Transport and tunnel mode

Last time we were discussing about AH one of the major thing in ah was SPI ,what was SPI ,that's the pointer that we are going to use for SA, that is going to use to fie nth related SA and we said that we can use two modes one is transport mode and the other is tunnel mode so lets have look at the packet structure in AH in transport mode and tunnel mode ipv4 and ipv6 packet format will be internet , this iipvv4 and no ip header and TCP is upper layer and original ip header that is version 4 and in ipv6 this data and we have upper layer protocol and we have extension header and original ip header and this is ipv6 header ,If you have ipv4 and there is not ip security then the packet goes like this if you are suingipv6 packet will be like this ,a lets apply authentication header in transport mode, if im ipv4 format is like this data TCP and AH, and original ip header , ah will be placed between upper layer protocol means between orig ip header before upper layer protocol headed what was the definition of AH its going to provide authentication for whole ip header what's the ip header over here TCP and data and also tis going to provide particularly for the ip header what was that partial thing was why I said its going to partially authenticate its going to changing during transmission in other words its going to look at immutable fields and not mutable fields in transport authenticate expect for mutable fields ,what about ipv6 ,data ,TCP ,dest option field , remember while discussing we said that this destination option is going to come after authentication header and ESP , DH is going tobe here and followed by AH , it will be placed between destination ip header and other ip header and other fields where is the security authentication will be provide for this data for this destination header and TCP ,extension headers and some part of ipv6 header these are very important as im going to asking in final exam im going to out the format I will say authenticate this part which part we are using for this part and structure and modes used from each structure, lets have a look at tunnel mode, data TCP and when you are using tunnel mode, we are going to have a new ip header this one is going to carry all the data, original ip header is right here and here is AH now you guys tell me authenticate is going to calculate do not his data or this TCP header or original ip header with full fields because original ip header is not going to change , itds not going to change the actual routing is going to be one by this new ip header so that why I will be able to provide the full authentication for old ip address and partial for new one we are going ot authentications only for immutable field in new ip address in IPV6 orig ip header and orig extension and it is placed between TCP and AH , this is the new ip header and extension im going to provide full authenticating for old ip header and partial authentication for new ones , so ah is used in this way if you are using tunnel mode or transport mode, in other words on the network yo will have this structure , this network address is transferred in the destination address when the firewall receives this on it will get the whole thing but where is the authentication part , how am I going to authentication , im firewall how am i going to authenticate this packet, ?..i using AH remember in ah there were 976 fields and we called it ICV and I explained how we are going to calculate this value and how we are going to authenticate this value ,destination header and ip header and icv will be 0 in the whole header and mutable fields are going to be 0 in te fields with t0 im going to calculate the whole data has dh from the data and im going to get these results ,form one result 96 bits sha 1 and md 5 95bits md5, Im going to place 96 bits icv field , so AH icv field is carrying the icv and now im recalculating the data and im still calculating the icv, with the same rues icv of AH will be 0 and mutable fields will be 0, hash it recalculated icv is same iwht the recalculated with same icv header that means it is authenticated

,authentication will work like this ,then firewall will work like this and forward the packet by using the original ip header to the network, this is the case why do I need authentication in IPSec , major things is ip spoofing this way I have the hashed value of source and destination no one can change if they can then this used to detect we can detect those kind of attacks so ip spoofing is not possible with those kind of attacks in the AH im binding source and destination address in such a way that it is unforgable, so icv calculation is required usage of sha and md 5 algorithm sha1 and md5 doesn't require any secret info so any body can calculate the secret info so what are you going to do?.. when we calculate the authentication we are using sha1 and md5 , but we are also using the hmac algorithm hamc required secret key so the destination requires that secret key for the calculation header and that key is going to come from wherer? From SA, that key is going to be in the SA so then the firewall is going to look at the spi and define the relegated security application and it can use the hmac key for the calculating the key no one can forge that icv value it depends on a secret info.

ESP

Provides message content confidentiality and limited traffic flow confidentiality it can optionally provide same authentication services as AH actual AH and authentication option in ESP it didn't deal with header it provide authentication for payload, the basic mode is cbc and algorithm are in IPSec you a can use it, lets have look at this one , first big field is SPI like in AH ,spi over here and spi AH do you think its same , itsn ot SA SPi is related to only one protocol and that's going to authentication or ESP and this is to same from the AH in the ip context, if you need esp but you have only SA for AH then you are going to generate Authentication , for this ESP header and the sequence number to avoid replay attacks the size is 32 bit and you are going to use 32 bit and this is the payload the actual data will be carried over here and this data will be encrypted it says encryption and confidentially coverage this data is encrypted and let say you use 3 des encryption what is the block size 64 bits and 1 kb is multiple byte 64 bits?. No you need packet this field 0 to 255 bytes you need pad length and he next header is going t be destination header, and if you select the authentication option for this field then you are going to only authenticate this one and place it to the data , so this is called esp nby sending youa re going to provide the confidentiality for the data you are using , you are using this esp in transfer mode and tunnel mode ,

Transfer vs tunnel modeESP

Transport mode is used to encrypt and optionally authenticate IP data, it is protected but header left is clear its not thing to do with header protocol can do traffic analysis and this time you are going to have new Ip address and its not going to add the id of the destination , it is good for esp host to host header, add new header for the next hop this is going to be the basic for VPNs, transport layer security we are using the encrypted TCP session and this is in tunnel mode and encrypted by and im using ht external network im having the encrypted TCP version and VPN or you can have it like this encrypted tunnel and lot of VPN based on your requirement once you have this VPN you can face this way or this way you are going ot behave like this cloud is you r entire network , but how are you gong to do that lets have look at packet structure win transport wee are going to do what?, we are going to have security fort the ip data and it will be in clear form in ipv4 there is orig ip header and TCP header ,ESP header and data and ESP trailer and this is t he data that we place in ESP data field and these are all encrypted this tried part if

you select authentication part then you are going to just authenticate the data if you didn't select the n no authentication field and ESP authentication option if you have selected then you will have ESP authentication and then I m going to have orig ip header it is not going to have orig ip header in clear and esp header in clear form the only thing is the payload encrypted and that data is TCP and other data lets say you have email and this data SMTP header an the data itself and its going to go to transport layer and its going to use TCP or udp layer and then its going to go ip header ,.what about ipv6 , you are going to have ipv6 header and related header and the orig ip header and then the data in the data destination header will be encrypted and every time destination comes after authentication or after es header its not going to come before that's the order and it will become like a payload for the ESP and the payload of the esp will be encrypted that's why im encrypting destination extension header of ipv6 and the rest , red part is representing that im providing confidentiality and the blue part and the rest of the data is authenticated if you select authentication option if you don't select authentication option so they will be no authentication this is for transport mode and in that everything looks ok , but in tunnel mode it is going to be the basic for VPN, im going to have new ip header as some body has to carry my header ,, im going to have the firewall address of the destination header so the destination address not the dest address of the receiving client tan the ESP header with the original ip header this is the actual header to that we are going to use in the actual header which is the actual recipient of this packet, and TCP data and esp , you see everything is encrypted including my ip header im providing full confidentiality of my ip header that is the important thing for the tunneling mode and VPN and you are going to have connecting and machine but the original ip address is going to be encrypted and the data as well you can easily use public encryptions now as no one can see your data and no one can use the original ip address so full protection , this is for ipv4 ,for ipv6 new ip header, ext header , ESP header ,orig ip header ext header TCP ,data ESP trailer all encrypted im providing encryption for the original ip address ,orig ip version 6 header in the same way im going to transfer this message by using by any public network no one can play with my data and no one can treat content of my data and this is called VPN and when you have those kind of things what you are doing is you are using esp in tunnel mode this is the definition and it is changing for VPN ,this encryption part is SSL encryption and I f they are using SSL for confidentiality of this data its going to be called SSL VPN and this is called SSL VPN and now im going to talk about VPN and these kind of stuffs, imagine you have form SA for al these stuffs , its going to be hell It does require client installation for every machine and every for every user and if you are using VPN it is web based and its SSL and it's a big advantage and that's why this IPSec is getting decreasing in today's commercial world , and it is replaced in SSL and still IPSec is used in military world and in some financial world but this is difficult to implement when you see the definition of IPSec , you are going to say what you are going to do with this.