There are a lot of different error messages you can get when trying to set up or troubleshoot an IPsec tunnel. These messages can be pretty cryptic, this guide is meant to help understanding the most common error messages and how you can troubleshoot them.

When troubleshooting IPsec tunnels there is primarily a console command called "ikesnoop" (with verbose mode) that you will use in order to see the negotiations between the initiator and terminator. It is also when using this command you will in most cases see the various error messages that can appear depending on the problem with the tunnel.

The 5 most common error messages are:

Error message-1: could not find acceptable proposal / no proposal chosen
Error message-2: Incorrect pre-shared key
Error message-3: Ike_invalid_payload, Ike_invalid_cookie
Error message-4: Payload_Malformed
Error message-5: No public key found
Problem symptom-1: The tunnel can only be initiated from one side.
Problem symptom-2: Tunnel is unable to establish, Ikesnoop reports CFG mode XAuth problem.

Error message-1: Could not find acceptable proposal / no proposal chosen

Explanation: This is the most common error message. It means that depending on which side that initiates the tunnel, replies that the negotiation of either IKE or IPSec phase of the tunnel failed since they were unable to find a matching proposal that both sides can agree on.

Troubleshooting:

Troubleshooting this error message can be quite extensive since the reasons for this message can be multiple depending on where in the negotiation it fails.

If the negotiation fails in phase-1 – IKE.

The IKE proposal list does not match. Double check that the IKE proposal list matches that of the remote side. A good idea is to use the "ikesnoop verbose" command in the console and get the tunnel to initiate from the remote side. Then you will be able to see what proposals the remote side is sending, then you can compare the results with your own IKE proposal list.
At least ONE proposal has to match in order for it to pass phase-1. Don't forget that the lifetimes are also important as will be mentioned in Problem symptom-1. Note: In newer versions it is not possible to set the lifetime in KB for the IKE Phase, only seconds.

If the negotiation fails in phase-2 – Ipsec.

The IPsec proposal list does not match. Double check that the IKE proposal list matches that of the remote side. You can use the same method described above of using an ikesnoops from when the remote side initates and compare it against your own proposal list. Whats "extra" in the Ipsec phase is that the networks are negotiated here, so even if the Ipsec proposal list seem to match the problem may be with mismatching networks. The Local network(s) on your side needs to be Remote Network on the other side and vice versa. Remember that multiple networks will generate multiple IPsec SA's, one SA per network (or host if you use that option). The defined network size is also important to have exactly the same size on both sides, as will be mentioned in Problem symptom-1.

There are also some settings on the IPsec tunnel's IKE tab that can be involved in a no-proposal chosen issue. Such as Main or Aggressive mode, DH Group (for the IKE phase) and PFS (for IPsec phase).

Error message-2: Incorrect pre-shared key (PSK)

Explanation: A problem with the pre-shared key on either side causes the tunnel negotiation to fail.

Troubleshooting:

This is the easiest one of all the error messages since it can be only one thing, and that is incorrect pre-shared key. Double-check that the pre-shared key is of the same type (Passphrase or Hex key) and correctly added on both sides of the tunnel.

Another reason why it detects that the pre-shared key is incorrect could be because the wrong tunnel is triggering during tunnel negotiations. IPsec tunnels are processed from the top to the bottom and are initially matched against the remote gateway. An example is if you have a roaming tunnel that is ABOVE your currently defined tunnel. A roaming tunnel uses all-nets as its remote gateway and this tunnel will trigger before your defined tunnel due to that. Example:

Name, Local Network, Remote network, remote gateway.
VPN-1 Lannet Office1Net Office1GW
VPN-2 Lannet Office2Net Office2GW
L2TP IP_Wan All-nets All-nets (or <none>)
VPN-3 Lannet Office3Net Office3GW

Since L2TP is above the VPN-3 tunnel it will match before VPN-3 because of the remote gateway. And since they use different pre-shared keys you will see the "incorrect pre-shared key" as error message. Moving VPN-3 above the L2TP tunnel will solve the problem in this case since it will then correctly match the Office3GW gateway and then trigger the VPN-3 tunnel.

Error message-3: Ike_invalid_payload -> Ike_invalid_cookie

Explanation: The IPSec engine in the Security Gateway receives an IPSec IKE packet but is unable to match it against an existing IKE.

Troubleshooting:

If the tunnel is only up on one "side", this can be the resulting error message when traffic arrives from a tunnel that does not exist. An example would be if for some reason the tunnel has only gone down from the initiator side but the terminator still sees it as up. It then tries to send packets thru the tunnel but when they arrive on the initiator it will drop them since no matching tunnel can be found.

Simply remove the tunnel from the side that believes it's still up to solve the immediate problem. An investigation as to why the tunnel only went down from one side is recommended. It could be that DPD and/or Keep-Alive is only used on one side. Another possible cause could be that even though it has received a DELETE packet, it has not deleted/removed the tunnel. This _should_ not happen.

Error message-4: Payload_Malformed

Explanation: This problem is very similar to Incorrect pre-shared key as a possible reason is that the PSK is of the wrong TYPE on either side (Passphrase or Hex key).

Troubleshooting: Verify that you are using the same type on both sides of the IPsec tunnel. If one side is using Hex and the other Passphrase, this is most likely the error message that you will receive.

Error message-5: No public key found

Explanation: This is a very common error message when dealing with tunnels that use Certificates as authentication.

Troubleshooting: Troubleshooting this error message can be very difficult as the possible cause(s) of the problem can be quite extensive. Also it is very important to keep in mind that when dealing with Certificates you may need to combine the Ikesnoop logs with normal logs as ikesnoop does not give that much information about Certificates, while normal logs can provide you with important clues as to what the problem could be. A good suggestion before you start to troubleshoot Certificate tunnels is to first configure it as a PSK tunnel and then verify that it can

successfully establish, then move on to using Certificates. (Unless the configuration type prohibits that).

Possible cause-1: The Certificate on either side is not signed by the same CA server.
Possible cause-2: The Certificate's validity time has expired or it has not yet started to be valid. The latter can happen if the clock is set incorrectly on either the CA server or the Clavister.
Possible cause-3: The Clavister is unable to reach the Certificate Revocation List in order to verify if the Certificate is valid or not. Double-check that the CRL path is valid in the Certificate properties. (Assuming you want to use CRL as this can be turned off)
Make sure that there is a DNS client configured in the Clavister in order for it to correctly be able to resolve the path to the CRL.
L2TP Note: Vista tries by default to contact and download the CRL list, while XP do not. This option can be turned off in Vista.
Possible cause-4: If multiple similar or roaming tunnels exist and you want to separate them using ID lists, a possible cause can be that none of the ID lists are matching the Certificate properties of the connecting user. Either the user is non-authorized or the Certificate properties are wrong on the Client or the ID list needs to be updated with this user/information.
Possible cause-5: (L2TP) The client Certificate is imported into the wrong Certificate store on the Client(Windows). When the client connects it's using the wrong Certificate. More information on how to correctly import the client Certificate can be found in the How-To : "Setting up a L2TP Server using Clavister Security Gateway with Microsoft CA server issued certificates".

Problem symptom -1: The tunnel can only be initiated from one side.

Explanation: This is a fairly common problem; the reason is due to a mismatch of the size in network on Local or Remote and/or the lifetime settings on the proposal list(s).

Troubleshooting: To troubleshoot this you need to examine the Local Network, Remote Network, Ike proposal list and IPsec proposal list on both sides to try locate the miss-matching problem.

To best describe the problem and how to solve it, please see this example:

Site-A
Local Network = 192.168.10.0/24
Remote Network = 10.10.10.0/24
Site-B
Local Network = 10.10.10.0/24
Remote Network = 192.168.10.0/16

In this scenario you will see that the defined Remote Network on Site-B is larger than what is defined on Site-A's Local Network. This means that Site-A can only initiate the tunnel successfully towards Site-B as its network is smaller. When Site-B tries to initiate the tunnel Site-A will reject it as the network is bigger than what is defined. The reason it works the other way around is because a smaller network is considered more secure and will be accepted. This applies for the lifetimes in the proposal lists as well.

Problem symptom-2: Tunnel is unable to establish, Ikesnoop reports CFG mode XAuth problem.

Explanation: The reason for this message is basically "No proposal chosen". The case where this will appear is when there is something that fails in terms of network size on either Local Network or Remote Network. Since the Core has determined that it is a kind of network size problem, it will try a last ditch attempt to get the correct network by sending a CFG mode request.

Troubleshooting: By using Ikesnoop when both sides initiates the tunnel you should easily be able to compare the network both sides are sending in phase-2, and with that information be able to spot the network problem. It can be that it's of the wrong size or that it doesn't match at all.

End of document.