SA selectors

We saw the details of SA, SPI and we know the parameters of SA as SA selectors for SA ,lets go and have a look at the details of AH and ESP

Transport and tunnel mode

Before explaining the AH and ESP we have to define the modes that we are using in ipsec, as I said before we are going to have 2 modes one is transport and the other is tunnel , AH is transport mode SA or AH is tunnel mode SA , ESP header with Tunnel mode SA and ESP with transport mode SA , so you can use AH and ESP in 2 modes transport and tunnel modes ,lets have a look at the difference between these two, ets start with AH , it authenticated IP payload and selected portions of ip header and ipv6 extension headers so theirs is going to only authentication ,it will be done using HMAC and we are calculate the HMAC its says the whole ip payload when you receive the packets the network layer, lets say this is packer and its coming for application lets say email and top of that one its SMTP header so this is the one and this going to go ,forget session layer ,we are using TCP/ip network it directly goes to TCP if it email its not going to TCP as its connectionless it will go to UDP ,lets say TCP and UDP will be for the transport layer and then we are going to take ip layer ,version 6 or version 4 , if its then ipv6 , then , its extension header when we say ip payload that is the ip payload that means all the data comes form upper layer a d some parts of this will be used to calculate the HMAC and to authenticate there is fields ,so we are going to fully authenticate the ip payloads but we are going to ipv portion and ipv6 extension headers, those portions are going to be very important in ipv6 all the fields ,that we saw in the we know ipv6 some of them are going to change to transmission , like you prepared he packet over here something ,but when it goes into the destination and it will be changed by the routers and if there is those kind of changed I cannot provide authentication, I don't know that will be the value for that field but some of the field by source and destination address , so these changes some of the fields will not change at all , im going to used not change fields fort the portions means unchangeable fields we are going to call it mutable and immutable, mutable is changeable fields, immutable unchangeable fields , so we are going to use immutable field for authentication and the whole payload, remember one of the reason we use ipsec was , ip spoofing attack ,people were changing the source address and making there addresses to impersonate some other people identity to avoid those kind of stuff im providing authentication os any change will be detected by destination and ip spoofing is not possible because I will be using immutable fields you may argue about destination ,in some cases destination address will be changed by the router if you are using sting routing or something but source address will not change at all , destination will not change also that means source and destination address will be bind in a way that it wont change imagine you are calculating address fields and somewhere on the destination you will be getting send the destination address, that's why this transport SA will be used to transfer the data and those fields , so any change will be detectable, look at the tunnel mode ,its going to authenticate entire inner packet ,there's a new concert its called inner ip packet, lets say that my original ip packet was there, here we go , this is my original message that I created and ipsec , added another header which is ipv6 and the extension headers its going to append another header ,this is called inner ip and this is called outer ip , we are going to do this , why they are doing ?lets c , so it authenticate inner ip address plus selected portions of outer IP header and outer ipv6 extension header,

when you go to tunnel mode you are going to always add a new header, new header is going to be added, if this is ipv6 you are going to have another one ,why they are doing this, we rare only providing only the portions of ip header and right now im providing , full authentication of ip header the actual thing that and using destination address of the outer ip address, will be network of the destination the destination address will be the firewall of the destination when the firewall checks this then it will forward this packet to the network , so then the destination can receive the packet may be the local network is the big packet and it is going to be transferred in the firewall to the destination machine and this is going o go in the intranet ,right now in the tunnel mode, I will provide full authentication in the ip header in the previous one I only provided partial authentication of ip header they know they are going to have this security association with the firewall and they are going to sue the destination address ,these are firewall transparent as long as you have firewall ,you don't have to deal with it , you are going to use transport mode essay , tunnel mode SA in other one it is tunnel mode SA and in this we are going to use all those things, are you really curious about the full packet changing is it that important for you then you are going to do this you are only looking for source changes it depends on your requirements ,in military channel they are using that's kind of default condition , but they are going to make more, this is tunnel mode lets have look at the ESP as it provides confidentiality , ESP encrypts ip payload and any ipv6 extension headers following the ESP headers lets remove this ipv6 right here and im going to have ESP header some where and this part of extension header and some other header which is routing header and everything is going to been crypto upto ESP header, as I said don't forget the ipv6 header, it is also going to be encrypted but also original ip header im not doing anything nor im asking for authentication ,im not going to click for this header so ip spoofing is possible now but im providing confidentiality for ip payload and some part of extension headers, bunch of encryption algorithm are possible most likely is 3 des and now AES is very important ,IDEA and cast are over there option ,from now on after that we are not going to have only one option ,anymore in security , we are going to have crypto pool and we are going to support that pool we will be having bunch of algorithm from that pool and one of them are going to be my choice, but 3edes and aes are there ,SSL forms with cipher suit its nothing to do with ipsec, so are we clear, we are going to have confidentiality , but confidentiality can be authentication only in payload if any one changes anything when i decrypt it is going to be easy and it is going to be source basically ,but ESP is going to be user id in tunnel mode what we are going to have is additional ip header ,lets put actual ip header, lets say their have my ip header and im going to include my original ip header , it is fully protected, this si the based for vpns, we will talk about it we are creating a tunnel in public communication link and we are sending through the tunnels , so I have two types of transportation lets say that I have a truck cars are my message and trucks are going from one direction to another , it is driver you have to stop at the station and that's transport mode of authentication if I build the truck from this direction to other direction we are using this tunnel to that destination then that is ESP tunnel mode because no one can see inside the tunnel basically so that is two ways are working that way , original carries is des guy and original packet is secret and no one will know the destination address , not exactly every body know s that this packet is going to that destination address and that will definitely in the previous it could be but now it must be other wise thee is not meaning ,if I put the original destination address then im loosing this ESP mode in tunnel mode and this is firewall address, everyone knows that this packet will go to firewall and it will remove this parts and decipher it and this going to recover the ip address and it will forward that packet to destination address in original

ip header ,so as you see with the ESP im going to have encryption in transport or tunnel mode, does not matter the major difference between transport and tunnel mode is in tunnel I need another carrier ,I can give you another example ,there is a tunnel between England and Europe you can drive to England through british channel but actually we are not driving train is driving is driving as we are driving till the station and it will drive from this station to that station in the England side or franc side and that train is ip version 6 header and your car is this ip and you cannot drive your car in the tunnel you need another carrier like train in this mode with the new address, the address of the train is the destination of station the actual destination will be in somewhere London or in paris so no one knows where you are heading after reaching the station , so that kind of analogy will work with tunnel and transport mode, we have ESP and authentication , we will see the description here ip payload is encrypted in transport and ip extension field and authenticates ip pay load but not ip payload over here some portion of ip payload is authenticated , in tunnel mode it authenticates only inner ip packets anything for the outer ip header its only authenticate only inner ip id ,so when you get ESP with ah , then it is limited compared to authentication header because lot of people are asking why you need AH when you have ESP with AH ,this is a little bit different this guys does not provide ip spoofing attack protection but AH does , this Is important if this is done with the ip part of the data if this is really important to you then you need ah for that one ,as I said encryption is some form of ah ,because this guys are asking something extra in military no body is going to use esp with AH , but this is an option and available over there , only diference you have to know is this authentication is different than AH of authentication , so now we know SA, transport mode and tunnel mode and lets go and look details of this protocol.