IPSEC services

IP sec is going to provide these services but which service provided by which protocol so ,lets have a look, access control can do this, ESP can do this, ESP with authentication can do this 3 things you can have access control, connection less integrity , you will get , authentication header and ESP with authentication option but with single ESP you are going to get, Data origin authentication same thing, rejection of the replayed packets 3 of them and confidentiality with ESP and ESP with authentication, confidentiality same , limited traffic flow confidentiality, in this one it is come with ESP. and not with AH and in this one I have to encrypt the message I use the ESP. but this is not the end of the story {question form a student}. Whenever you need the content of the message that you are exchanging you are using ESP, you don't need AH, we are going to do some kind of authentication for us, this AH is totally different protocol ,

Security Associations

To use this IPSEC we are going to have two different mode we have two different header and these headers are used in two different modes one is called transport mode and the other is called tunnel mode so the normal transport ESP, things are going to get more complex and we will look at that later, before defining the modes we have very basic thing for IPSEC without that defining io IPSEC will not work that's called security association, before exchanging any mode, these two modes, IPSEC message are must have established security association, during the installation of IPSec the technicians are defining this security associations, there are one way associations, this is also very important lets say that I have two point a and point b and this will use IPSEC ,what I said is I'm going to have security association with these guys and it will be one ways association, what we are going to do is this , im going to define security association from a to b but this definition will not be going to valid for the SA from b side, from side you need to have another SA, and this SA have 3 parameters one is called security parameter index SPI this SPI is going to be seen in every AH, because that is very important for us to locate the SA, this is the very imp part of security association ,lets say that I have the database of SA, in that database I have to find the id of the SA and that id is the SPI it is profiled I m going to define everything key ,key time everything is going to be defined, you may also define firewall , there is nothing like this is for individual user until you define one way SA for two nodes that two nodes will be able to communicate for one direction, inside there is some when you say acknowledgment if they identify the replayed packets hey are not going to say that I dint receive and all ,they are going to reject it, there is another one which is ip address destination and the third one is Security protocol identifier , it has number of other parameters sequence number, AH and EH info lifetime, and it has database of security associations, this is as I said database of SA we have to find that SA when I receiver the packets ,lets say that when I receive the packet then it is in ESP protocol in ESP protocol what is going to be field and that field is going to be spi and by using that im going to go to all the algorithmic field so on and so for those that I can process that message and its same for AH, it has a field for spi field by using that they are going to find the field see they are going to able to process the packets ,and then the profile you are going to create is another spi like you can see a bit string assigned to this S A ,having a local significance only the spi is carried in AH and ESP headers are enable the receiving system to select a SA under which a received packet will be processed .otherwise recipient cannot process, im trying to remember I don't

know how many profile ,IP destination address this is also important currently only, unicast address are allowed this is the address of the destination endpoint of SA which may be an end user system or a network system such as firewall system .this is unicast you cannot multicast this one , this is one to one this cant be one to many as we don't SA defined to one to many we have only for one to one tere are some research going on to be multicast address, people are working on it, this is unicast. This also means this could be firewall .for simplicity what we are doing is as SA are concerned we have a firewall and everytime the user IPSEC client side for each user an IPSEC firewall l handling all the people as we are not dealing with the people once ipsec everybody is getting for m firewal so the transfer is clear from the end user so behind the firewall everything is celar but outside you original ip header is encrypted and also protected against changes in the fields of the ip address that is for the ESP we may not require confidentiality all teh time you may also send authentication part as well that AH is providing integrity for the whole message in the ip header so that no one can change the source , we call that ICV integrity check value using the hash algorithm , in the security protocol identifier, this indicated whether the association AH or ESP security association ,without the security association you will not be able to proceed, or process the incoming message, because from the protocol find the SA and read the SA because when I come to that SA there are going to be this parameters and lot of things ,and based on those things I can process the incoming message .