Application Note

Connecting Networks with ePipe

A Simple Site to Site VPN

Contents

1 Introduction

This application note provides an example of how to configure a simple two site VPN using a pair of ePipe gateway units with ePipe's Multilink IP (ML-IP) technology. ML-IP includes the E2B (End to End Bonding) technology in previous versions of ePipe software/firmware.

ML-IP allows an IPSec based VPN tunnel to be established between two networks that are connected to the Internet. The advantage of using an ML-IP tunnel over a standard IPSec tunnel is that ML-IP multilinks (bonds) together several low cost Internet connections at one or both sites to provide more bandwidth for inter-site traffic. This provides scalable bandwidth for the VPN tunnel using dial-up (PSTN or ISDN), ADSL or router based connections.

2 The SSV Feature Set

The ML-IP (E2B) and IPSec technologies are included in an optional Feature Set of the ePipe called Site to Site VPN (SSV). As of firmware version 2.3.0, limited support for E2B based IPSec tunnels (E2B-IPSec) is included free of charge. This allows up to two (2) client side and two (2) server side E2B-IPSec tunnels. This is sufficient for a two site VPN.

If you require more E2B-IPSec tunnels then you will need to purchase the SSV Feature Set, which will increase the number of tunnels to 16 client side and 50 server side tunnels. The easiest way to obtain Feature Set Activation Keys is by following the instructions on the Feature Set Registration Card, which you will have received when you purchased the SSV Feature Set. Alternatively, use a web browser to browse to the Setup page of the ePipe Management Assistant (web-based user interface of the ePipe) and click on the icon to the left of the Feature Set name and follow the instructions to enable a Feature Set.

The ePipe Management Assistant refers to the inbuilt web server of the ePipe, which provides setup wizards, status information and help, allowing easy configuration of the ePipe. Simply use your favorite web browser (that supports JavaScript) and enter the IP address of the ePipe in the address or URL field. Browse to Setup and then click on the icon to the left of the SSV Feature Set. Take the appropriate action according to the icon you see, from the table below.

	Feature Set is activated and available for setup. Simply click on the Setup Wizard option to the right of the Feature Set name.
	Feature Set is activated for a limited number of tunnels. Applies to the SSV and SRA Feature Sets ONLY. Applies to ePipes running version 2.3.0 or later firmware ONLY. Click on the icon to fully activate this Feature Set, once you have obtained an Activation Key. Click on the Setup Wizard option to the right of the Feature Set name to start setup.
	Features Set is temporarily activated in DEMO mode ONLY. This Feature Set will be enabled for a period of 21 days, after which the permanent Feature Set will need to be purchased. Click on the icon to permanently activate this Feature Set, once you have obtained a Permanent Activation Key. Click on the Setup Wizard option to the right of the Feature Set name to start setup.
	This Feature Set is inactive. An Activation Key will need to be obtained to activate this Feature Set. DEMO and Permanent Activation Keys are available. Permanent Activation Keys can be purchased from your supplier. Click on the icon to activate this Feature Set, once you have an Activation Key. Setup cannot commence until the Feature Set has been activated.

NOTES:

1. Each Feature Set Activation Key is generated from the MAC address of a specific ePipe unit and will not work on any other ePipe.
2. On ePipe models with more than one Ethernet port, the address of Ethernet 1 must be used. This is the lowest of the MAC addresses.

3. On ePipe ServerWare models all feature sets are activated by default.
4. After you "activate" a Feature Set, the ePipe will restart. Approximately 30 seconds later you will be returned to the ePipe Setup page. The status of the feature sets should now reflect the addition of a new feature (or features). If not then repeat the process of activating the feature, as the most likely reason for the activation failing is a mistake during key entry. Also ensure that the key supplied is for this ePipe and that the MAC address is correct.

3 Connecting to the Internet

Before starting the setup of the E2B-IPSec Site to Site VPN, ensure both ePipes are connected to the Internet. This will involve creating an Internet Connection Bundle and Links for each ePipe. To setup a bundle, browse to the ePipe Management Assistant and navigate to *Setup* > *SIA Setup Wizards* > *Shared Internet Access* and follow the prompts. For more information, please refer to the ePipe User Documentation.

This Application Note only covers the process of configuring a Site to Site VPN. When configuring an E2B-IPSec tunnel, the following notes are important to remember:

- One end of the tunnel is setup as the "server" end, while the other is setup as the "client" end. The server end ePipe must have at least one static or fixed IP address, which needs to be connected to the Internet and online any time the E2B-IPSec tunnel needs to connect.
- There should not be any device performing NAT (Network Address Translation) between the ePipes. If this is unavoidable, it may be possible to work around the problem, depending on the capabilities of the device doing NAT – contact ePipe Technical Support (mailto:support@ml-ip.com) for further assistance.
- You will need to allow E2B (TCP port 2000) through the filters on both ePipes – incoming traffic allowed on the server end ePipe, outgoing on the client end ePipe. This allows the encrypted packets to be transmitted through the ePipe firewall.

4 VPN Design

Before configuring an E2B-IPSec tunnel, it is important to design the VPN and assign IP addresses to the VPN and each network (if necessary). In the ePipe documentation on http://www.ml-ip.com/, there are two documents that should prove useful during the design stage, the "Site to Site VPN Worksheet" and the "Site to Site VPN Design Template". We recommend these worksheets be completed before configuring the ePipes. The worksheets are available from the following URLs:

- Site to Site VPN Worksheet
  http://www.ml-ip.com/html/userdoc/epipe/epipe-ssv-worksheet.pdf
- Site to Site VPN Design Template
  http://www.ml-ip.com/html/userdoc/epipe/epipe-ssv-design-template.pdf

When designing the VPN, you will need to make decisions about IP addressing and security settings. IP addresses need to be allocated to avoid conflicts (between individual addresses and networks). Security settings need to be chosen based on your needs for performance and security. More information about how to choose these addresses and algorithms is in the SSV documentation on ePipe's website.

This application note will use network addresses as in Figure 1 (below).

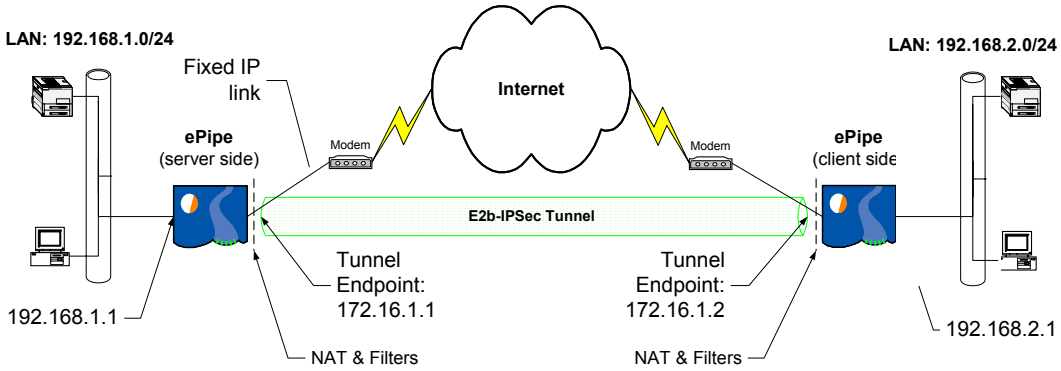

Figure 1 - Example network showing IP addressing.

In the above example, we are connecting two networks that have the addresses 192.168.1.0/24 and 192.168.2.0/24 respectively. It is important to note that while the specific address ranges being used are arbitrary, the two sites do need to be on separate IP networks. To connect the two, we have a VPN tunnel running over a single modem connection (this could be any form of connection or multiple connections in other situations, this application note is focused only on the setup of the VPN itself). Each site has a single public IP address for the modem connection, and one (the server side) needs to be a static or fixed IP address, for the client side to connect to. The tunnel will connect ePipe to ePipe, providing a way for the networks to route internal traffic to each other securely, bypassing NAT and filters on both ePipes. IPSec encrypts and authenticates the packets for transmission across the Internet. This tunnel has end-point IP addresses which allow the ePipes to route traffic to and from the internal networks – these IP addresses should be from one of the private address ranges and should be from a subnet that is not used anywhere else in the network. In this example, the end-points of the tunnel were assigned the IP addresses 172.16.1.1 and 172.16.1.2.

In this example, the security algorithms used will be Blowfish for encryption and SHA-1 for authentication. These algorithms provide a high level of security while maximizing performance.

5 Configuration

5.1 Configuring the Server Side of the Tunnel

To setup the server side of the E2B-IPSec tunnel, perform the following steps. (These steps assume that you already have the ePipe set up with an operational Internet Connection Bundle, and have incoming E2B allowed through your filter.)

1) Go to *Setup* > *SSV Setup Wizards* > *Site to Site VPN (IPSec with E2B)* (in pre-2.3.0 firmware) or *E2B-IPSec Site-to-Site VPN* (in 2.3.0 firmware or later versions).
2) Select 'Use an existing Internet Connection Bundle' and select the bundle you wish to use for the VPN tunnel. Click *Next*.
3) Select *Server Side* and click *Next*.
4) Enter a *Tunnel Name* (e.g. "**tunnel1**"), a *Local Address* of **172.16.1.1**, and a *Remote Address* of **172.16.1.2** (assuming these addresses are not in use in your network and have not been used for any other tunnel). The *Group Name* is used for grouping tunnels together on the Advanced > Summary page and is optional. We will leave this field blank. Click *Configure*.
5) Enter **192.168.2.0** in the first *Network Address* text box, and **255.255.255.0** in the first *Subnet Mask* text box. Click *Next*. This step sets up the routing for

the tunnel by specifying the network/s that are on the other side of the tunnel (as viewed from this ePipe).

6) You have now reached the security settings page. The following items will need to be provided:
   a) SPIs
      Enter a unique number for each SPI. In this instance, type "**1001**" in the *Local SPI* text box, and "**1002**" in the *Remote SPI* text box.
   b) Encryption
      In the *Encryption* section, change the *Algorithm* drop down box to **Blowfish**. Type in some encryption keys in the spaces provided. When using Blowfish, your key should be at least 80 characters in length.
   c) Authentication
      In the *Authentication* section, change the *Algorithm* drop down box to **SHA-1**. Type in some authentication keys in the spaces provided. When using SHA-1, your key should be at least 100 characters in length.
7) Click *Configure*.
8) Ensure that the correct bundle is selected for use by the VPN, and click *Start VPN Now*.

5.2 Configuring the Client Side of the Tunnel

As in the previous section, these instructions assume that you have a working Internet Connection Bundle already set up and ready to use on the ePipe at this site.

1) Go to *Setup > SSV Setup Wizards > Site to Site VPN (IPSec with E2B)* (in pre-2.3.0 firmware) or *E2B-IPSec Site-to-Site VPN* (in 2.3.0 firmware or later versions).
2) Select '*Use an existing Internet Connection Bundle*' and ensure that you also have selected the bundle you wish to use for the VPN tunnel. Click '*Next*'.
3) Select '*Client Side*' and click '*Next*'.
4) Enter a '*Tunnel Name*' of "**tunnel1**" (this must be the same name as used on the server side), and the '*Fixed IP*' of the server side ePipe's connection to the Internet. Click '*Configure*'. The '*Group Name*' is a purely cosmetic parameter to aid in maintenance of a large number of tunnels in one ePipe, so in this instance it can be left blank.
5) **[2.x.x firmware only]** Select '*Don't use a Traffic Filter*' and click '*Next*'.
6) Enter the address of the network you wish to connect to by typing **192.168.1.0** in the first '*Network Address:*' text box, and **255.255.255.0** in the first '*Subnet Mask*' text box. Click '*Next*'.
7) You have now reached the security settings page. The following items will need to be provided:
   a) SPIs
      Enter a unique number for each SPI. In this instance, type "**1002**" in the *Local SPI* text box, and "**1001**" in the *Remote SPI* text box. Note that these values are the reverse of those used on the server side of the tunnel.
   b) Encryption
      In the *Encryption* section, change the *Algorithm* drop down box to **Blowfish**. Type in some encryption keys in the spaces provided. These keys must be the same as those entered in the other ePipe, but in reverse, i.e. Local key becomes the remote key and vice versa.
   c) Authentication
      In the *Authentication* section, change the *Algorithm* drop down box to **SHA-1**. These keys must be the same as entered in the other ePipe but with the local key swapped for the remote key.

NOTE: The keys and SPIs on the client side of the tunnel are the reverse of those on the server side – i.e. the remote keys and SPIs on the client side are the same as the local keys and SPIs on the server side and vice versa. Ensure you don't have any spaces on either end of the strings. The best way to transfer these is to copy and paste them. If these keys do not match exactly then the tunnel will not connect.

8) Click '*Configure*'.
9) Ensure that the correct bundle is selected for use by the VPN, and click '*Start VPN Now*'.

6 Testing and Troubleshooting

E2B connection problems are usually due to tunnel configuration issues.

6.1 Tips for configuring E2B tunnels

The following tips may help when configuring an E2B tunnel:

- The tunnel name needs to be the same on both ends.
- Tunnel names must not match the name of any existing bundle or link.
- Local and remote IP addresses for the tunnel must not overlap any subnet addresses in use elsewhere in the WAN.
- Ensure the gateway setup contains the IP addresses of the networks at the other end of the tunnel.
- Ensure the local and remote SPIs, encryption keys and authentication keys are reversed at the other end of the tunnel
- Ensure the encryption and authentication algorithms are the same on both ends of the tunnel.
- Ensure the tunnel is connected, using the *Status* > *Raw Stats* > *SSV* screen on both ePipes. If the tunnel cannot connect and all parameters are OK, try to ping the Fixed IP address of the tunnel from the client side ePipe – if this doesn't work, you need to check the connections at both ends. (Make sure ping (ICMP echo and echo reply) is allowed through the filters on both ePipes.)

6.2 Troubleshooting Tunnel Communication Problems

If you cannot get data to travel across the tunnel, follow the steps below:

1) Test communication from the original host to the final destination host using the ping command.
2) If 1 fails, test reachability by doing a ping from the local ePipe to the remote ePipe (from the CLI).
3) If 2 works but 1 fails, check the routing table on both hosts and on the ePipes using the CLI command:

   SHOW INTERNET GATEWAY

4) If 1 & 2 both fail then the problem is between the ePipes.
5) Check the tunnel by doing a ping to the remote IP address of the tunnel. If this works then the tunnel is working. The problem may be the gateway setup. Check the configuration of the gateways for each tunnel.

Other things to check include:

- Check the default gateway on PCs and other hosts. In simple networks, the default gateway of the PCs should be set to the internal IP address of the local ePipe.
- Remember that many routing problems are due to the destination host not knowing how to reply to a packet. Check the routing table of the destination host to ensure it knows how to route packets back to the source network.

7 Conclusion

A VPN is a cost-effective way of creating a WAN between two or more sites. ePipe allows you to establish secure IPSec tunnels between sites using multiple Internet links at each site to transport the tunnel traffic. This technology is part of Multilink IP (ML-IP) and is referred to as End to End Bonding (E2B).

One of the most important parts of setting up a site-to-site VPN is designing the VPN and assigning the IP addresses. By using the design templates and the ePipe Management Assistant, setting up a VPN should be relatively simple.

Further information about ePipe can be obtained from the ePipe web site (http://www.ml-ip.com/). See the support section for user documentation and further assistance.

INFORMATION CONTAINED IN THIS DOCUMENT (referred to as an Application Note) IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND BY EPIPE, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

The user assumes the entire risk as to the accuracy and the use of this Application Note. This Application Note may be copied and distributed subject to the following conditions:

1) All text must be copied without modification and all pages must be included.

2) If software is included, all files on the disk(s) must be copied without modification.

3) All components of this Application Note must be distributed together.

4) This Application Note may not be distributed for profit.

Copyright (C) 2002 ePipe. All Rights are Reserved.

For further information, contact ePipe by sending email to support@ml-ip.com, quoting the name of this paper in the subject header.

Document Number: AN-EP-005 First Edition: December, 2001

Keywords: VPN IPSec E2B WAN ML-IP Multilink This revision: September, 2002