The Cryptographic Overhead of IPSec Protocol Suite During The Packet Exchange Process

I. INTRODUCTION TO IPSec

IPSec provides security to the Internet Protocol Layer. It does this by giving us the choices to use any encryption-decryption algorithm along with the mandatory security protocols.. IPSec uses some different important protocols such as AH (Authentication Header), ESP (Encapsulating Security Protocol), ISAKMP (Internet Security Association and Key Protocol) and IKE (Internet key exchange). Each has their own responsibility and functionality. To operate all this functionality, there are two basic modes such as: Transport Mode & Tunnel Mode.

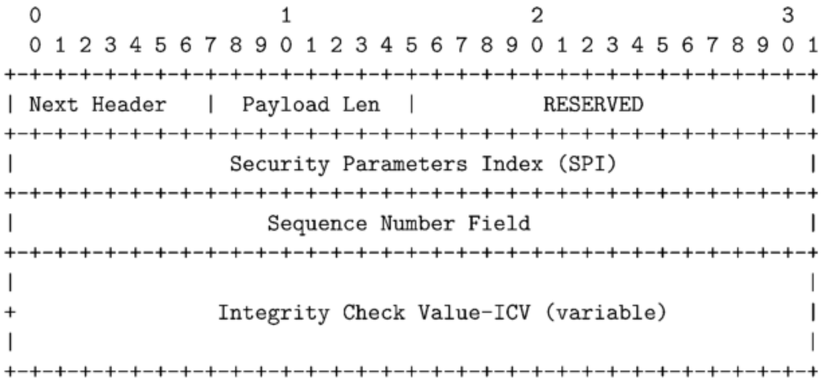
II. IMPLEMENTATION OF IPSEC

The introduction part shows the essential cryptographic design protocols in IPSec. The essential main 3 protocols are as follows :

1. AH -> Authentical Header
2. ESP -> Encapsulating Security Protocol
3. IKEv2 -> Internet Key Exchange v2
4. ISAKMP -> Internet Security Association & Key Management Protocol

Authentication Header

AH provides payload integrity protection as well as data origin authentication. The other important which is provided by AH is anti-relay service. The AH protocol uses the insertion of bit sequence to add the cryptographic protection. It adds AH into the IP packets before it transmit to the end.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Header   |  Payload Len  |          RESERVED             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Security Parameters Index (SPI)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Sequence Number Field                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                Integrity Check Value-ICV (variable)           |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

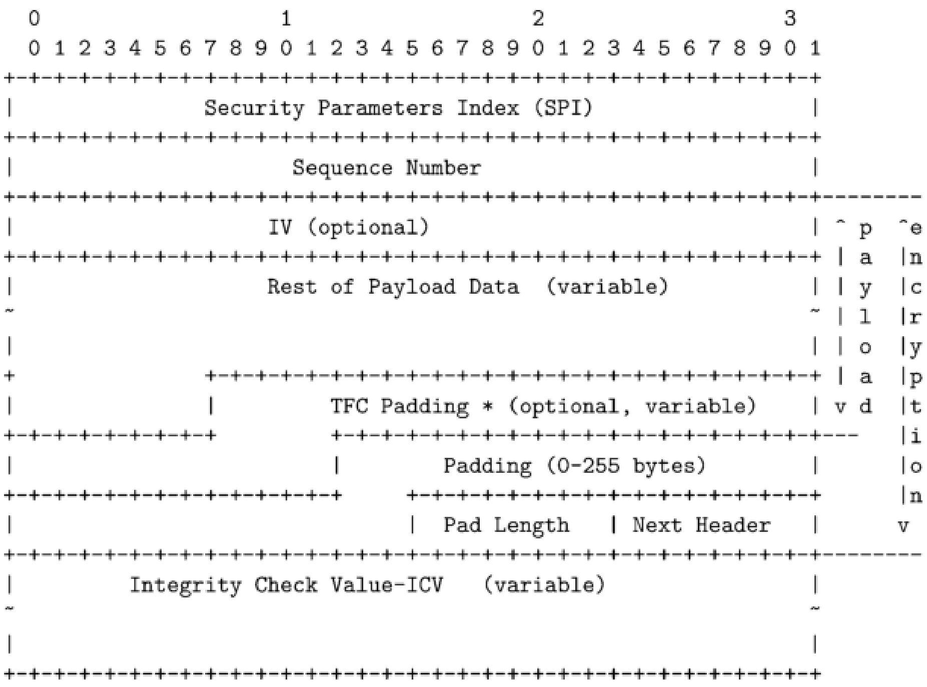
Fig (a) : Authentication Architecture

Generally AH contains the MAC value and it is depended upon the particular MAC algorithm used in it. AH must be in a multiple of 32 bits lengths which is used for IPV4 and it has to be in a multiplication of 64 bit length for IPV6. Below table shows the mandatory MAC algorithms being be used for AH described in RFC 4305

Algorithm	Requirement	Key Size (Bits)	Output (Bits)	RFC Reference
HMAC-SHA1-96	MUST	160	96	RFC 2404
AES-XCBC-MAC-96	SHOULD+	128	96	RFC 3566
HMAC-MD5-96	MAY	128	96	RFC 2403

Encapsulating Security Protocol

This protocol is cryptographic transformation. It gives integrity as well as confidentiality in one package, but the primary purpose of this protocol is to provide confidentiality. The ESP header is having a sequence number field and SPI. The below figure illustrates the format of the ESP protocol mentioned in RFC 4303.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Security Parameters Index (SPI)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Sequence Number                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--------
|                    IV (optional)                              | ^ p  ^e
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | a  |n
|                    Rest of Payload Data  (variable)           | | y  |c
~                                                               ~ | l  |r
|                                                               | | o  |y
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | a  |p
|               |         TFC Padding * (optional, variable)    | v d  |t
+-+-+-+-+-+-+-+-+         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+---     |i
|                         |        Padding (0-255 bytes)        |      |o
+-+-+-+-+-+-+-+-+-+-+-+-+-+     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+      |n
|                               |  Pad Length   | Next Header   |      v
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--------
|         Integrity Check Value-ICV   (variable)                |
~                                                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig (b) : ESP Header Architecture

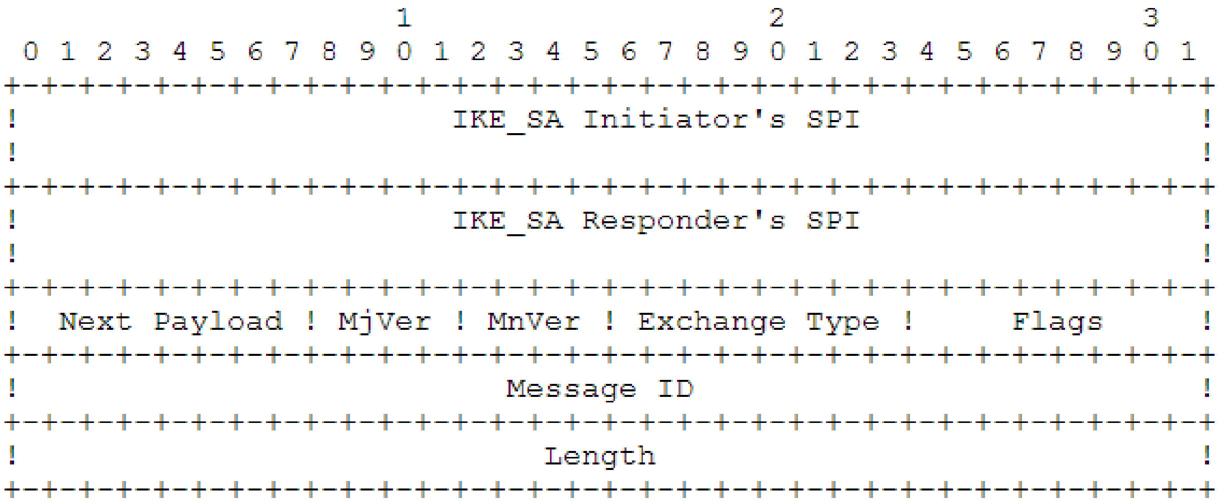
There are some mandatory encryption algorithms which have to be used for ESP which is specified in RFC 4305, in which 3DES, AEC-CBC, DES-CBC and AES-CTR is used.

Algorithm	Requirement	Key Size (Bits)	Block Size (Bits)	RFC Reference
NULL	MUST	0	N/A	RFC 2410
Triple DES-CBC	MUST-	192	64	RFC 2451
AES-CBC	SHOULD+	128	128	RFC 3602
AES-CTR	SHOULD	128	N/A	RFC 3686
DES-CBC	SHOULD NOT	56	64	RFC 2405

ESP is optional, therefore there is a null encryption which has to be implemented if required. DES CBC is used for general purpose and public demonstration where 3DES is widely used algorithm now a days due to having its longer key length and bigger block size. Thus all encryption algorithms are used in a different manner as per their need.

Internet Key Exchange

The main role of IKE is exchanging messages between the two ends. The best way to learn IKEv2 is to compare it with IKEv1.The essential features of IKEv2 is identity hiding, Negotiation of cryptographic function, flexibility and the variety of securities. There are mainly 2 phases in IKEv2 the first phase is called IKE-SA. Once this phase is initiated, it is used it is used to send the messages between 2 peers. Below figure shows the architecture of IKE phase.



```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                       IKE_SA Initiator's SPI                  !
!                                                               !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                       IKE_SA Responder's SPI                  !
!                                                               !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!  Next Payload ! MjVer ! MnVer ! Exchange Type !     Flags     !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                          Message ID                           !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                            Length                             !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig (c) : IKE Phase Architecture

Generally IKE protocol uses UDP packets on port 500. On an average it requires 4 to 6 packets in order to create SA at the both ends. After this SA creation key material will be provided to the IPsec stack.

Internet Security Association And Key Management Protocol

It is responsible for defining all procedures at both ends. It also plays a vital role in authenticating procedures. It generates SAs and it also manges key integration. ISAKMP has an ability to prevent Denial of Service Attacks. It defines the packet format for the establishment and negotiation of security. It also defines the payload for key generation which gives a constant framework for exchanging authenticated data as well as key. ISAKMP and key exchange protocols both are different things.

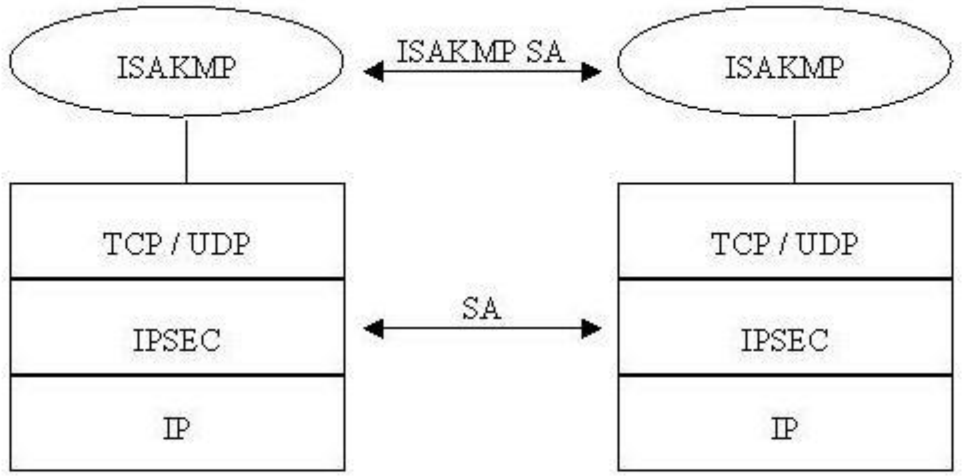


Fig (d) : ISAKMP Architecture and Use

Generally it is implemented on a transport level protocol which uses UDP protocol on 500th port number.

III. IPSEC ALGORITHM KEY LIMITATIONS

IPSEC limitation can be expressed in terms of lack of expressive power in IPSEC policy control. Also there can be lack of application control on the different different polices.
The biggest challenge in IPSEC is the deployment. Also authorization handling is a big challenge in the IPSEC mechanism because it needs security as well as application information.
As we have seen that cryptographic algorithms are used in a different manner and need, at a same time there are a couple of limitations in cryptography algorithms. Some of the major algorithm scenario and their limitations are shown below:

Talking about DES, it uses 64 bits of key size. In this DES 8 bits of all 64 are used for the odd parity. This is the cause of less effectiveness of this algorithm also DES have compromised on many occasions. There are some specially crafted hardwares which can crack DES in some few hours. Due to this researcher are motivated to invent more secured DES. Thus the 3DES algorithm born which does the triple repetition of the DES encryption. It can be said that 3DES is able to use a larger key length of 112 bits. It is quite obvious that 3DES runs 3 times slower than normal DES due to a large number of key size repetition processes.

MD5 and SHA1 are both single way hash functions. 512 blocks of bits are used to create 128 and 160 bit hash values. The limitation of them is they cannot be used directly as MAC algorithm due to not having a secret key. This is the reason that why they are being used in conjunction with key hashing technique.

RSA algorithm requires modular exponentiations which lead it towards its main 2 limitations such as large memory space and the more complexity for computational performance.

IV. IPSEC OVERHEAD ANALYSIS

To measure the IPsec overhead, firstly we need to measure the CPU cycle processing. This analysis can be done on essential security algorithms such as DES, 3DES, AES, HMAC-MD5 and HMAC-SHA1. There is a processing overhead as we all know in IPsec, but apart from it there is one more extra overhead which is called space overhead. It is generated by the increased size of packets transmitted on both ends.

If the application is lighter weighted such as DES, HMAC-MD5 and HMAC-SHA1, then it does not in decrease more system throughput, which has a null impact on the total delay of the process. Here the MS processing rate is 100 MIPS or around it. On the other hand 3DEC and AES are more complex which uses bigger size of key length such as 192 and 256 bits. No doubt that it provides resistance against the targeted attacks but the high volume of processes decrease the throughput of the system. Here the MS processing rate is more than 300 MIPS. AES, DES and 3DES generate more strain on the system.

Overhead is not only depended upon the encryption algorithms but it also depends upon the size of the data which you are sending. Here in my demonstration I have rapidly increased the packet size to send from source to destination and we can clearly see that, as the number of packets are being increased the time taken to send each packet is also getting increased. We can also able to determine the fluctuation in time to send each packet.

```
C:\Documents and Settings\Administrator>ping -l 16000 10.10.10.11

Pinging 10.10.10.11 with 16000 bytes of data:

Reply from 10.10.10.11: bytes=16000 time=4ms TTL=128
Reply from 10.10.10.11: bytes=16000 time=6ms TTL=128
Reply from 10.10.10.11: bytes=16000 time=7ms TTL=128
Reply from 10.10.10.11: bytes=16000 time=6ms TTL=128
```

```
Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 7ms, Average = 5ms

C:\Documents and Settings\Administrator>ping -l 32000 10.10.10.11

Pinging 10.10.10.11 with 32000 bytes of data:

Reply from 10.10.10.11: bytes=32000 time=10ms TTL=128
Reply from 10.10.10.11: bytes=32000 time=14ms TTL=128
Reply from 10.10.10.11: bytes=32000 time=9ms TTL=128
Reply from 10.10.10.11: bytes=32000 time=13ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 14ms, Average = 11ms

C:\Documents and Settings\Administrator>ping -l 64000 10.10.10.11


Pinging 10.10.10.11 with 64000 bytes of data:
Reply from 10.10.10.11: bytes=64000 time=18ms TTL=128
Reply from 10.10.10.11: bytes=64000 time=28ms TTL=128
Reply from 10.10.10.11: bytes=64000 time=27ms TTL=128
Reply from 10.10.10.11: bytes=64000 time=16ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 28ms, Average = 22ms
```

Here we can clearly see that as the packet size/buffer size is increasing the time taken to send the packet is also getting increased and there is a fluctuation in timing for each packet to be sent and that causes large average time.

This is just a basic simple analysis of one machine to another machine with some simple encryption and hashing techniques. Researchers of the university of Athens have found how the delay gets increased with the use of different encryption algorithms. The below figure illustrates the results presented by those researchers.

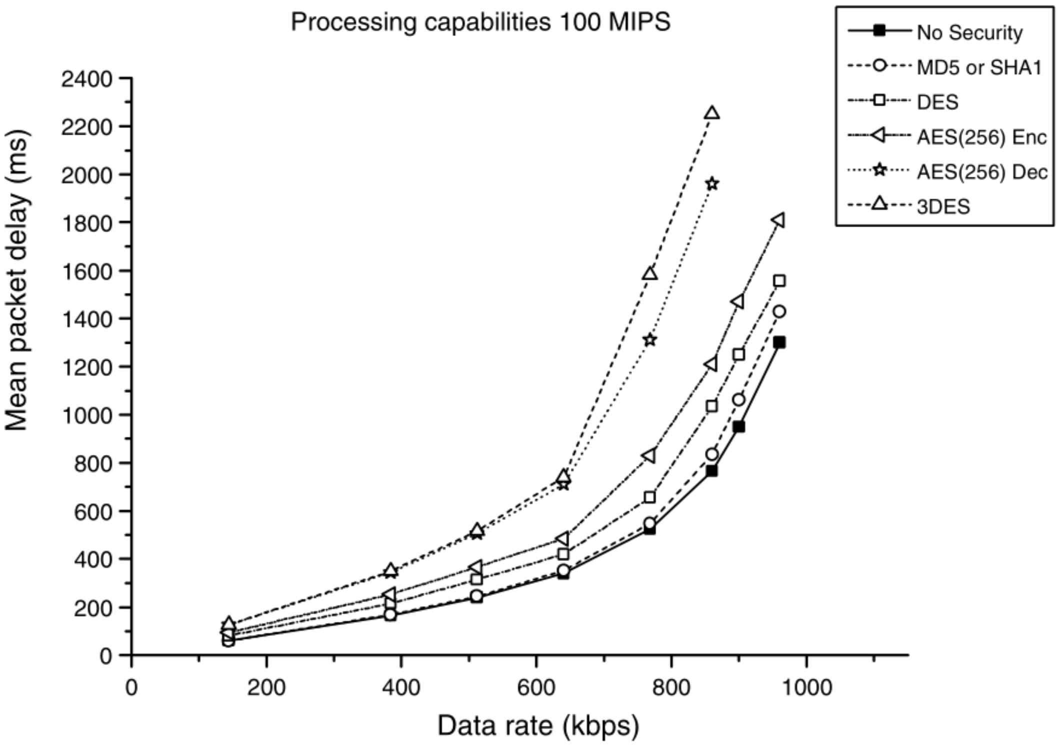


Fig (e) : Total Mean Delay Analysis by Processing 100 MIPS

It is very clear from the graph that DES produces higher delay than other encryption techniques. On the flip side of it, it does not affect the rate of data transfer on the system. We can also see that 3DES and AES are those encryption methods which have a stronger impact on delay taken by packets in transmission. It is very clear from this graph that if the amount of data rate is increased then the total mean daily will be decreased compared to one another.

V. IPSec Key Attacks

To improve the encryption and integrity standard we need to understand the previous IPSec key attacks well in deeper. So that we can secure our IPSec standard in a more efficient way in the future. There are some well known attacks on the IPsec key which are as follows:

- Padding Oracle Attack = Side Channel Attacks
- Chosen Plain Text Attacks = Plain Text Injection Attacks
- Options Based Attacks
- Splicing Attacks

Padding oracle attack is also called as side channel attack. This attack performs padding on messages. These attacks are mostly associated with CBC decryption, which are used in the block cipher. These attacks are widely used in the world for decrypting the cipher text without knowing the key. These attacks are broadly used to crack the CAPTCHA systems.

In Choosing Plain Text Attack, the attacker chooses the arbitrary plain text in order to decrypt the cipher text. This attack has also an ability to revel the secret key of the whole cryptanalysis process. At the time of world war 2, Gardening Machine was used to crack the codes of the Enigma Machines with the help of plain text injection attacks.

In Option Based Attacks, only cipher text is presented against the ESP. The complexity of this attack is more than average 2^{14} trials. The number of trials can vary for 64 bit key length and 128 bit key length.

Splicing attacks are done on ESP. If ESP is used without any authentication then an attacker can intercept anyone’s packet because both the transmission will be on the same SA. Then he might use CBC splicing in order to place a new UDP packet instead of original one. Thus, reinjection of data can be done by using this attack.

VI. Conclusion

Thus IPSec uses a security policy to secure the communication channel as well as the messages. It supports network level end-to-end authentication, payload authentication, confidentiality and integrity. One can use different algorithms and encryption techniques for their desired security.

Block 2 : Configure a system in which IPSec will be deployed to support packet encryption justifying the cryptographic functions used. You should demonstrate a clear overview of the installation and configuration process using the appropriate explanation(s) and screenshots (where applicable). You should use an isolated environment using Virtual machines for your test bed and exhaustively comment upon your selection and configuration criteria. There is no word/page limitation for this block as long as it presents accurately the whole process. To fortify your answer you should present results from your investigation using the appropriate diagrams and Tables. Extra marks will be given for demonstration of understanding and synthesis of existing work in your approach.

Block 2 : IPSec Configuration Demo

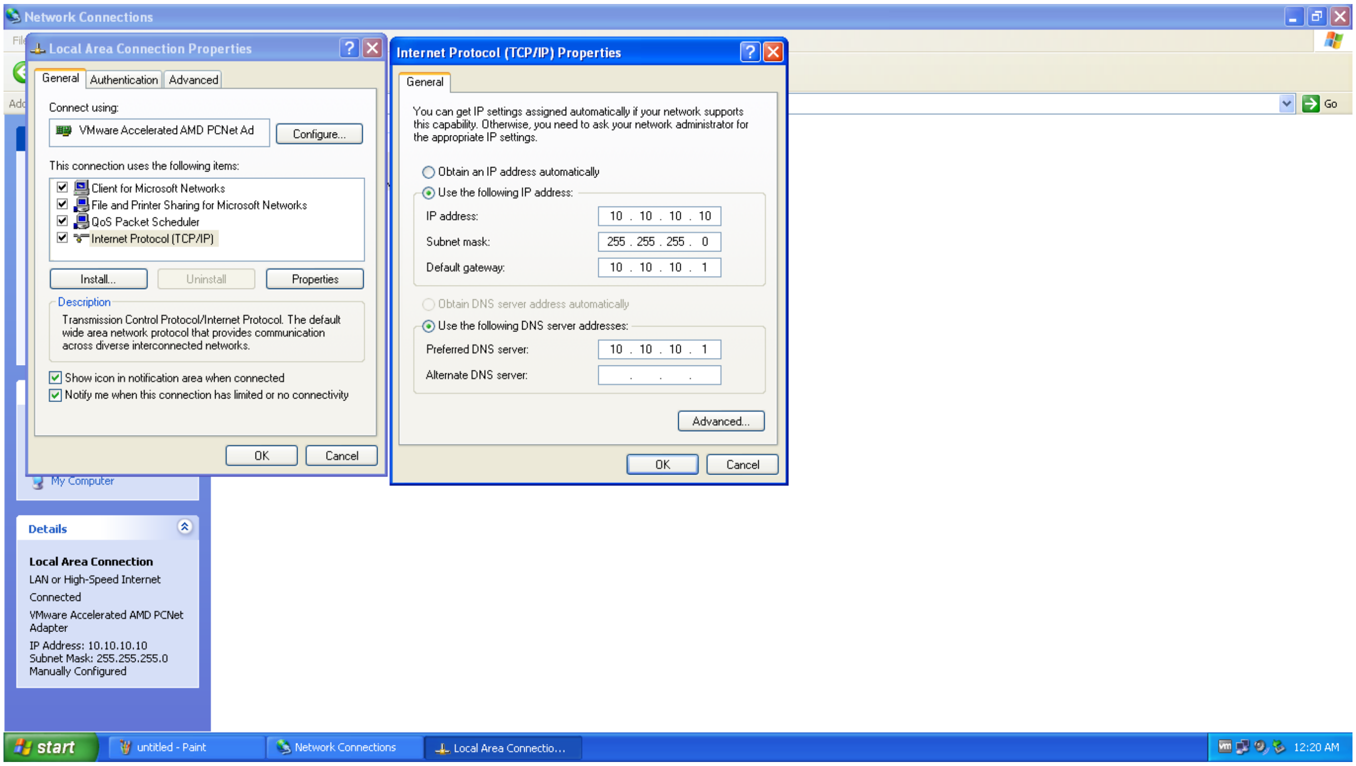
2.1 Installation Process Overview

The main machine is windows 8 in which VMware workstation software is installed. In VMware two windows xp machines are installed which are in LAN segments. One of the windows machine is client and another one is server. I am going to implement IPSec between two XP machines using VMware workstation.

2.2 Server Configuration

These are the simple steps to follow the server configuration.

Step 1 : Assign manual IP address and gateway to the server machine by using TCP / IP options. As shown in the below picture.



Connect using:

VMware Accelerated AMD PCNet Ad

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

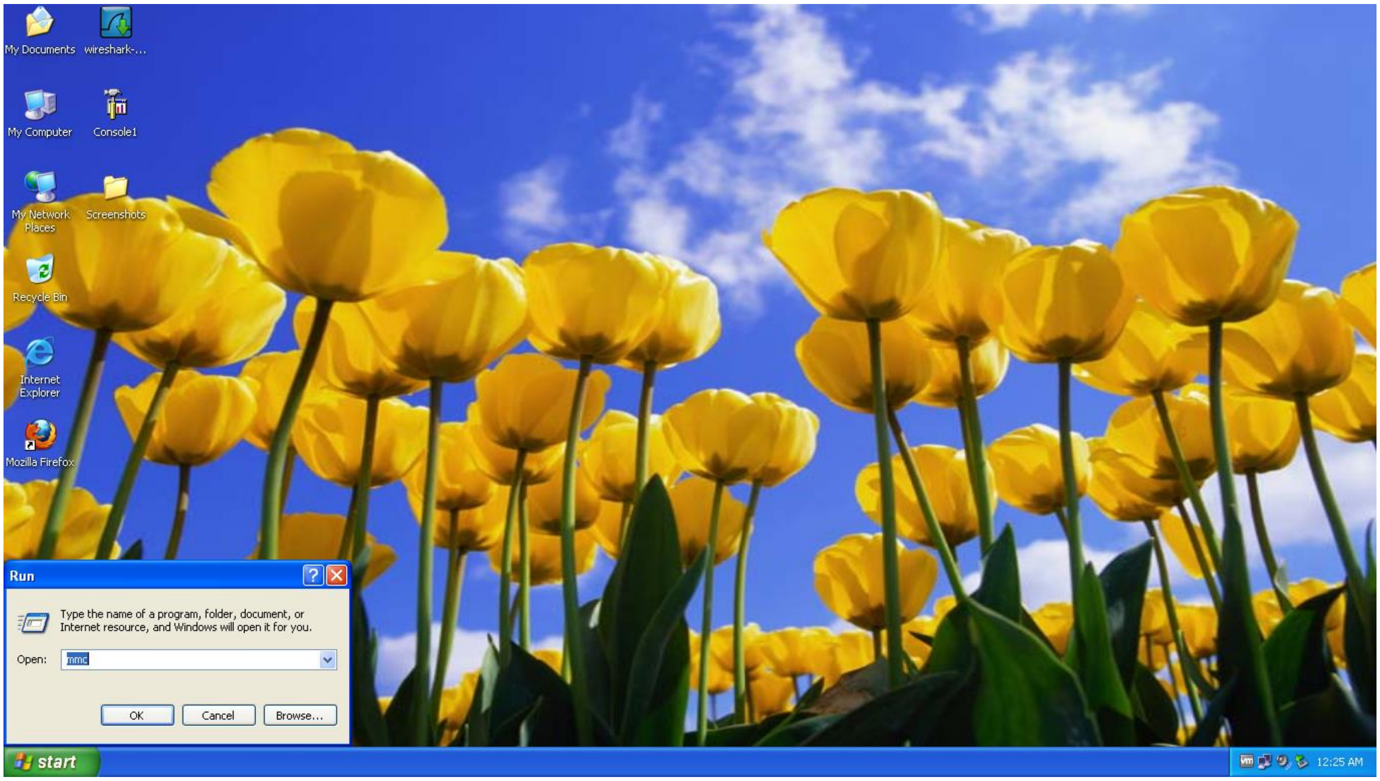
IP address:	10 . 10 . 10 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 10 . 10 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	10 . 10 . 10 . 1
Alternate DNS server:	. . .

Local Area Connection
LAN or High-Speed Internet
Connected
VMware Accelerated AMD PCNet Adapter
IP Address: 10.10.10.10
Subnet Mask: 255.255.255.0
Manually Configured

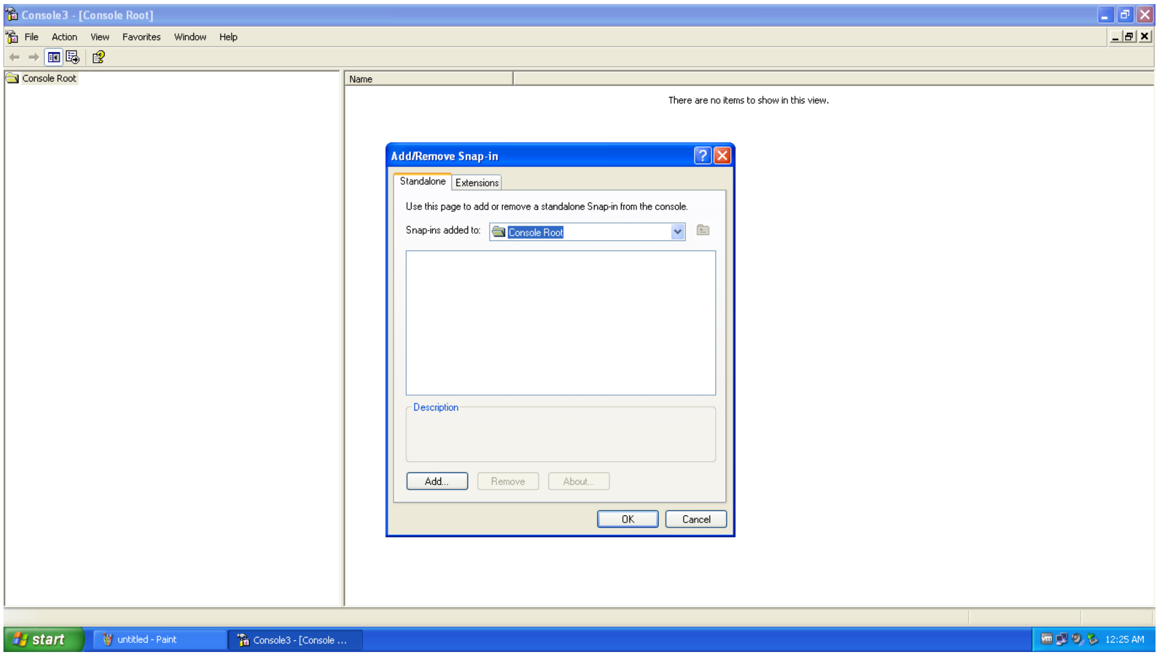
Step 2 : Open Microsoft Management Control by typing *“mmc”* in run.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

Step 3 : After the console gets opened, click on *file* -> *“add/remove snap-in“*. As soon as you add it, you will see the new dialog will come of add/remove snap-in.

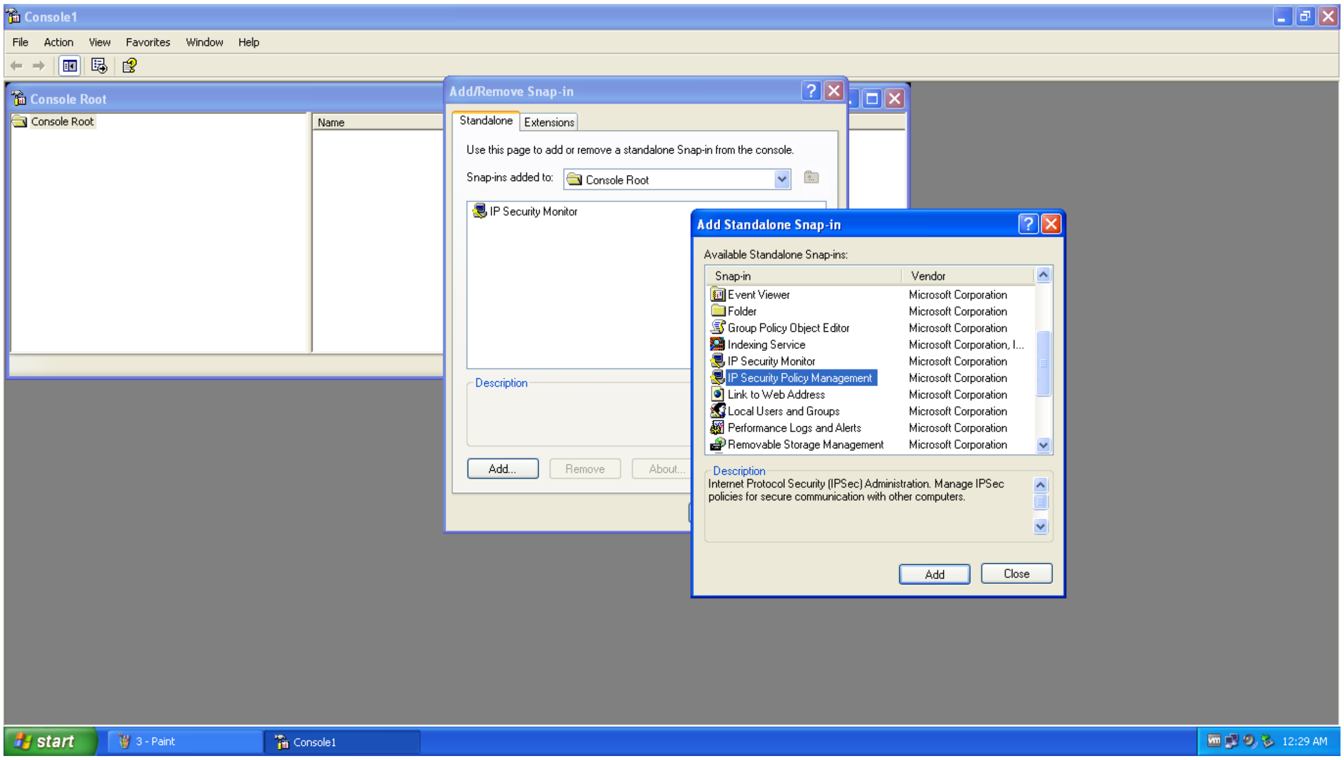


There are no items to show in this view.

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Step 4 : As soon as you see the console you need to click on add to add *“IP Security Monitor”* Snap-in & *“IP Security Policy Management”* Snap-in.



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

IP Security Monitor

Available Standalone Snap-ins:

Snap-in	Vendor
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation
Group Policy Object Editor	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
IP Security Monitor	Microsoft Corporation
IP Security Policy Management	Microsoft Corporation
Link to Web Address	Microsoft Corporation
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
Removable Storage Management	Microsoft Corporation

Description

Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.

Steps 5 : There will be some default policies under IP Security Management such as

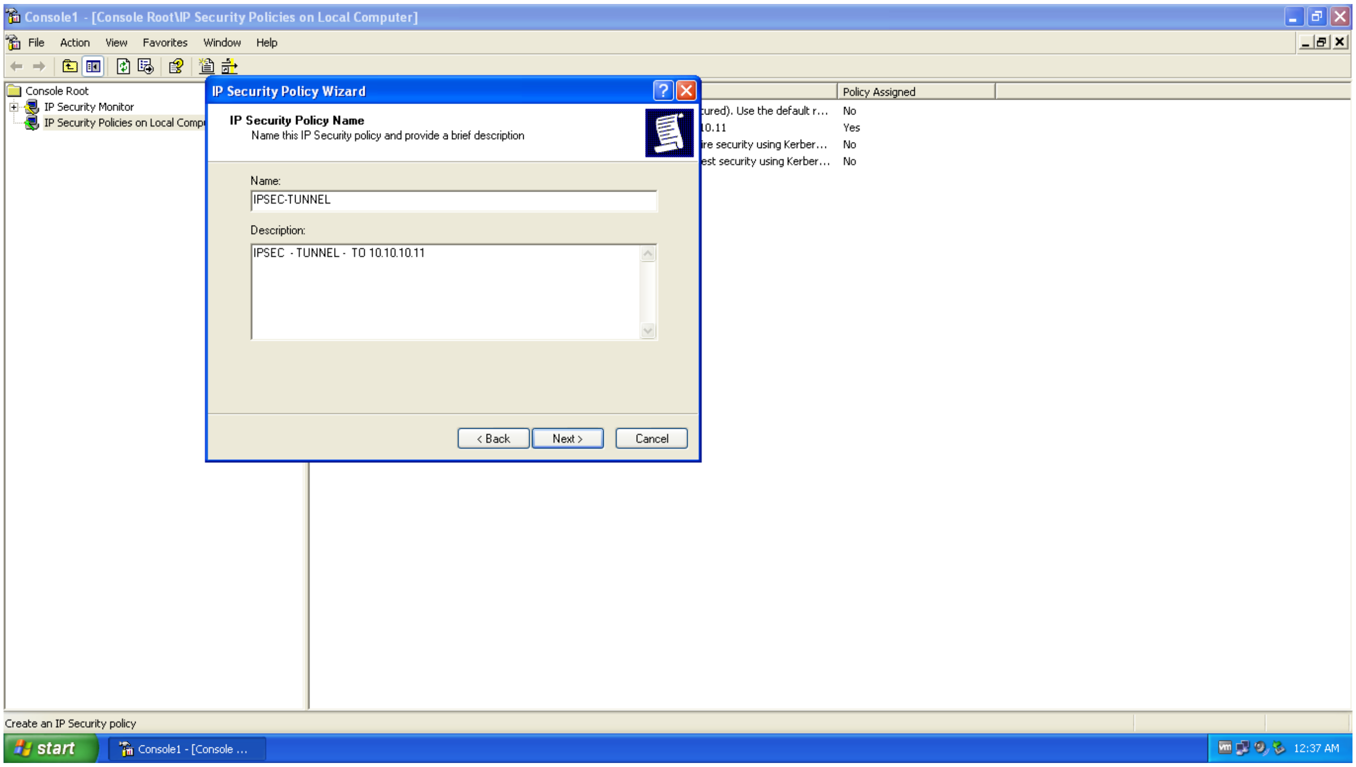
Client (Respond Only)

Secure Server (Require Security)

Server (Require Security)

But we will be adding the new Security policy right clicking on the IP Security Policy Management then click on *“Create IP Security Policy -> Click on Next “* as shown in below picture. Give the name of the policy and the description for the policy.

As I am going to give names such as IPSEC TUNNEL and in the description I will be going to write IPSEC TUNNEL TO 10.10.10.11, which clearly describes that we are running 10.10.10.10 machine and we will be creating an IPSEC TUNNEL to 10.10.10.11 machine.



Console1 - [Console Root\IP Security Policies on Local Computer]

IP Security Policy Wizard

IP Security Policy Name

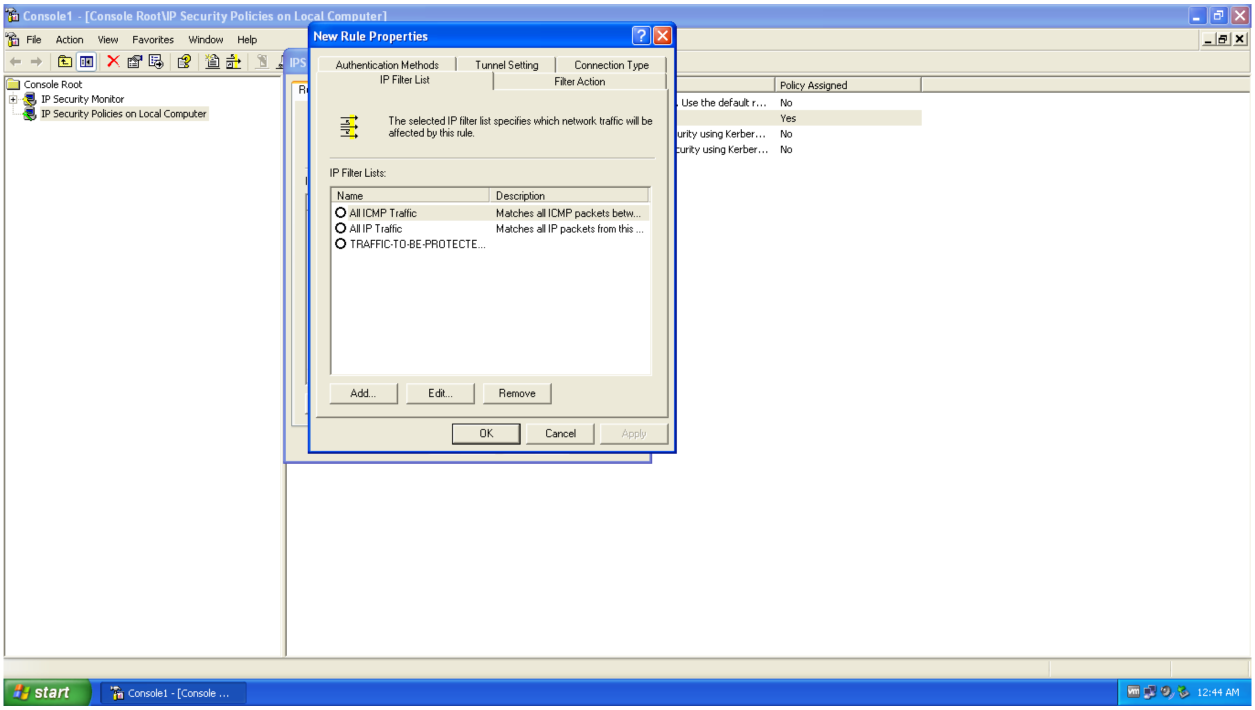
Name this IP Security policy and provide a brief description

Name: IPSEC-TUNNEL

Description: IPSEC - TUNNEL - TO 10.10.10.11

Create an IP Security policy

Steps 6 : Now our policy has been created. Now we will be adding IP Security rules for that. To set the IP Security rules we need to click on *“Add”* button as shown in figure.



New Rule Properties

The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

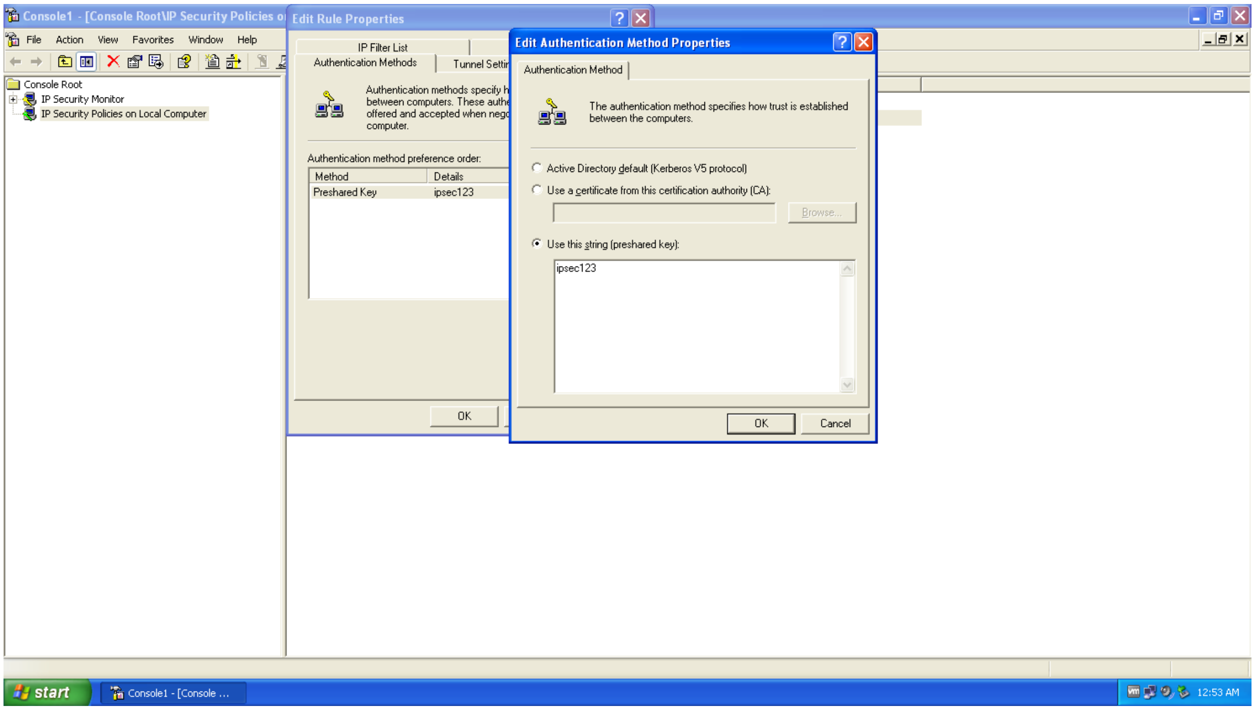
Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ TRAFFIC-TO-BE-PROTECTE...	

	Policy Assigned
. Use the default r...	No
	Yes
urity using Kerber...	No
curity using Kerber...	No

Steps 7 : Now here there are plenty of options which we need to set manually for the security rules of the policy which we created. Options which we need to set are as follows :

a. Authentication Methods
b. IP Filter List
c. Filter Action

Authentication Methods : There will be the default authentication method named *"Kerberos"*. But we will be creating a new authentication method and for that we will put shared key named *"ipsec123"*. This is an essential phase of the whole configuration. This key has to be exactly same for the both client and the server machine. After that you will see two authentication methods in which one will be your created and another will be Kerberos. So you need to click on *"Move up"* button to call your authentication method above than the default one such as shown in figure. In my case there is only one authentication method so I don't need to click on that button for setting the priority.



Authentication methods specify h
between computers. These authe
offered and accepted when nego
computer.

Authentication method preference order:

Method	Details
Preshared Key	ipsec123

Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

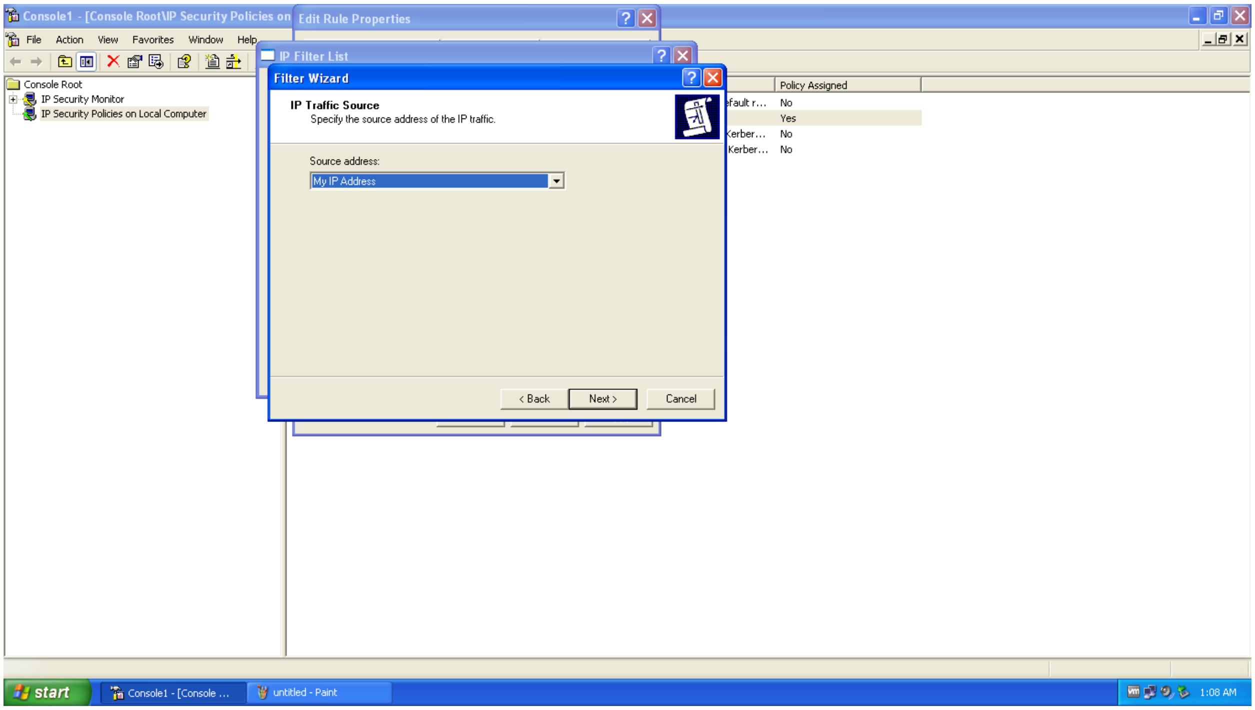
Browse...

● Use this string (preshared key):

ipsec123

OK Cancel

IP Filter List : Then select the IP Filter List tab. Here also there will be two default IP Filter List such as *"ALL IP Traffic"* and "*ALL ICMP Traffic*". We will create our own IP filter list. For that click on *"add"* button and then a new dialog box will come up. You will have to give the name as I gave such as *"TRAFFIC TO BE PROTECTED BY-IPSEC"*. After that click on *"add"* so that IP filter wizard will be open. Click on next. Select *"IP Traffic Source"* select *"My IP Address"*.

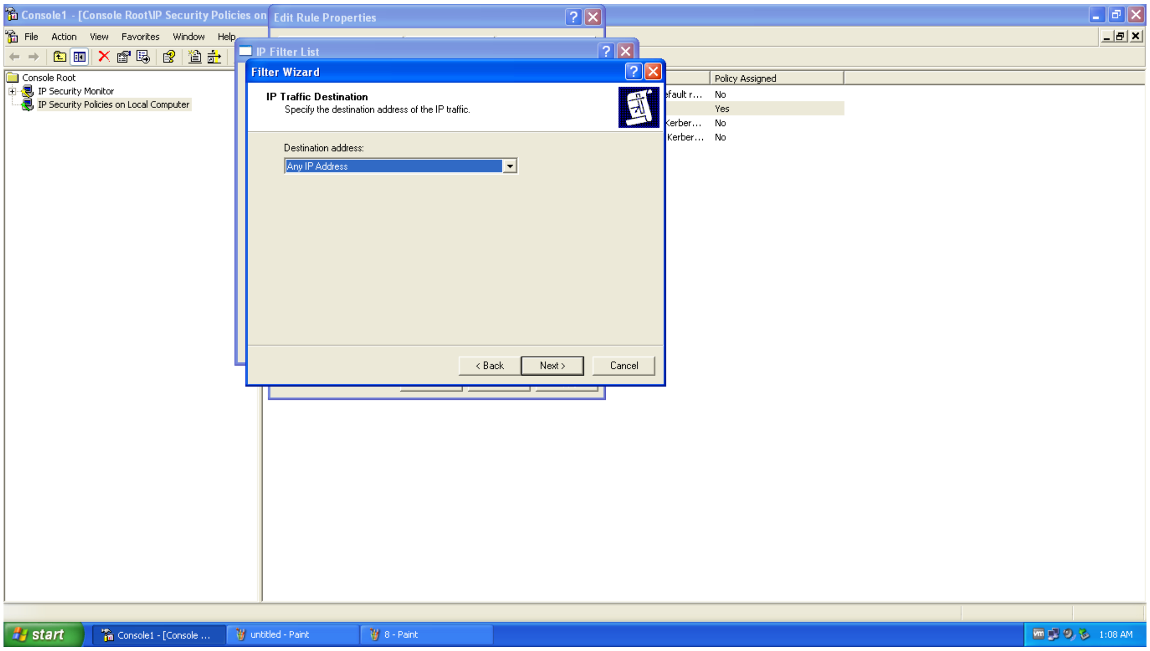


IP Traffic Source

Specify the source address of the IP traffic.

Source address: My IP Address

Now select the destination IP address and in that sekect *“Any IP Address”*.

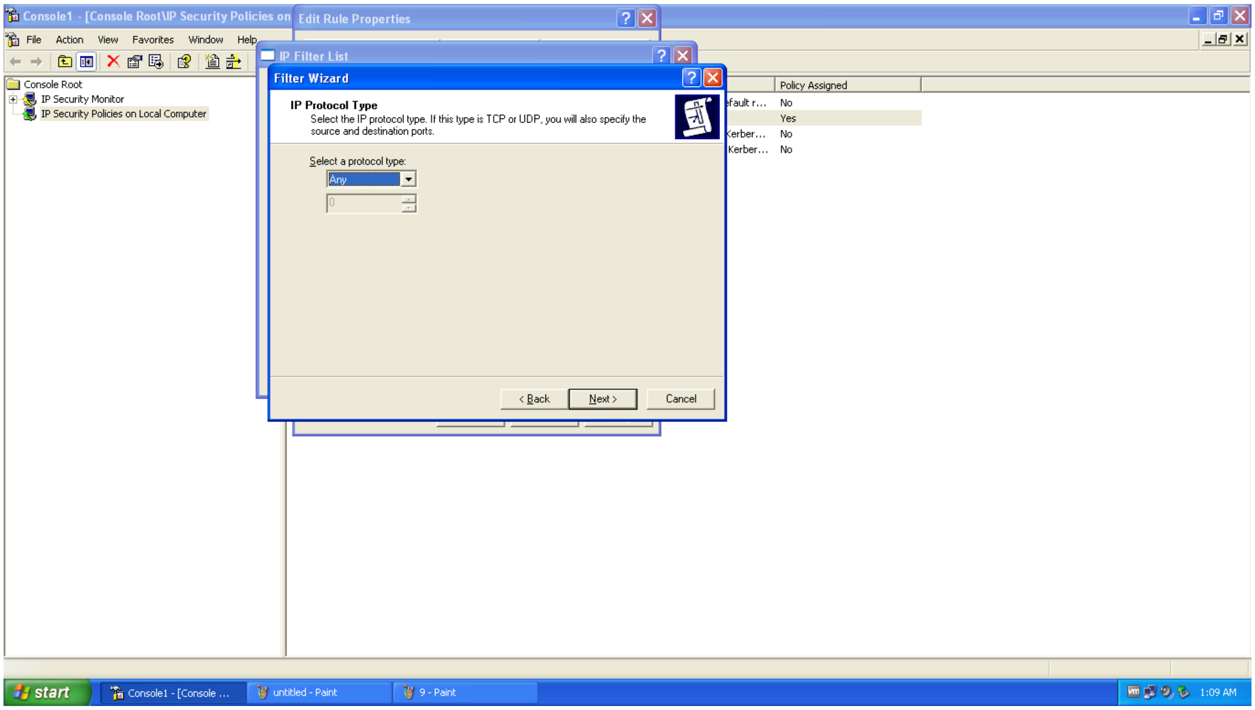


IP Traffic Destination

Specify the destination address of the IP traffic.

Destination address: Any IP Address

After that the last option is protocol. Select the *“Any”* option for protocol selection.

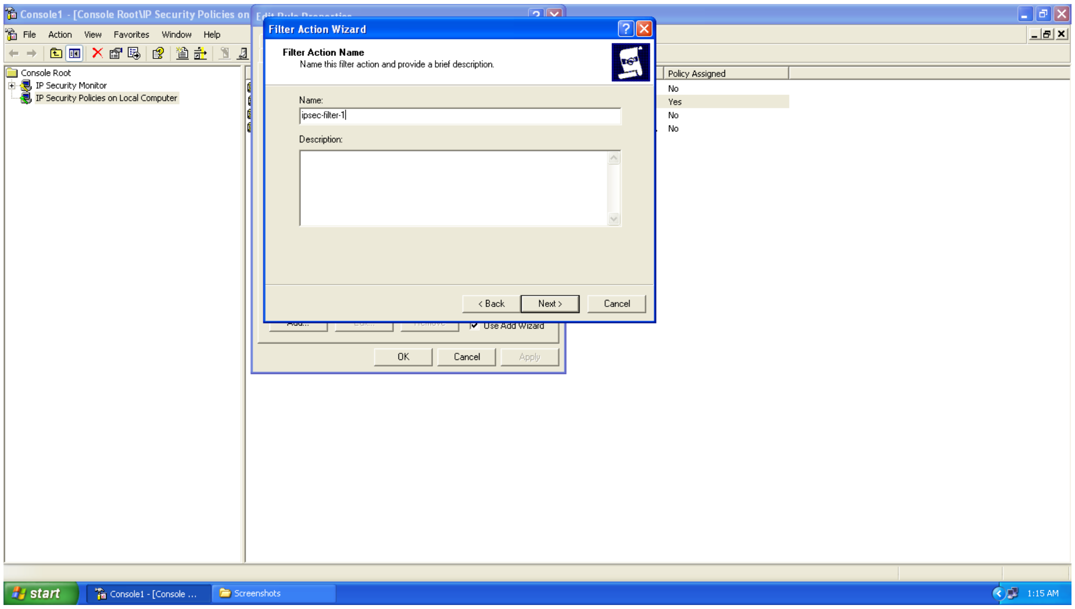


IP Protocol Type

Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.

Select a protocol type: Any

Filter Action : The third and the last option is filter action. In which there will be three by default filter actions but we will be creating our new own filter action. For that we need to click on *"Add"* *.* By clicking on add Filter Action Wizard will come and give the name of the filter action name for that as I have given such as *"ipsec-filter-1"*. Under the security method we must select *"Negotiate Security"* option and the security method will be the *"Encryption and integrity"*, if it is not selected then make it select and apply it.

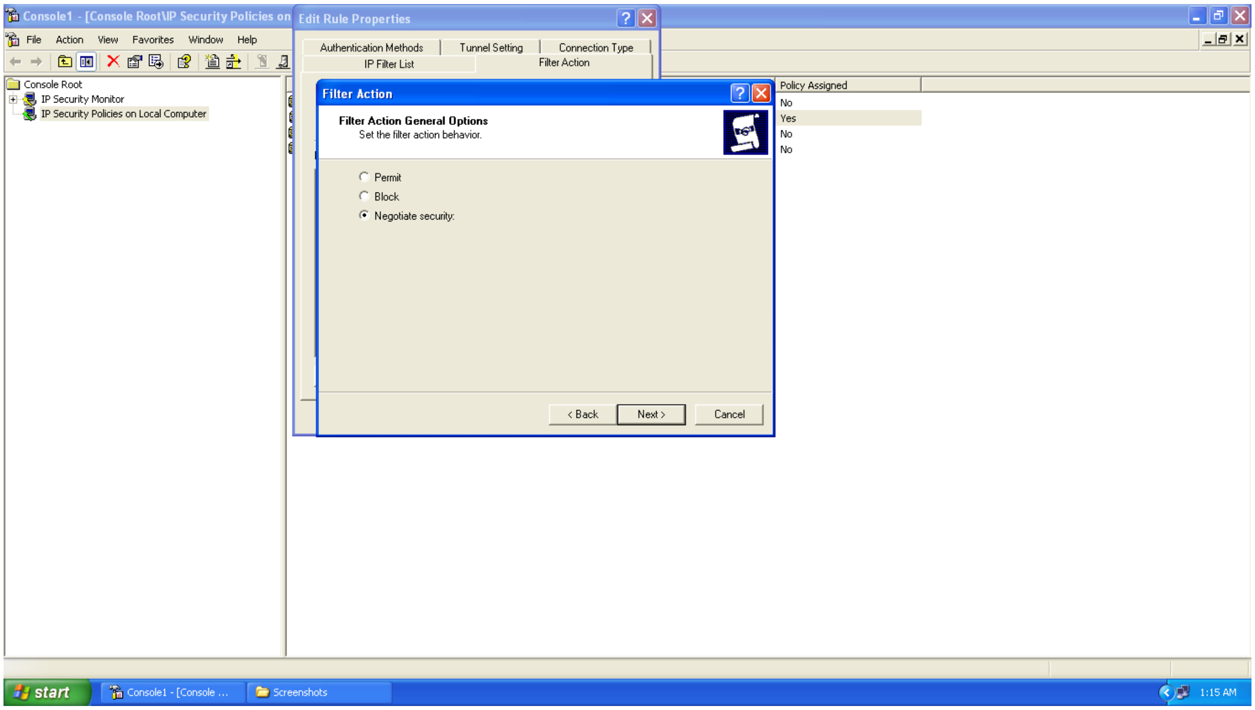


Filter Action Name

Name this filter action and provide a brief description.

Name: ipsec-filter-1

Description:

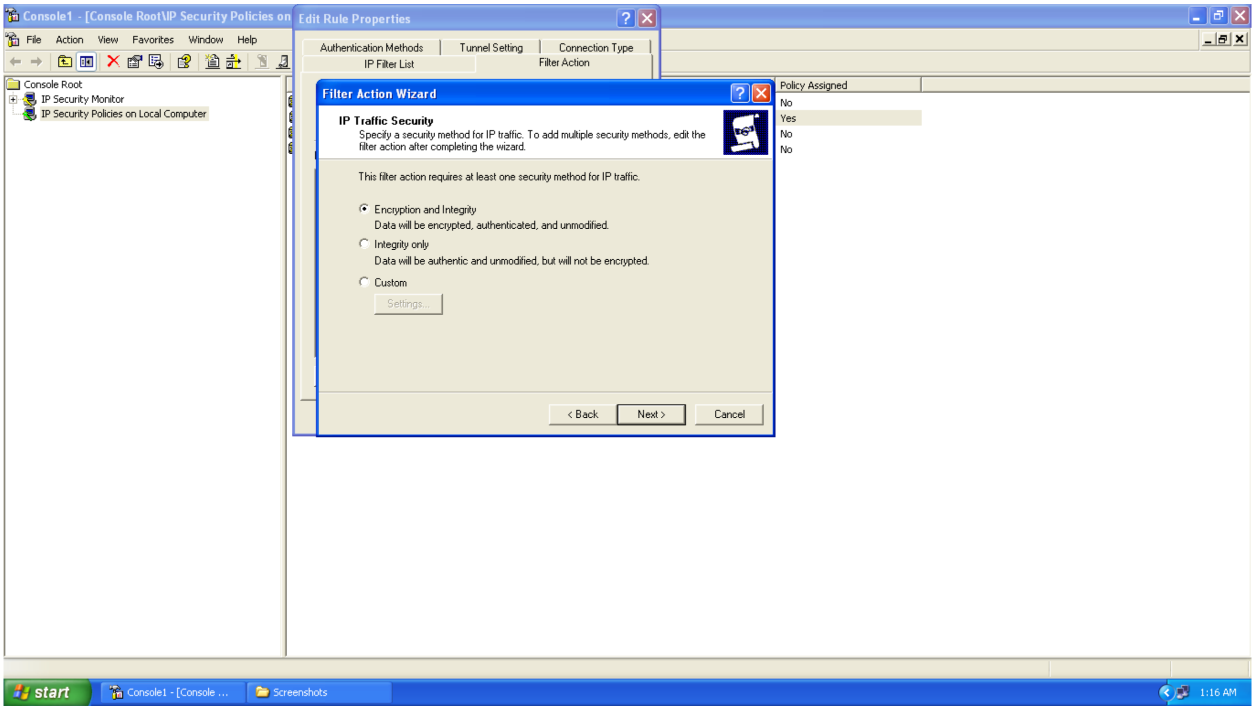


Filter Action

Filter Action General Options

Set the filter action behavior.

○ Permit
○ Block
● Negotiate security:



Filter Action Wizard

IP Traffic Security

Specify a security method for IP traffic. To add multiple security methods, edit the filter action after completing the wizard.

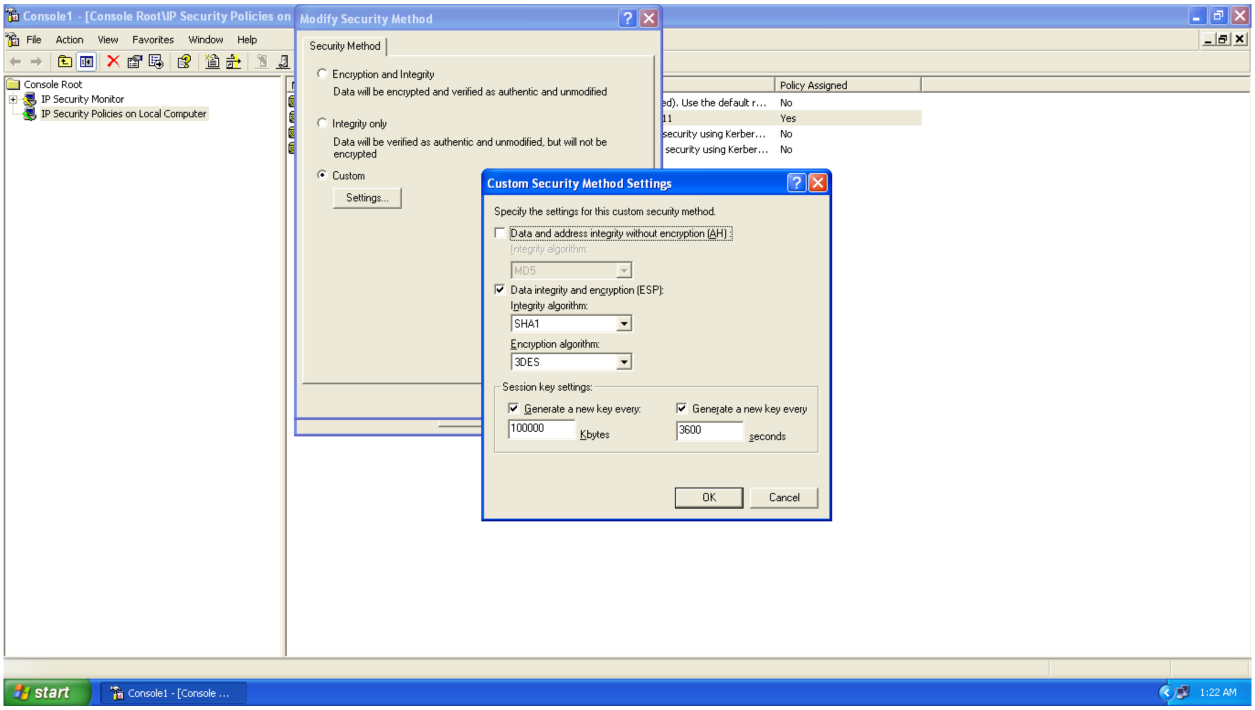
This filter action requires at least one security method for IP traffic.

● Encryption and Integrity
Data will be encrypted, authenticated, and unmodified.

○ Integrity only
Data will be authentic and unmodified, but will not be encrypted.

○ Custom

Here integrity & confidentiality are provided under ESP filter action. For ESP integrity or authenticity SHA1 is used and for confidentiality 3DES is used.


Console1 - [Console Root\IP Security Policies on
File Action View Favorites Window Help
Console Root
IP Security Monitor
IP Security Policies on Local Computer
Policy Assigned
start
Console1 - [Console ...
1:22 AM

Modify Security Method

Security Method

○ Encryption and Integrity
Data will be encrypted and verified as authentic and unmodified

○ Integrity only
Data will be verified as authentic and unmodified, but will not be encrypted

● Custom
Settings...

Custom Security Method Settings

Specify the settings for this custom security method.

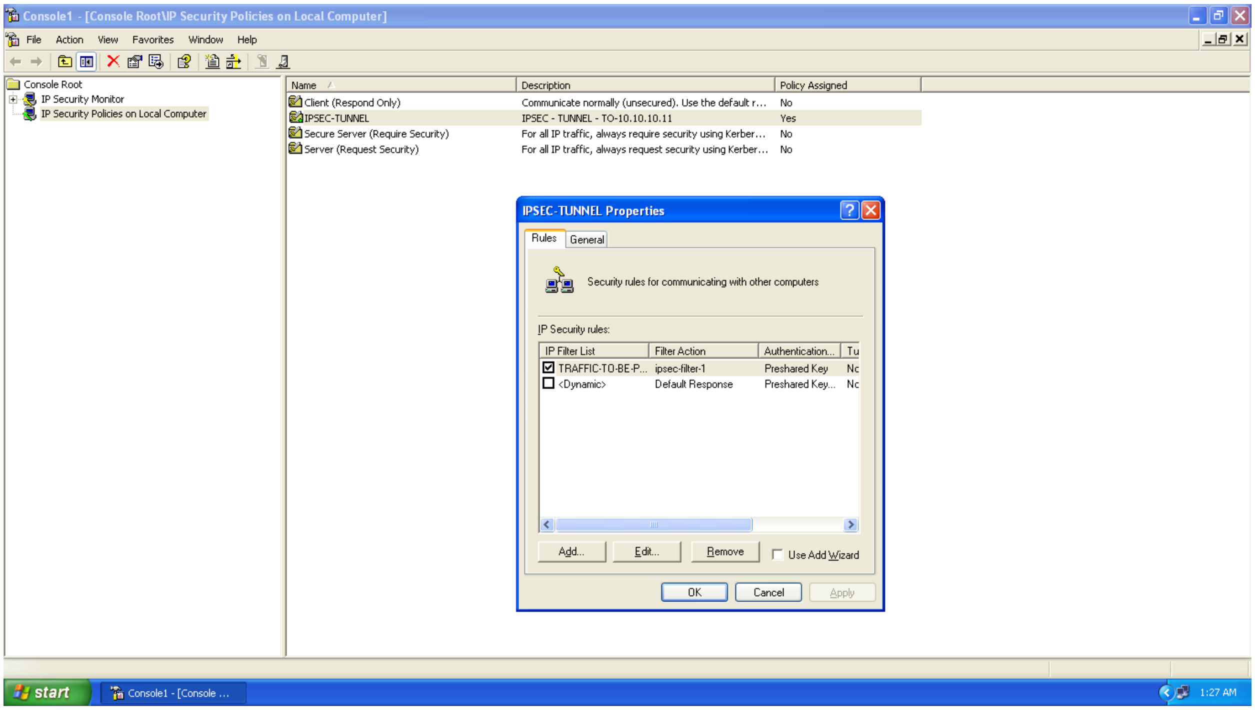
□ Data and address integrity without encryption (AH) :
Integrity algorithm: MD5

☑ Data integrity and encryption (ESP):
Integrity algorithm: SHA1
Encryption algorithm: 3DES

Session key settings:
☑ Generate a new key every: 100000 Kbytes
☑ Generate a new key every 3600 seconds

OK Cancel

Now our policy rules have been created which is *“TRAFFIC-TO-BE-PROTECTEDPBY-IPSEC”*. Make sure it has to be clicked after that apply it.


Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Monitor
IP Security Policies on Local Computer
start
Console1 - [Console ...
1:27 AM

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). Use the default r...	No
IPSEC-TUNNEL	IPSEC - TUNNEL - TO-10.10.10.11	Yes
Secure Server (Require Security)	For all IP traffic, always require security using Kerber...	No
Server (Request Security)	For all IP traffic, always request security using Kerber...	No

IPSEC-TUNNEL Properties

Rules | General

Security rules for communicating with other computers

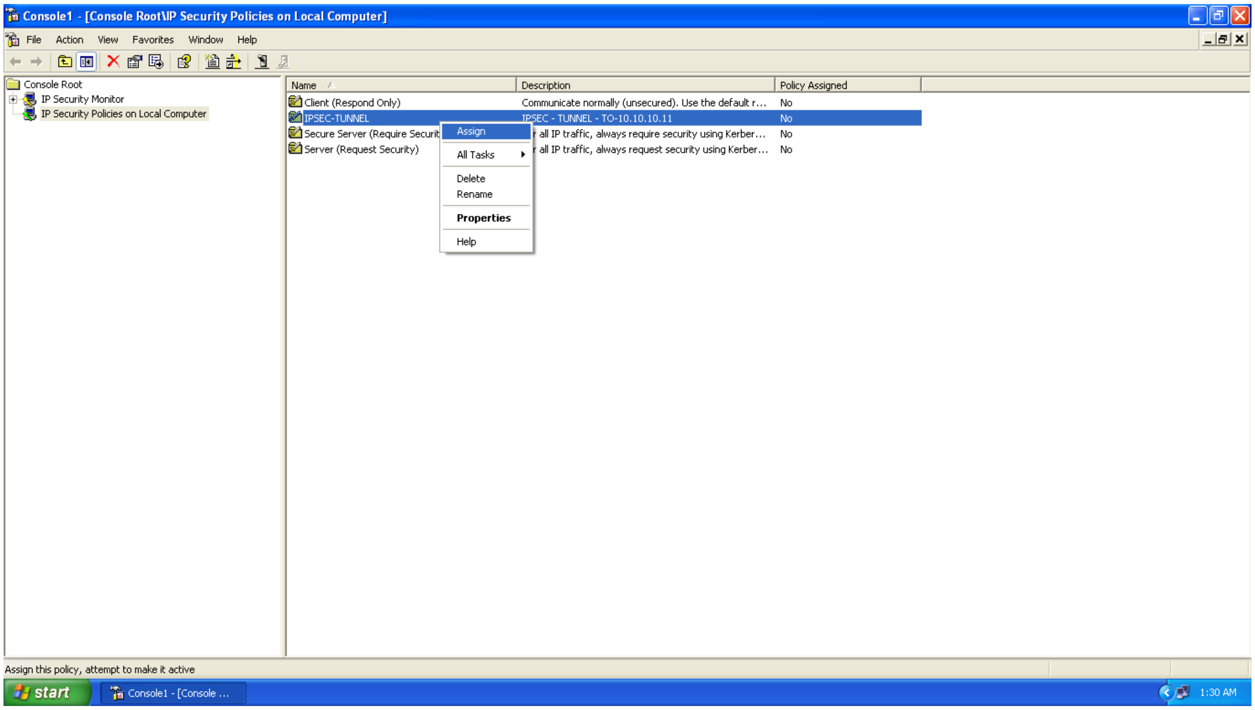
IP Security rules:

	IP Filter List	Filter Action	Authentication...	Tu
☑	TRAFFIC-TO-BE-P...	ipsec-filter-1	Preshared Key	Nc
□	<Dynamic>	Default Response	Preshared Key...	Nc

Add... Edit... Remove □ Use Add Wizard

OK Cancel Apply

Now we can see that our policy is listed in IP Security Policy Management. We can right click on the policy and we need to click on *“Assign”* option to assign our security policy as shown in figure.


Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Monitor
IP Security Policies on Local Computer
Assign
All Tasks
Delete
Rename
Properties
Help
start
Console1 - [Console ...
1:30 AM

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). Use the default r...	No
IPSEC-TUNNEL	IPSEC - TUNNEL - TO-10.10.10.11	No
Secure Server (Require Securit	r all IP traffic, always require security using Kerber...	No
Server (Request Security)	r all IP traffic, always request security using Kerber...	No

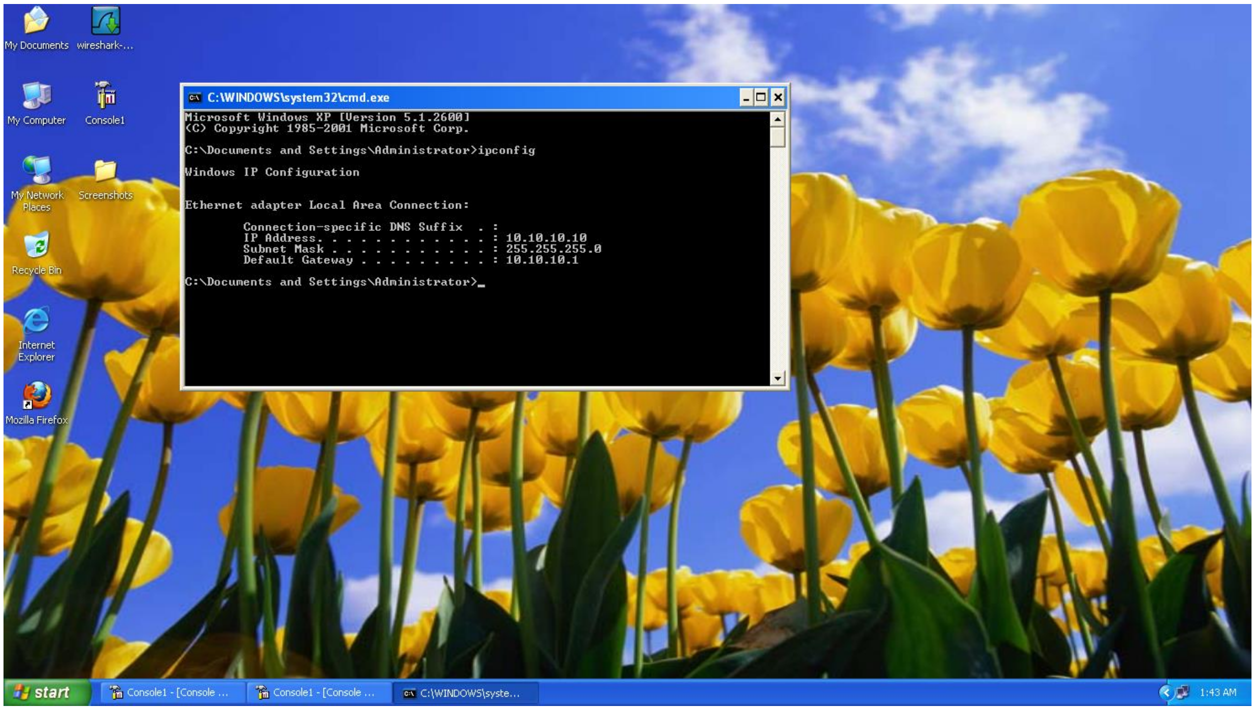
Assign this policy, attempt to make it active

2.3 Client Configuration

Same steps have to be followed for the configuration for client systems. But make sure that we need to assign the IP address before starting the actual configuration process. As we have given 10.10.10.10 in our server system we can give 10.10.10.11 to our this client system.

2.4 Client - Server Information

IP address of the client machine is set to 10.10.10.11 and our server machine’s IP address is 10.10.10.10 as shown in figure.

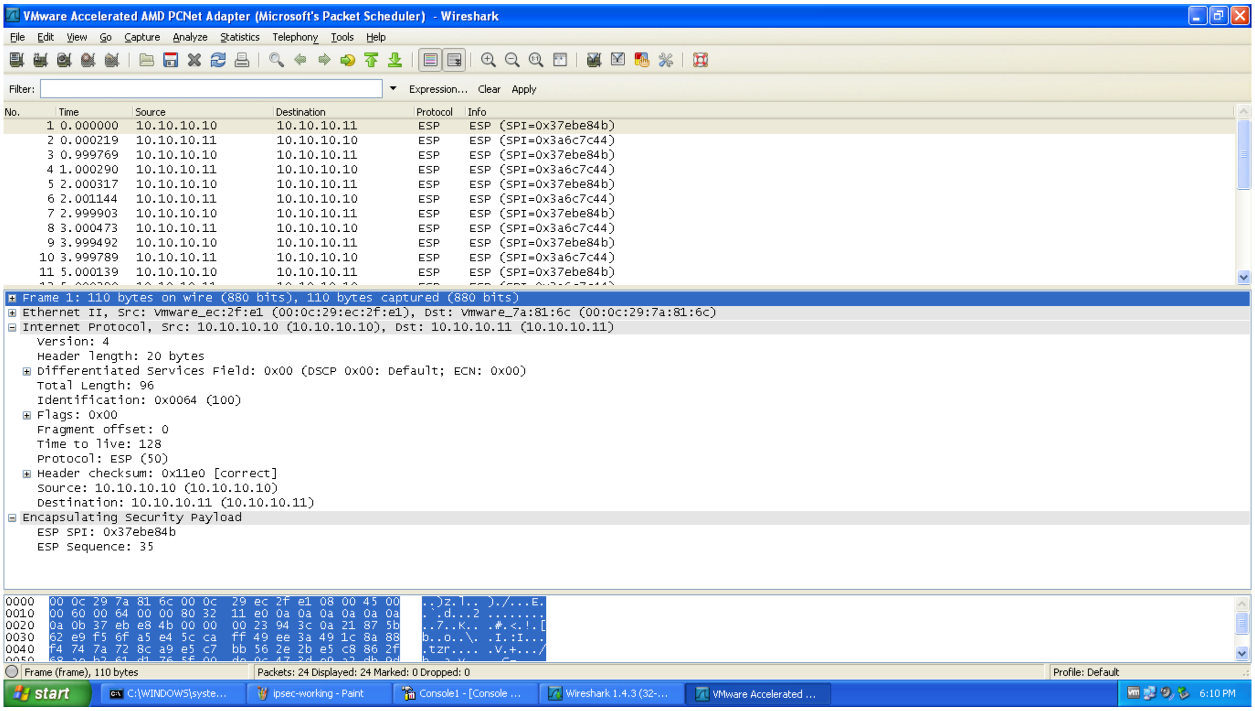


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.10.10.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.10.10.1

C:\Documents and Settings\Administrator>_
```

Now we will send the actual packets from our server machine to a client machine and we will monitor the packet analysis using Wireshark tool. As we will ping first time machine will negotiate security and it will give you the reply coming from the client machine.

2.5 Packet Analysis Result

As we can clearly see here packets are being sent from 10.10.10.10 (Server) to 10.10.10.11 (client). Both the client and server are specified clearly. The protocol which is specifically used is also mentioned here as ESP (Encapsulating Security Payload) which shows that the transmitted packets are encrypted and they are being sent by IPSEC protocol.


VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
start
C:\WINDOWS\syste...
ipsec-working - Paint
Console1 - [Console ...
Wireshark 1.4.3 (32-...
VMware Accelerated ...
6:10 PM

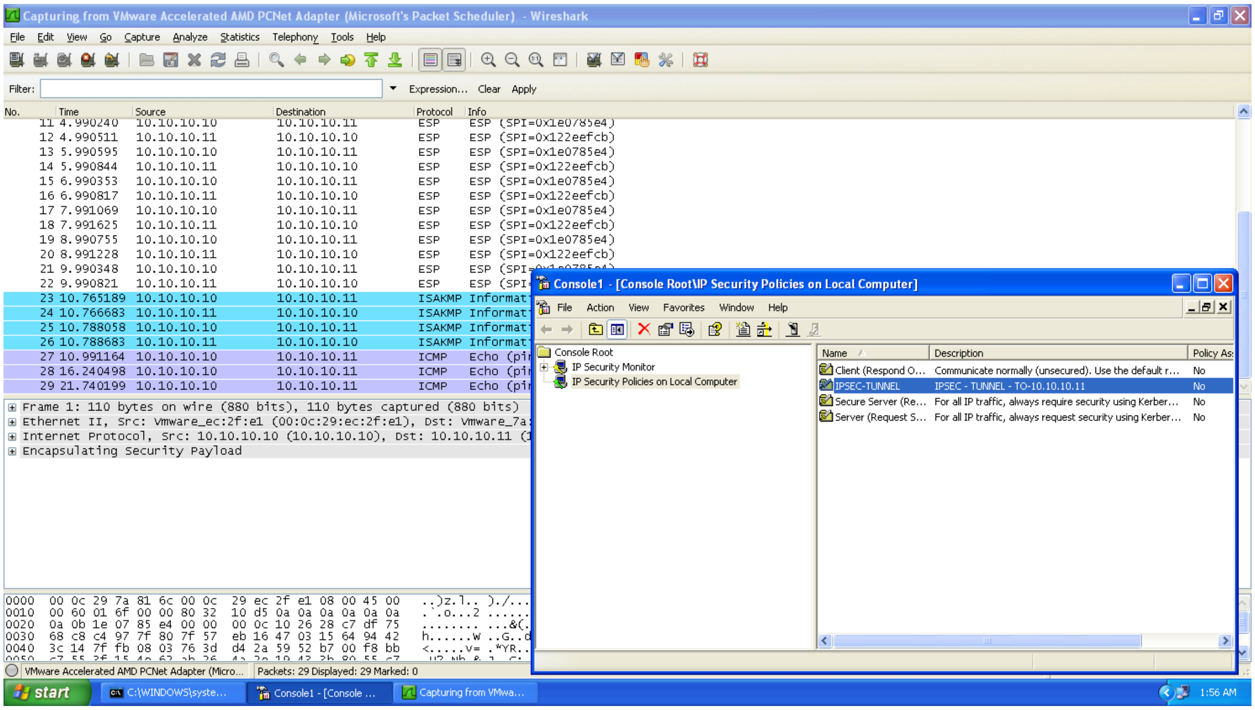
```
No.     Time       Source         Destination    Protocol  Info
      1 0.000000   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x37ebe84b)
      2 0.000219   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x3a6c7c44)
      3 0.999769   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x37ebe84b)
      4 1.000290   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x3a6c7c44)
      5 2.000317   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x37ebe84b)
      6 2.001144   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x3a6c7c44)
      7 2.999903   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x37ebe84b)
      8 3.000473   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x3a6c7c44)
      9 3.999492   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x37ebe84b)
     10 3.999789   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x3a6c7c44)
     11 5.000139   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x37ebe84b)
```

```
⊞ Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
⊞ Ethernet II, Src: Vmware_ec:2f:e1 (00:0c:29:ec:2f:e1), Dst: Vmware_7a:81:6c (00:0c:29:7a:81:6c)
⊟ Internet Protocol, Src: 10.10.10.10 (10.10.10.10), Dst: 10.10.10.11 (10.10.10.11)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 96
    Identification: 0x0064 (100)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ESP (50)
  ⊞ Header checksum: 0x11e0 [correct]
    Source: 10.10.10.10 (10.10.10.10)
    Destination: 10.10.10.11 (10.10.10.11)
⊟ Encapsulating Security Payload
    ESP SPI: 0x37ebe84b
    ESP Sequence: 35
```

```
0000  00 0c 29 7a 81 6c 00 0c  29 ec 2f e1 08 00 45 00   ..)z.l.. )./...E.
0010  00 60 00 64 00 00 80 32  11 e0 0a 0a 0a 0a 0a 0a   .`.d...2 ........
0020  0a 0b 37 eb e8 4b 00 00  00 23 94 3c 0a 21 87 5b   ..7..K.. .#.<.!.[
0030  62 e9 f5 6f a5 e4 5c ca  ff 49 ee 3a 49 1c 8a 88   b..o..\. .I.:I...
0040  f4 74 7a 72 8c a9 e5 c7  bb 56 2e 2b e5 c8 86 2f   .tzr.... .V.+.../
```

```
Frame (frame), 110 bytes    Packets: 24 Displayed: 24 Marked: 0 Dropped: 0    Profile: Default
```

While the machine is sending continuous packets from server to client, I am on assigning the security policy and I will look at the Wireshark result that in which manner the packet transmitting process is done.


Capturing from VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
start
C:\WINDOWS\syste...
Console1 - [Console ...
Capturing from VMwa...
1:56 AM

```
No.     Time       Source         Destination    Protocol  Info
     11 4.990240   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x1e0785e4)
     12 4.990511   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x122eefcb)
     13 5.990595   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x1e0785e4)
     14 5.990844   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x122eefcb)
     15 6.990353   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x1e0785e4)
     16 6.990817   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x122eefcb)
     17 7.991069   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x1e0785e4)
     18 7.991625   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x122eefcb)
     19 8.990755   10.10.10.10    10.10.10.11    ESP       ESP (SPI=0x1e0785e4)
     20 8.991228   10.10.10.11    10.10.10.10    ESP       ESP (SPI=0x122eefcb)
     21 9.990348   10.10.10.10    10.10.10.11    ESP       ESP (SPI=
     22 9.990821   10.10.10.11    10.10.10.10    ESP       ESP (SPI=
     23 10.765189  10.10.10.10    10.10.10.11    ISAKMP    Informat
     24 10.766683  10.10.10.11    10.10.10.10    ISAKMP    Informat
     25 10.788058  10.10.10.10    10.10.10.11    ISAKMP    Informat
     26 10.788683  10.10.10.11    10.10.10.10    ISAKMP    Informat
     27 10.991164  10.10.10.10    10.10.10.11    ICMP      Echo (pi
     28 16.240498  10.10.10.10    10.10.10.11    ICMP      Echo (pi
     29 21.740199  10.10.10.10    10.10.10.11    ICMP      Echo (pi
```

```
⊞ Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
⊞ Ethernet II, Src: Vmware_ec:2f:e1 (00:0c:29:ec:2f:e1), Dst: Vmware_7a
⊞ Internet Protocol, Src: 10.10.10.10 (10.10.10.10), Dst: 10.10.10.11 (1
⊞ Encapsulating Security Payload
```

```
0000  00 0c 29 7a 81 6c 00 0c  29 ec 2f e1 08 00 45 00   ..)z.l.. )./...
0010  00 60 01 6f 00 00 80 32  10 d5 0a 0a 0a 0a 0a 0a   .`.o...2 ......
0020  0a 0b 1e 07 85 e4 00 00  00 0c 10 26 28 c7 df 75   ........ ...&(.
0030  68 c8 c4 97 7f 80 7f 57  eb 16 47 03 15 64 94 42   h......W ..G..d
0040  3c 14 7f fb 08 03 76 3d  d4 2a 59 52 b7 00 f8 bb   <.....v= .*YR..
```

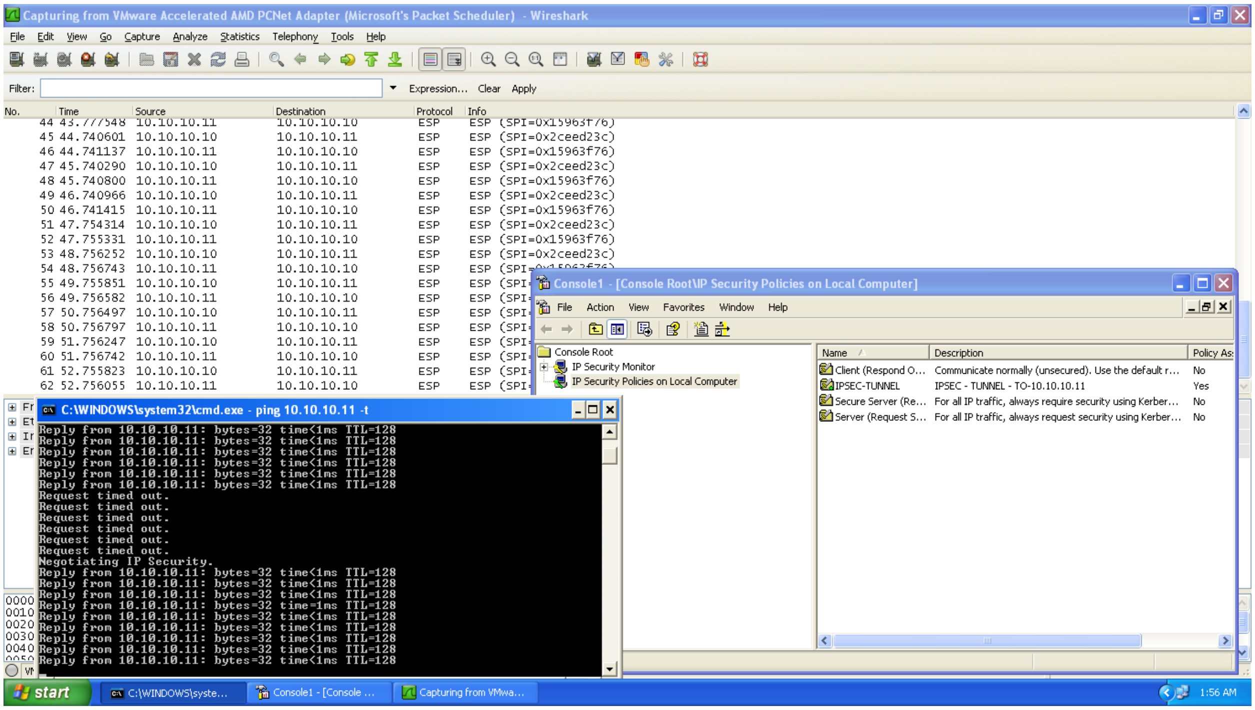
```
VMware Accelerated AMD PCNet Adapter (Micro...    Packets: 29 Displayed: 29 Marked: 0
```

Console Root
⊞ IP Security Monitor
IP Security Policies on Local Computer

Name	Description	Policy As:
Client (Respond O...	Communicate normally (unsecured). Use the default r...	No
IPSEC-TUNNEL	IPSEC - TUNNEL - TO-10.10.10.11	No
Secure Server (Re...	For all IP traffic, always require security using Kerber...	No
Server (Request S...	For all IP traffic, always request security using Kerber...	No

As we can see that it has changed from ESP to ISAKMP which is known as Internet Security Association and Key Management Protocol. Then immediately, it will change the protocol to ICMP which is known as Internet Control Management Protocol. So ICMP is not secured. One can see the payload data in Wireshark as the packets are being sent via ICMP protocol. It means packets are not encrypted.

When security policy is reassigned, It will start transmission of packets via ESP protocol which is secured and thus encrypted transmission continues to occur which is shown as below.



Capturing from VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

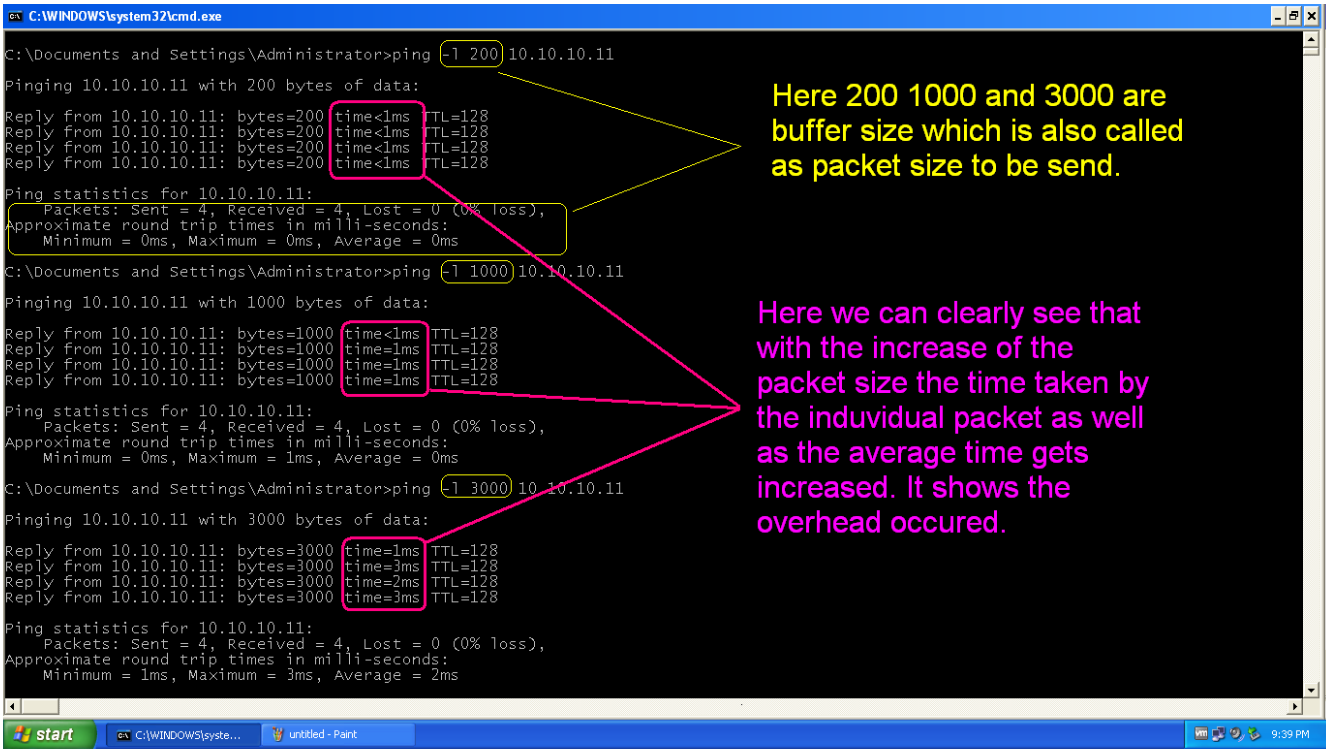
```
No.     Time        Source          Destination     Protocol  Info
     44 43.777548   10.10.10.11     10.10.10.10     ESP       ESP (SPI=0x15963f76)
     45 44.740601   10.10.10.10     10.10.10.11     ESP       ESP (SPI=0x2ceed23c)
     46 44.741137   10.10.10.11     10.10.10.10     ESP       ESP (SPI=0x15963f76)
     47 45.740290   10.10.10.10     10.10.10.11     ESP       ESP (SPI=0x2ceed23c)
     48 45.740800   10.10.10.11     10.10.10.10     ESP       ESP (SPI=0x15963f76)
     49 46.740966   10.10.10.10     10.10.10.11     ESP       ESP (SPI=0x2ceed23c)
     50 46.741415   10.10.10.11     10.10.10.10     ESP       ESP (SPI=0x15963f76)
     51 47.754314   10.10.10.10     10.10.10.11     ESP       ESP (SPI=0x2ceed23c)
     52 47.755331   10.10.10.11     10.10.10.10     ESP       ESP (SPI=0x15963f76)
     53 48.756252   10.10.10.10     10.10.10.11     ESP       ESP (SPI=0x2ceed23c)
     54 48.756743   10.10.10.11     10.10.10.10     ESP       ESP (SPI=0x15963f76)
     55 49.755851   10.10.10.10     10.10.10.11     ESP       ESP (SPI
     56 49.756582   10.10.10.11     10.10.10.10     ESP       ESP (SPI
     57 50.756497   10.10.10.10     10.10.10.11     ESP       ESP (SPI
     58 50.756797   10.10.10.11     10.10.10.10     ESP       ESP (SPI
     59 51.756247   10.10.10.10     10.10.10.11     ESP       ESP (SPI
     60 51.756742   10.10.10.11     10.10.10.10     ESP       ESP (SPI
     61 52.755823   10.10.10.10     10.10.10.11     ESP       ESP (SPI
     62 52.756055   10.10.10.11     10.10.10.10     ESP       ESP (SPI
```

```
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Negotiating IP Security.
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time=1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
```

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Monitor
IP Security Policies on Local Computer

Name	Description	Policy As:
Client (Respond O...	Communicate normally (unsecured). Use the default r...	No
IPSEC-TUNNEL	IPSEC - TUNNEL - TO-10.10.10.11	Yes
Secure Server (Re...	For all IP traffic, always require security using Kerber...	No
Server (Request S...	For all IP traffic, always request security using Kerber...	No

We can see that in the transmission of packets we are getting “Request Timed Out” which is a clear proof that there is a break in transmission while we were reassigning the policy for our secure transmission. Also here overhead occurs while sending the packets. Let us try to understand the below figure which sends different different size of packets from source to destination.



```
C:\Documents and Settings\Administrator>ping -l 200 10.10.10.11

Pinging 10.10.10.11 with 200 bytes of data:

Reply from 10.10.10.11: bytes=200 time<1ms TTL=128
Reply from 10.10.10.11: bytes=200 time<1ms TTL=128
Reply from 10.10.10.11: bytes=200 time<1ms TTL=128
Reply from 10.10.10.11: bytes=200 time<1ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping -l 1000 10.10.10.11

Pinging 10.10.10.11 with 1000 bytes of data:

Reply from 10.10.10.11: bytes=1000 time<1ms TTL=128
Reply from 10.10.10.11: bytes=1000 time=1ms TTL=128
Reply from 10.10.10.11: bytes=1000 time=1ms TTL=128
Reply from 10.10.10.11: bytes=1000 time=1ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\Administrator>ping -l 3000 10.10.10.11

Pinging 10.10.10.11 with 3000 bytes of data:

Reply from 10.10.10.11: bytes=3000 time=1ms TTL=128
Reply from 10.10.10.11: bytes=3000 time=3ms TTL=128
Reply from 10.10.10.11: bytes=3000 time=2ms TTL=128
Reply from 10.10.10.11: bytes=3000 time=3ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

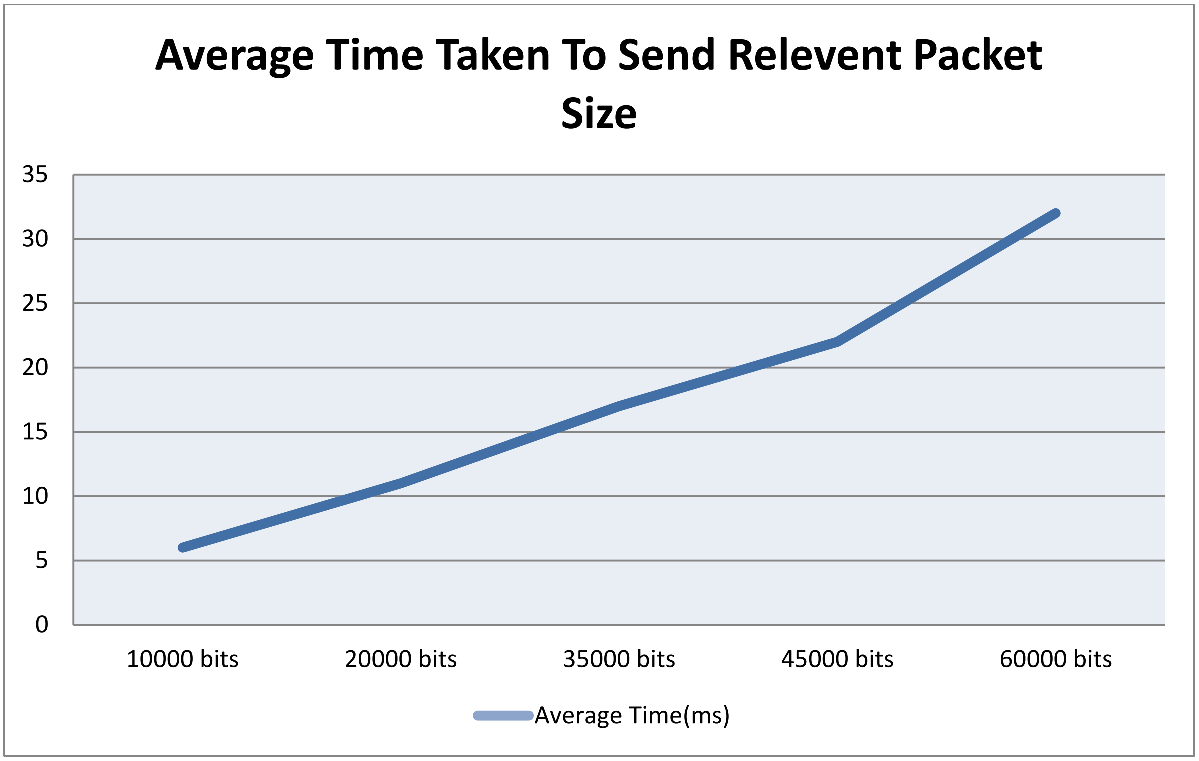
Here 200 1000 and 3000 are buffer size which is also called as packet size to be send.

Here we can clearly see that with the increase of the packet size the time taken by the induvidual packet as well as the average time gets increased. It shows the overhead occured.

As per the figure we can clearly see that as soon as I increased the packet size to send at the destination, the individual time to be taken by packet to send as well as the average time gets increased. So it clearly shows the overhead in packet sending. With these analyses I have sent many different sizes of packets and here is the table which describes the scenario very clearly.

Packet Size	Minimum Time(ms)	Maximum Time(ms)	Average Time(ms)
10000 bits	4	7	6
20000 bits	6	13	11
35000 bits	9	24	17
45000 bits	12	29	22
60000 bits	19	38	32

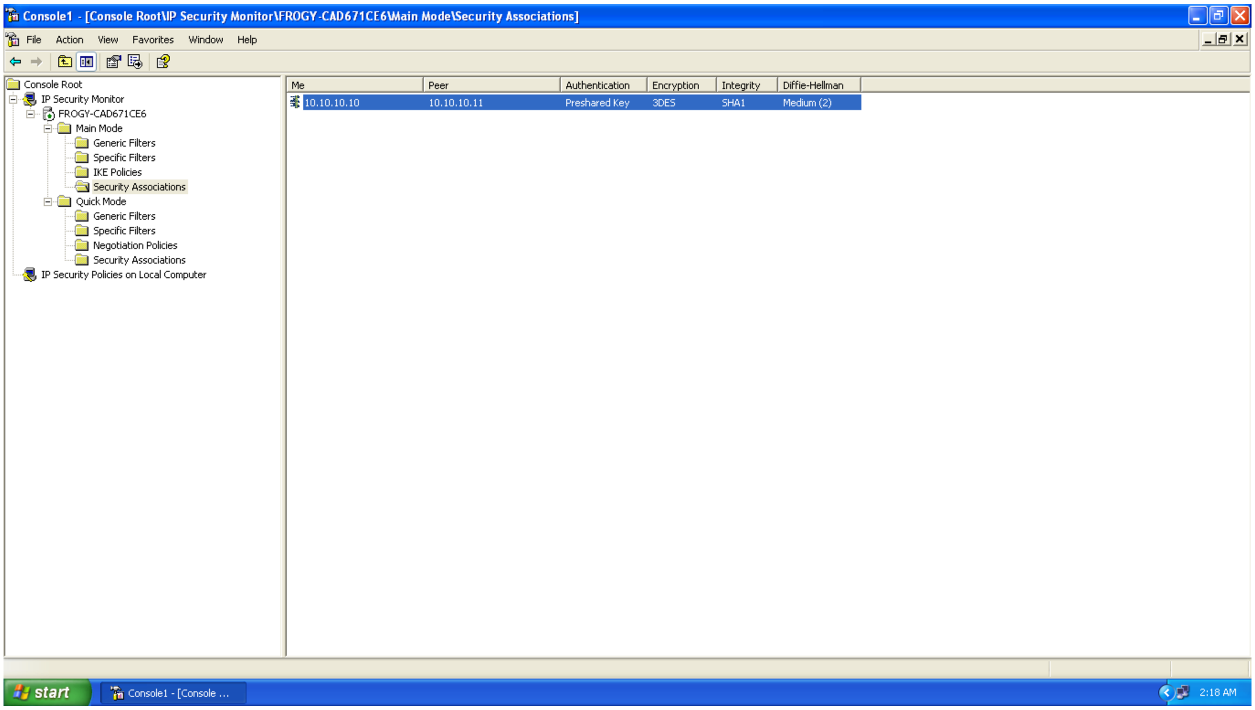
If we are going to plot a graph of these calculations then it will become like this. X-axis will be the packet size or the buffer size to be sent at destination host and Y-axis will be the average time taken to send the whole packet.



As we all know that overhead and throughput are in inverse mode of each other if overhead increases then throughput will be decreasing and if throughput will be increasing then overhead have to decrease.

2.6 Proof of Concept – Security Associations

When we assign IPsec policy, Security Association will occur at both side client and server.Which can be usually seen under IP Security Policy -> Main Mode/Quick Mode. Here server’s main mode security association is shown below :



Console1 - [Console Root\IP Security Monitor\FROGY-CAD671CE6\Main Mode\Security Associations]

Me	Peer	Authentication	Encryption	Integrity	Diffie-Hellman
10.10.10.10	10.10.10.11	Preshared Key	3DES	SHA1	Medium (2)

2.7 Conclusion

It can be concluded from whole demonstration that, the IPSEC Protocol suite is clearly explained in detail with the necessary key functionality and the certain limitations which are mentioned in block 1 in this document. In block 2, I have shown the full configuration process along with the necessary screenshots.

Bibliography

Mr. Hitesh dhall, M. D. (2012). *IMPLEMENTATION OF IPSEC PROTOCOL.* Rohtak, India .

Nikander, J. A. (n.d.). *Limitations of IPsec Policy Mechanisms.* Jorvas, Finland: Ericsson Research NomadicLab.

Paterson, J. P. (n.d.). *Attacking the IPsec Standards in Encryption-only.* Bristol, UK.

Paterson, K. G. (2006). *A cryptographic tour of the IPsec standards.* Elsevier Ltd.

S. P. Meenakshi, S. V. (2010). *Impact of IPSec Overhead on Web Application.*

References

I. CHRISTOS XENAKIS*, NIKOLAOS LAOUTARIS, LAZAROS MERAKOS, IOANNIS STAVRAKAKIS, *A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms.* Communication Networks Laboratory, Department of Informatics and Telecommunications, University of Athens, Athens 15784, Greece.

II. JARI ARKKO, P.N., *Limitations of IPsec Policy Mechanisms.* Ericsson Research NomadicLab, 02420 Jorvas, Finland.

III. JEAN PAUL DEGABRIELE,KENNETH G. PATERSON, *Attacking the IPsec Standards in Encryption-only Configurations.* Information Security Group, Royal Holloway University of London, Egham, Surrey TW20 0EX, UK,Hewlett-Packard Laboratories, Bristol Filton Road, Stoke Gifford, Bristol BS34 8QZ, UK.

IV. KENNETH G. PATERSON, 2006. *A cryptographic tour of the IPsec standards.* Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK.

V. S. P. MEENAKSHI,S. V. RAGHAVAN, *Impact of IPSec Overhead on Web Application Servers.*

VI. Mr. Hitesh dhall, M. D. (2012). *IMPLEMENTATION OF IPSEC PROTOCOL.* Rohtak, India .

VII. Nikander, J. A. (n.d.). *Limitations of IPsec Policy Mechanisms.* Jorvas, Finland: Ericsson Research NomadicLab.

VIII. Paterson, J. P. (n.d.). *Attacking the IPsec Standards in Encryption-only.* Bristol, UK.

IX. Paterson, K. G. (2006). *A cryptographic tour of the IPsec standards.* Elsevier Ltd.

X. S. P. Meenakshi, S. V. (2010). *Impact of IPSec Overhead on Web Application.*

XI. (n.d.). Retrieved from http://www.onlinebusiness.newstipstricks.com/wp-content/uploads/2013/03/Cryptography.png