of the performance boost here is simply a better driver and NIC all-around.



Figure 32 - Laptop file transfer with IPsec and the INTEL NIC - Red line=CPU Green line = Bytes/sec

Appendix C: IPsec and Packet size –

Testing the size of the packets that were transferred with and without IPSec enabled also produced some surprising results. Without encryption the data transfer of the SP2 file used 74,448 packets to move the file. With IPSec encryption the same transfer used 76,190 packets. So this type of encryption, while increasing the work the computer or Intel hardware accelerator card must do - does not seem to have a great impact on network bandwidth usage. A large increase in packet sizes would mean extra work for configuring network bandwidth resources when planning an IPSec implementation. However it seems the results are negligible enough to fit within the headroom of all but the most burdened networks.

References

Cisco Systems - <http://www.cisco.com>
http://www.cisco.com/warp/public/cc/techno/protocol/ipsecur/ipsec/tech/ipsec_wp.htm

IETF – www.ietf.org
<http://www.ietf.org/html.charters/ipsec-charter.html>

Baltimore Securities – www.baltimore.com Contact:: Jeff Lewis
<http://www.baltimore.com/unicert/unicert/whatsnew.html>

Microsoft Windows 2000 Server Resource Kit, Microsoft Press ISBN – 1-57231-805-8

- Windows 2000 Server Distributed Systems Guide
- Windows 2000 Server Deployment Planning Guide
- Windows 2000 Server Internetworking Guide
- Windows 2000 Server TCP/IP Core Networking Guide

Microsoft TechNet – Articles Q253169, Q232817, Q253498

Also available at -
<http://search.support.microsoft.com/kb/c.asp?fr=0&SD=GN&LN=EN-US>

Windows 2000 Server online Help

Windows 2000: PKI, SANS Institute Document 5.6 version 4.0.1 - Author Jason Fossen

Windows 2000: IPSec, RRAS, and VPN, SANS Institute Documentation 5.7
Version 1.0.1 – Author Jason Fossen

Intel PRO100 S adapter CD Documentation and Help Files

Other References -

Digital Certificates, Addison-Wesley publisher ISBN 0-201-30980-7

Understanding Digital Signatures, CommerceNet Press ISBN 0-07-012554-6

Tuning and Sizing Windows 2000 Prentice Hall Press ISBN 0-13-089105-3