



Service Managed Gateway™

Debugging VPN

Issue 1.1
Date 14 August 2007

1	Introduction	3
1.1	Core VPN Concepts	3
1.2	Apply and Bypass Policies	3
2	The Trace Analyzer	5
3	Guidelines for debugging a VPN	6
3.1	Initiator and Responder	6
3.2	Bringing up a VPN	6
3.3	Trace Messages.....	6
3.4	Order of events	7
4	Configuration Issues	8
4.1	Issue: Connection to peer available, no negotiations take place.....	8
4.1.1	Fix: VPN Capabilities not enabled on local or remote end	8
4.1.2	Fix: Pre-shared key is incorrect size:	8
4.2	Issue: Main Mode Message one is sent but there is no reply	8
4.2.1	Fix: Remote Peer not configured	8
4.2.2	Fix: Difference in Exchange Types	9
4.3	There is a response to Main Mode Message one but it is not Main mode .	9
4.3.1	Fix: DH Groups on IKE policy mismatch.....	9
4.3.2	Fix: IKE Policy Encryption Algorithms are wrong	10
5	Main Mode Messages	11
5.1	Messages 1–4	11
5.2	Messages 5 and 6: failure to complete Main Mode	11
5.2.1	Pre-shared keys not matching.....	11
5.3	Difference in Group ID in SPD configuration parameters.	12
5.4	Difference in Encryption Algorithms settings on SPD or Difference in Addresses in SPD APPLY Policies	13
5.5	Security Protocol does not match in SPD	14
5.6	ESP Authentication set to 'no' on one side of the tunnel	14

1 Introduction

This is a very brief introduction to the concepts that lie behind a Virtual Private Network. Users who have not worked with a VPN before should refer to the VPN Application Guide before proceeding with this manual.

1.1 Core VPN Concepts

The purpose of a VPN is to set-up a secure tunnel between two subnets through which protected data may pass. There are several terms and concepts which the user should be familiar with when debugging a VPN problem. There follows a brief introduction to some fundamentals of Virtual Private Networks.

The set-up of a VPN is a two stage process. Each stage in turn has a number of steps that must be completed in a chronological fashion. The first stage of negotiation can be one of two modes: Main Mode, which is a six stage process or Aggressive Mode which is a three stage process. Main Mode is a more secure process but requires more information to set-up and takes longer to complete. Once either Main or Aggressive mode has completed then the second stage of negotiations takes place. This stage is known as Quick Mode and is a three stage process.

For the negotiations to complete successfully both Authentication and Encryption must complete. In that, each end of the secure tunnel must ensure that the far end is a bona fide peer and also that the data that is being passed is correctly encrypted.

Before set-up of a VPN it is essential that both sides of the VPN are configured accordingly, meaning that if a particular parameter is configured on one side it must be configured in precisely the same manner on the far side.

1.2 Apply and Bypass Policies

Policies are used to configure a VPN. There must be a policy present for the first mode of negotiation (Main or Aggressive) and there must also be a policy present for the second Mode (Quick) of negotiation. It is within these policies that the user configures all the relevant parameters.

Before data is presented to the Routing table of an SMG it will be checked against the what is know as an SPD (Secure Policy Database) list to check that there is a corresponding policy matching this data's characteristics, i.e. it's source and destination addresses and so on. If there is no corresponding entry for a particular packet it will be dropped and never presented to the Routing table.

If there is a problem encountered within the negotiations, parameters within these policies will require investigation.

When setting up a VPN it is worth noting that there should be a policy set-up which will accommodate all data passing through the router that is not destined for the far end of the tunnel. This policy will allow the data pass from the local

side of the Router out to any other destination beyond the router without the need for encryption.

NOTE:

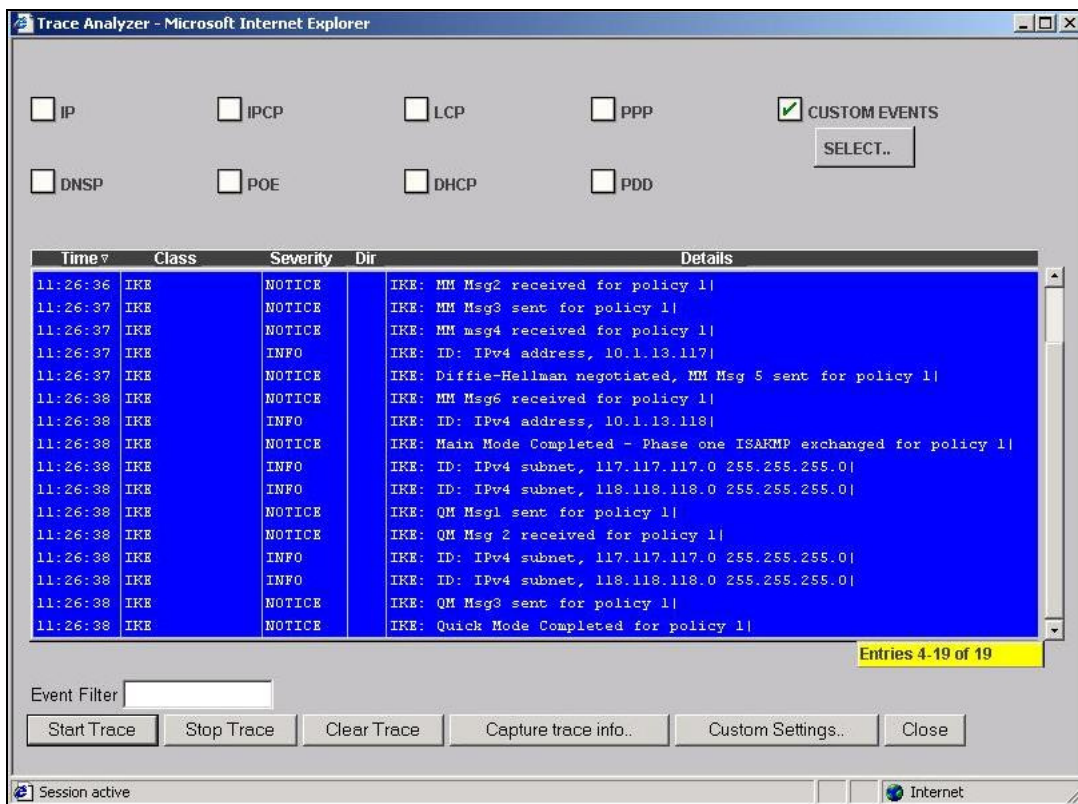
It is assumed throughout this document that such a policy exists, as it will be necessary to connect remotely to the remote side of the VPN through an unsecured channel from time to time to debug certain problems.

2 The Trace Analyzer

In order to view the negotiations progressing the user must employ the use of the Trace Analyzer. This is a diagnostics tool which enables users view packets leaving the Router in real time. It is also a mechanism to view any events which are generated, these event messages are often the best route to finding the cause of a poorly configured set-up.

The user can access this tool via: **Advanced>Diagnostics>Trace Analyzer.**

In order to view VPN negotiation the user must select custom events. Throughout this manual the user will be prompted to use this tool. Every time this tool is referenced in this manual the user should select 'IKE' from the custom list and 'add'. Having done so the user may then select 'Start Trace' this will cause all events and messages related to VPN negotiations to be recorded in the Analyzer/.



3 Guidelines for debugging a VPN

3.1 Initiator and Responder

It is possible to configure the SMG as either an initiator or a responder. The initiator is the side of the tunnel that starts the negotiations. The responder is the side that responds. The SMG can be configured to be both an initiator and a responder. If the SMG is configured to act solely as a responder then it will never attempt to send the first message of negotiations even if the packet is destined for the correct remote subnet.

However if the response type is set to 'initiator' or 'both' then it is assumed that the SMG is attempting to send the first message of Main or Aggressive Mode. This can be viewed under :

Expert View>System>VPN>SPD1-50> Index X> Secure Gateway.

3.2 Bringing up a VPN

To bring up a VPN (to complete the full set of negotiations) all that is required of the user is to pass data from the specified subnet (usually the local LAN) to the far specified subnet. On receiving the first packet with the specified destination the SMG will automatically commence negotiations with the remote side. There will be a slight delay as these negotiations take place, but after approximately five seconds data should be passing seamlessly to the user.

If this does not occur there is an issue with the VPN configuration and debug measures using the trace Analyzer should be undertaken.

3.3 Trace Messages

Throughout this manual there will be examples of traces taken while negotiation takes place. One such message can be seen below:

```
IKE    DEBUGIKE: Could not find ISAKMP SA
```

The above shows that the SMG did not have a current active tunnel set for the data being passed (Could not find ISAKMP) and therefore should attempt to initiate the VPN negotiations.

3.4 Order of events

There are some general rules that apply to debugging a VPN. As has been stated in the VPN Application guide there are three policies generated on a Serviced Managed Gateway for every VPN used, two SPD policies, and one IKE policy. The Apply SPD policy and the IKE policy are both used in the VPN negotiation process. Bearing in mind that the VPN negotiation is a two step process the following rule is a good starting point with respect to finding the cause of the problem.

If an error occurs in the first stage of negotiations there may be an issue with the IKE policy being used. If there is a problem encountered in the second stage (Quick Mode) there may be an issue with the SPD Apply process.

This manual will now go on to deal with specific configuration problems and direct the user towards a possible solution to each problem.

4 Configuration Issues

4.1 Issue: Connection to peer available, no negotiations take place.

4.1.1 Fix: VPN Capabilities not enabled on local or remote end

If no IKE messages are generated on the Trace Analyzer the user should first ensure that there are VPN capabilities enabled on both ends of the tunnel, this can be checked under:

Expert View>System>VPN>System> IKE Enabled.

If this is not set to 'yes' then the Serviced Managed Gateway is not capable of sending or replying to any VPN negotiation packet.

4.1.2 Fix: Pre-shared key is incorrect size:

There are circumstances which may lead to Main Mode message 1 not being sent even if IKE capabilities are set. A series of checks are carried out by the SMG to ensure that the parameters set are valid for VPN negotiations, if certain criteria are not met then negotiations will not take place.

A set of the following messages from the Trace analyzer would be symptomatic of this:

```
IKE  04  DEBUGIKE: Could not find ISAKMP SA|
IKE  04  DEBUGIKE: Could not find ISAKMP SA|
IKE  03  NOTICE      IKE: Deleting SA for policy 0|
```

One such problem is in the length of the pre-shared key used. The minimum length of the key is determined by the Authentication Algorithm used, there are two types of algorithm available, MD5 or SHA, if MD5 is selected then the pre-shared key must be a minimum of 16 characters long, if SHA is employed then a minimum key length of 20 characters must be used.

4.2 Issue: Main Mode Message one is sent but there is no reply

4.2.1 Fix: Remote Peer not configured

A case which may often arise is that the remote Peer may not be configured to accept VPN negotiations. If this is the case then there will be no reply received whatsoever to Main Mode Message one. If this is the case the following trace may be seen:

Initiator

```
IKE  DEBUGIKE: Could not find ISAKMP SA
IKE  NOTICE      IKE: MM Msg1 sent for policy 1
```

There is no response to this message by way of Main Mode message 2 being received. At this point it is best to ensure that there is connectivity to the remote peer. The user should start a ping not destined for the remote LAN but for the Remote Peer (The gateway address). If this Ping times out then there is a connectivity problem between the two nodes that needs to be resolved.

(This is assuming a valid "bypass all" policy is configured on the Serviced Managed Gateway)

4.2.2 Fix: Difference in Exchange Types

If connectivity is confirmed to the remote side and the user is certain that there are VPN capabilities enabled on both sides there may be an issue with differing exchange types.

One side of the tunnel may be configured to negotiate a Main Mode connection, but the other side is configured for Aggressive Mode. The trace below is symptomatic of this:

Initiator

```
IKE 04  DEBUGIKE: Could not find ISAKMP SA|
IKE 04  DEBUGIKE: Could not find ISAKMP SA|
IKE 04  DEBUGIKE: ID: IPv4 address, 10.1.13.118|
IKE 04  DEBUGIKE: AM Msg1 sent for policy 1|
```

Responder (set for main mode)

```
IKE 04  DEBUGIKE: Messages have differing exchange types|
IKE 04  DEBUGIKE: Failed to process packet received by IKE|
```

4.3 There is a response to Main Mode Message one but it is not Main mode

message two

(The following applies to Aggressive mode also)

If there is a problem in the first stage of negotiations in Main Mode or Aggressive Mode, there is an issue in the IKE policy

Several of these issues will lead to Main Mode message one being sent out by the SMG and getting received and recognized on the far side. However on receiving the packet on the far end the remote peer discovers some anomaly between the two configurations. This will lead to

4.3.1 Fix: DH Groups on IKE policy mismatch.

The DH Group (1 or 2) is a parameter employed by the DiffieHellman algorithm which is used in negotiations from Main Mode 1 to 4.

This parameter must match on both sides of the tunnel, if it does not then the following may be seen on the Trace Analyzer:

Initiator

```
IKE  04  DEBUGIKE: Could not find ISAKMP SA|
IKE  04  DEBUGIKE: MM Msg1 sent for policy 1|
IKE  04  DEBUGIKE: Informational Exchange message received|
IKE  03  NOTICE      IKE: Deleting SA for policy 1|
```

Responder

```
IKE  04  DEBUGIKE: MM Msg1 received for policy 1|
IKE  04  DEBUGIKE: IKE Attribute group did not match|
IKE  04  DEBUGIKE: Could not select an ISAKMP proposal|
IKE  03  NOTICE      IKE: Failed to process first message of main mode|
IKE  03  NOTICE      IKE: Deleting SA for policy 1|
IKE  04  DEBUGIKE: Failed to process packet received by IKE|
```

To remedy this issue make sure the DH Group on both sides of the VPN tunnel match.

4.3.2 Fix: IKE Policy Encryption Algorithms are wrong

This is an issue which will cause Main Mode message one to be received but the remote end will not reply with Main Mode message two.

Initiator

```
IKE  04  DEBUGIKE: Could not find ISAKMP SA|
IKE  04  DEBUGIKE: MM Msg1 sent for policy 1|
IKE  04  DEBUGIKE: Informational Exchange message received|
IKE  03  NOTICE      IKE: Deleting for policy 1|
```

Responder

```
IKE  03  NOTICE      IKE: MM Msg1 received for policy 1|
IKE  04  DEBUGIKE: IKE encryption algorithm did not match|
IKE  04  DEBUGIKE: Could not select an ISAKMP proposal|
IKE  03  NOTICE      IKE: Failed to process first message of main mode|
IKE  03  NOTICE      IKE: Deleted ISAKMP SA|
IKE  04  DEBUGIKE: Failed to process packet received by IKE|
```

5 Main Mode Messages

5.1 Messages 1–4

If Main Mode messages one and two are successful then there is a very high possibility that messages three and four will also be successful.

This is due to the fact that after message two has been received both sides of the tunnel are satisfied with the initial parameters that have been configured are correct. At this point the DiffieHellman algorithm is carried out which will lead to a level of encryption being agreed on between both ends of the tunnel. This encryption is then carried out on the packets which follow which are used for Authentication purposes (Be it pre-shared keys or certificates).

The following message is generated when Message four has been received:

```
IKE 04   DEBUGIKE: MM msg4 received for policy 1|
IKE 04   DEBUGIKE: ID: IPv4 address, 10.1.13.117|
IKE 04   DEBUGIKE: Diffie-Hellman negotiated, MM Msg 5 sent for policy 1|
```

5.2 Messages 5 and 6: failure to complete Main Mode

5.2.1 Pre-shared keys not matching

Having completed Diffie-Hellman negotiations the authentication process must take place immediately and this involves the passing and verification of the Pre-Shared Keys. From the point of view of the Initiator this process will work okay as it simply sends Main Mode Message 5.

However on the receiving side an error will be generated on if the Pre-Shared keys do not match. The message generated will look as follows:

Responder

```
IKE 04   DEBUGIKE: Diffe-Hellman negotiated, MM Msg5 received for policy 1|
IKE 04   DEBUGIKE: Invalid Payload|
IKE 01   ERRORIKE: IkeMMProcessIDMsg : IkeCheckPayloads failed
```

The responder will now send a message back to the initiator detailing this event. This message will read as Main Mode Message 6 when it is received by the initiator but the following message will be generated also;

Initiator

```
IKE 04   DEBUGIKE: MM Msg6 received for policy 1|
IKE 04   DEBUGIKE: Encryption bit not set|
IKE 04   DEBUGIKE: Failed to process packet received by KE
```

If this occurs then the user should re-enter the pre-shared keys on both ends of the tunnel.

Quick Mode Failure

Having completed Main or Aggressive Mode successfully the negotiations will progress automatically to Quick Mode, at this stage any issues which the user may run into will normally arise from a mis-configuration between the two SPD Apply policies being used.

NOTE:

There are similarities in most of the symptoms listed below, all the below will require scrutiny of the SPD apply policies

5.3 Difference in Group ID in SPD configuration parameters.

The following are the debug commands seen in this scenario:

Initiator

```
IKE 04  DEBUGIKE: QM Msg1 sent for policy 1|
IKE 04  DEBUGIKE: Informational Exchange message received|
```

Responder

```
IKE 04  DEBUGIKE: QM Msg 1 received for policy 1|
IKE 04  DEBUGIKE: ID: IPv4 subnet, 102.102.102.0
255.255.255.0|
IKE 04  DEBUGIKE: ID: IPv4 subnet, 103.103.103.0
255.255.255.0|
IKE 01  ERRORIKE: IkeSelectX form : Mismatch in PFS in policies or group
descriptors|
IKE 01  ERRORIKE: SelectIpSec Proposal : No matching proposal found|
IKE 04  DEBUGIKE: Unable to find a valid IPSEC proposal|
IKE 04  DEBUGIKE: Failed to process packet received by IKE|
```

The Group parameter is set under Advanced Options for a given SPD Apply policy

5.4 Difference in Encryption Algorithms settings on SPD or Difference in Addresses in SPD APPLY Policies

When Quick Mode Message 1 is received by the responder it will always state the Subnets which are set in the packet it received, this is useful as it will mean that verification of SPD Subnet Addresses is easy.

Initiator

```
IKE 03 NOTICE IKE: QM Msg1 sent for policy 1|
IKE 04 DEBUGIKE: Informational Exchange Message Received|
```

Responder

```
IKE 03 NOTICE IKE: QM Msg 1 received for policy 1|
IKE 06 INFO IKE: ID: IPv4 subnet, 118.118.118.0 255.255.255.0|
IKE 06 INFO IKE: ID: IPv4 subnet, 117.117.117.0 255.255.255.0|
IKE 03 NOTICE IKE: Could not match Encryption Algorithm|
IKE 01 ERRORIKE: No matching set of attributes found for the matching
proposal
IKE 01 ERRORIKE: SelectIpSecProposal : No matching proposal found|
IKE 04 DEBUGIKE: Unable to find a valid IPSEC proposal|
IKE 04 DEBUGIKE: Failed to process packet received by IKE|
```

5.5 Security Protocol does not match in SPD

Initiator

```
IKE 04  DEBUGIKE: ID: IPv4bnet, 118.118.118.0 255.255.255.0|
IKE 04  DEBUGIKE: ID: IPv4bnet, 117.117.117.0 255.255.255.0|
IKE 04  DEBUGIKE: QM Msg1 sent for policy 1|
IKE 04  DEBUGIKE: Informational Exchange message received|
```

Responder

Note the difference between this configuration problem and the previously mentioned issues with SPD parameters is that the subnets are correct and there is no message about the Encryption Algorithm.

```
IKE 03  NOTICE      IKE: QM Msg 1 received for policy 1|
IKE 06  INFO          IKE: ID: IPv4 subnet, 118.118.118.0 255.255.255.0|
IKE 06  INFO          IKE: ID: IPv4 subnet, 117.117.117.0 255.255.255.0|
IKE 01  ERRORIKE: SelectIpSecProposal : No matching proposal found
IKE 04  DEBUGIKE: Unable to find a valid IPSEC proposal|
IKE 04  DEBUGIKE: Failed to process packet received by IKE|
```

5.6 ESP Authentication set to 'no' on one side of the tunnel

Initiator

```
IKE 04  DEBUGIKE: QM Msg1 sent for policy 1|
IKE 04  DEBUGIKE: Informational Exchange message received|
```

Responder

```
IKE 03  NOTICE      IKE: QM Msg 1 received for policy 1|
IKE 06  INFO          IKE: ID: IPv4 subnet, 118.118.118.0 255.255.255.0|
IKE 06  INFO          IKE: ID: IPv4 subnet, 117.117.117.0 255.255.255.0|
IKE 01  ERRORIKE: IkeSelectXform : Auth defined in ESP of SPD but not in
proposal
IKE 01  ERRORIKE: SelectIpSecProposal : No matching proposal found
IKE 04  DEBUG          IKE: Unable to find a valid IPSEC proposal|
IKE 04  DEBUGIKE: Failed to process packet received by IKE|
```

NOTE:

If the responder is the SMG with the mis-configuration then the debug messages will manifest themselves as in the previous case where the

Security protocol did not match, as in there is the error message referring to the matching proposal and the two debug messages.