Combining security association

This is established for AH o r for ESP it is only one way you can have a message and you want to provide authentication for the message and we are going to provide AH, by using one SA but before transmitting you want one encryption for that you need another security Association ,in other words you can process the documents with more than one SA and that's called SA , SA can be implemented either AH or ESP we need to combine SA and it's called security bundle there are 4 cases first one lets say you have local internet and that is connected to internet via router and you are transmit to the router in this local intranet what you are doing is you are having AH SA between these guys and on top o f the ah you are having ESP or first SA I s ESP and second is Ah what we doing is we don't want to deal with the router the routers here have ,it doesn't have any IPSec thing and now what you are going to do is y oar e going to establish security associations for those guys so the SA you are going to establish is between these two hosts if you are using internet if you are transmitting you are definitely using intranet mode because that's going to provide security for your data, in other words upper is going to be your security but inner it could be AH this is the first case, this time imagine local host doesn't have any IPSec capability the routers are the firewalls for the network what you are going to do, you don't have to establish SA between the network , you are going to apply SA between firewalls this firewalls are going to establish connection between internet and in between ESP tunnel will be the major thing and that's how you will have vpn every body will have VPN , third case everybody will have capability you IPSec and every router is a firewall, network router is a firewall if that the case you are going to face this between these two gateways these are the general structure that you are going to use here but I must tell you guys in IPSec, I have worked a lot in military in there they are using this In commercial world as I said you don't have to depend on the client, the size is big it is a very big deal to install the client to every machine what we are doing is behind the firewall there is no IPSec but between firewall there will be ipsc this is the commercial application of vpn and this is the military application , but the other thing is sometimes you are not member of local internet ,you are getting some kind of security from ip the network you are in you are directly connected to this host and you don't know this guy basically that is called personal vpns we can have security application with vpn we don't have any router so these packets are used for that thing if they are using that kind of thing that means you are using personal vpn and case 4 you are using gateways and between host and gateways directly connected to internet and host and this host ,the destination and the endpoint is firewall of the destination network it may have more than 1 security available in the internet if it is more than one security esp may be AH in the circle definitely sa will be tunnel SA, so when you go to ESP you are going to use tunnel mode you are using AH or esp , generally this tunnel mode is ESP for this inner one is defined relation ship between these two host , but this tunnel is define te relationship between host and destination file because you are transmitting the data on internet, this way we are nesting the SA although we defining SA for only one protocol you can use more than one protocol esp in tunnel mode, esp in transport mode authentication in tunnel mode actually we have 4 , you may say its six as ESP comes with AH option , but to use all of those you have to use established SA, that is the deal how we are going to do that I will tell you later ,everything we told but we dint say the key issue ,t eh key distribution things , lets have a look at it.

Key management

It will be a manual key management ,generally it's the case in military application they are using local internet but in commercial network you may have automated key management it will come with two protocols Oakley and ISKMP so lets have a look at these two protocol

Oakley protocol

Oakley is key exchange protocol based on diffehell man key exchange it is going to use differ hel man add features to address differ hellman what Is there features man in the middle attack we are going to exchange those keys to avoid those things and its going to use cookies it is very important , groups global ,nonce ,this group defines which type of diffehellman they are using and they are going to have ecc diffehellman and it is going to define key size and modular size for this kind of global parameters and are called groups there are 4 or 5 groups for the dife helman and they are going to use nonce to avoid replay attack but there are 1 thing in differ hell man is this some one may impersonate the somebody information with source information , this is going t be legitimate im not a legitimate user and im going to send this to whoever is dealing with key exchange and this guy is going to keep trying to calculate the the key for IPSec protocol im going to send cookies im going to send groups info and different nonce and every time Im going to send this info to the server so the server is going to be overwhelmed with my request so the server is very busy in calculating the keys remember the server of diffehell man will take time, this is called clogging attacks or what you are doing is you are clogging the server so that it will so busy that to calculate the is Diffe Hellman this to avoid this clogging attack Oakley comes wit the concept of cookies , cookies are going to another parameter like nonce its will show that these requests come from this user and it is going to avoid impersonation so that the calculation of cookies will require destination , between source and destination what we are going to do is this we are going to hash the source and destination ip address along with tcp port and we are going to ad d a secret local generated secret by two entities so hashing the source address and destination address and tcp host is going to be used as cookies so im going to send my address with cookie so destination is going to verify the cookie, if its going to verify the cookie it can understand that this is coming from legitimate user ,because cookie is using a legitimate an d the secret so then no oen can forge it , so this is the Oakley protocol ,, initiator is sending the cookie ,calculating the cookie and putting the cookie over there and it is going to change message types and there are message types and I will explain it after iskmp is going to definer the message type whatever the group or ephemeral diffe Hellman or normal difehelman in oter words we are exchanging the information by exchanging the parameters and difehelm any group with key size and everything because when you define the diffehelman you should define the primitive route not the primitive route but generated points the curves are defined by standard descriptive points and with this groups they are giving the standard those things and something telling us that we have this parameter for this things, either it could be diffehelman or ECC differ helman , remember diffehel man key exchange they are exchanging public key exchange so e to power x public key of initiator is going to placed over there along with g , and then this EHAO, this is encryption hash authentication function offered im saying hmac and I want to use triple des , do you thing it will use this things ,Im going to use mac calculations if you don't support those algorithms you are not be able to authenticate or verify those packages so im offering something most probably in response im going to get selected and destination will provide options not just one option but options Im supporting md5 sha1 and im also

supporting sha1 ,3des CAST , I will ask destination which one is good and destination will reply that md5 sha1 is good, and im selecting 3des with three different keys and aes with 256 bit key size then im negotiating it and nidp indicates that this id is not using this message and this id are the id of into and this initiator nonce and initiator of none and id of the key and everything and algorithms offered is signed , in cse the signature x is using the private key so initiator of the private is used to sign this message so im exchanging the diffehelman parameters by signing it that means there will be no main then middle attack first the initiator will check the cookie why hashing the source and destination and port address that is shared between the source and destination if the cookie is ok then the cookie is shared between legitimate nonce where is the nonce this nonce must be new because people may replay this with nonce im going to avoid replay attacks and with cookies im going to avoid clogging attacks , so no one can make the responder busy to calculate the differ hellman keys because this guy received the g^x and this is going to do he is going to raise it to the private key and it is the public key and in crypto anyway for short responder is going to check the cookies and he is going to look at the ids and everything and then its going to prepare its own cookie and all the parameter sorter there except g^x and instead of this he is sending g to power y and it is the public key info of the responder as they have to send the public key and then both of the m are going to raise there public key and result is going to be there private key dn they are going to use basically and that is dfie helman key exchange and algorithms are secreted here and then its going to sign and signature includes received public key info so that initiator can understand that responder uses everything correctly there is no modification and then it is going to send the cookie back and its says the desire key and im agreed with your offer or selection s o they are agreeing and they are signing incoming public key a so that means responder can understand and initiator can understand everything correctly now they have the key what is the size of the key ?..if depends on that size of group of dfife hellman you are using because it is going to define modulus and form that you are going to say first time its 128 bits and first 256 bits for aes and second is for the hmac calculation so the size of the key si huge and you can select whatever you need from that selection the important thing is this im going to send cookie im going to send group or something but I don't define anything max of the parameter , you must send the cookie, you must send the initiator id and you must send the public key of the initiate im just defining the parameter to be sent but im not defining how you are going to send this parameter, that is defined by another protocol that is ISKMP, iskmp have a format for everything we exchange ,for example we are going to establish SA and im going to exchange same message type and in this message type you are going to see what kind of message you are going to send which field of the packet format and there is not ways that you can look at every parameter its 5000 pages that is the difficult part of implementation part and im just going to mention something like this is the security association and that's the type and this is transformed using the SA attributes so SA are used in key exchange so its says suppose for key exchange one of the key exchange is differ hellman and it is exchange by using by exchanging message type and nonce are going to go with this message type and signature are going to go with this message type you see we have to go inside each one of them where they have write en the info and in which h format we cannot this kind o f stuff so iskmp is going to do this kind of stuff , delete is one that kind of stuff you re going to remove the SA by using this and the parameter that you are using in Oakley is also going to be defined like this , that is the relation between oakey and iskmp in iskmp initiator cookie is going to be transferred in this field cookie I and responder cookie r are here and then exchange type or whatever the type that we are using like delete,

SA, is going to be used over here flags is encrypted or not message id and length this is the header info of the iskmp and depending on this info I can have this payload, so the payload is defined like this, so by using this right now, I can actually I can define this exchange type , it is basic exchange, identity protection exchange ,authentication only exchange , aggressive exchange and informational exchange ,what they are doing is this initiator is sending SA that means it is negotiating SA that means its using the new SA and that means basic SA agreed upon and right now they establish the SA by exchanging the SA and then key exchange and the id of I is send along with the key exchange authentication and they are generated by the initiator key generator of the responder in other words we are doing the authentication basically and then also Id of the initiator is initiated by the responder so both partied are authentication each other other by id to the id type Key a goes to key a message type al the keys are going to go to there message type and can you see the stuff over there in it ,its difficult and lets say I have id message type im going to have this field 32 ingto2 bit is going to be used and that is going to be placed right here and size is 64 bits and there will be crc amd error check mechanism and this is the format of Id packet message exchange and when I say id_i then we are exchanging some information over there like this that kind of definition valid for everything , that's defined in iskmp mean type if you curious you can look into the details but there are 1000 of message types and there is no implementation of IPSec which fully comply the whole specification of IPSec it is that kind of complex protocol they are always implementing with so limited version and identity protecting mechanism what Im doing is im negotiation SA with the nonce but key exchange is going to go tot eh nonce and id are authenticated is a slightly different version , here I use the same but when the authentication ask me I have to send to the responder while im negotiating SA im also negotiating the responder and the responder is negotiating the id of me ,so you may say that it seems that you can send everything in one so that's why it is called aggressive so you are negotiating SA and you are creating the ,keys and then you are sending to the nonce so that there will be no replay attacks and you are sending $ID_{I,}$ so this guy will send id_r well be authenticated and this is optional and it will be authenticated by the responder that is the initiator and this is the standard used in IPSec and can be used in any one of them there are some advantage and disadvantage , like if you look at here number of packets that you are transmitting is not that much but here there 6 transmission that is coming and going and here it is 2 transmission and here the contents of the message are higher compared to this guy in other words any one of them can be used to negotiate the essays to create the keys and to send the nonce and everybody will be having and carrying the iskmp header and everyone will be defined in message type and that is the relationship between Oakley and iskmp, Oakley will say change the parameters and iskmp will say if you want to change parameters then you want to send info in this type so that is the idea.