Application Note

Configuring the ePipe Firewall:
Basic Filters

Contents

1 Introduction

With small to medium business (SMB) and small office home office (SOHO) business increasingly using 'always on' broadband Internet connections or permanently connected dial-up connections, it is becoming more important to protect a PC or network from malicious attack. A common and effective method of securing a PC or network is to use a firewall between the PC or network and the connection to the ISP.

A firewall is a means by which a network can be secured against external attack, whilst also limiting internal users access to a public network like the Internet. By using the firewall within ePipe ePipe, a network may be secured against certain external attacks whilst also preventing unauthorized access by a third party outside of the Local Area Network (LAN). This feature should be used when the ePipe is the gateway for the LAN to the Internet or other public network. This Application Note will go through the process of setting up the firewall in the ePipe gateway for users requiring access to the Internet and email using common applications.

2 Firewalls

2.1 What is a firewall?

Firewalls are used to prevent unauthorized access both out of the network to the Internet and from the Internet into the network. A firewall implemented correctly can help to protect a network from intruders whilst also limiting the types of traffic allowed out of the LAN to the Internet. Without a firewall implemented, a network is open to a wide variety of malicious or damaging external attacks.

2.2 How does the ePipe firewall work?

ePipe's firewall is made up of two components:

1. A packet filter
2. Network Address Translation (NAT)

ePipe gateways use a packet filter which bases its filtering on TCP and UDP port numbers or traffic (protocol) types. Individual filter rules are combined into an ordered list called a filter rule set. Each packet that then passes across the Internet connection, whether it is incoming or outgoing, is then matched against the list of filter rules. If no match is found, the packet is discarded. If a match is found, the packet obeys the rule.

NAT is a process that modifies the IP addresses of packets as they pass through the ePipe's Internet connection so that the packets appear, to the Internet, as if they come from the ePipe rather than the PCs on the private LAN. NAT is used so that the private LAN does not need globally unique IP addresses for each PC and, instead, can use a private range of IP addresses. This conserves the number of globally unique IP addresses being used on the Internet. NAT has the effect of hiding the details of the private LAN from the Internet and also prevents inbound traffic reaching PCs on the LAN since their IP addresses are unknown. Therefore NAT provides an important measure of protection from external attack.

NOTE:	NAT by itself is not considered to be a sufficient security mechanism of firewall without some form of packet filtering being used to control the passage of packets through the firewall.

This application note covers the process of filter design and implementation. NAT is not covered in this application note.

3 Design and Implementation

With filter design, careful consideration should be given to the requirements of the network and the way in which those requirements are to be implemented. Setting a policy for traffic allowed both out of and into the network is a good idea and this can be the basis for the filter implementation. This policy can then be implemented as individual filter rules in the filter rule set. The ePipe gateway firewall, once configured, discards all traffic for which there isn't a rule in the ruleset.

3.1 Filter Design

Filter design is the process of determining what traffic types need to pass through the firewall and in which direction the traffic originates. For example, to allow a user to browse the World Wide Web, the HTTP protocol needs to be allowed through the firewall. Since the connection from the PC on the LAN to the web server on the Internet originates from the LAN, the HTTP traffic needs to be allowed out of the network. Traffic can also be allowed into the network and traffic can be allowed in both directions. Traffic can also be rejected or discarded silently by the firewall.

In many circumstances, all that is required for Internet access is to allow the pre-defined filter rules called "Common Internet Access" out of the network. The 'Common Internet Access' rules include:

- HTTP (normal web page traffic)
- HTTPS (secure web page traffic)
- FTP (a protocol used primarily for file transfers)
- DNS (resolves Internet names (e.g. www.stallion.com) to IP addresses)

Almost every office uses email, so specific email rules will need to be added to this list. To add the correct rules, it is important to understand how the mail server or PCs on the LAN receive mail.

Almost all email is sent using SMTP, so SMTP will need to be allowed OUT of the network. Mail servers generally receive external mail via SMTP or fetch it from another mail server using one of the POP protocols. If email is forwarded to the user's mail server directly, SMTP is being used and this will need to be allowed both INTO and OUT of the network in the filter rules. If the mail server is configured to 'pop' mail from a server on the Internet (usually at the ISP), then POP3 (or in some cases POP2) will need to be allowed OUT of the network.

Many other traffic types are listed in the ePipe Management Assistant (the web based user interface of the ePipe). If additional traffic types need to be allowed through the ePipe gateway firewall, other than the rules listed above, firstly consult the Appendix in this document for a full list of all traffic types currently included in the ePipe Filter Wizard (with a brief explanation). If the traffic type is not in this list then the Advanced Rule option will need to be used to allow this traffic through the ePipe firewall. Consult the ePipe documentation and the filter tutorial available in the ePipe Management Assistant for more information.

3.2 Filter Implementation

Filters should be implemented using the Filter Wizard in the ePipe Management Assistant. This can either be accessed as a part of the Shared Internet Access (SIA) wizard or else by clicking on Advanced, then Filters in the ePipe Management Assistant. Once the wizard has been started, please follow the following steps to create the traffic filter:

1. Give the filter a meaningful name like "officefilter" then click *Next*
2. Click on *Add Rule*

3. In the box which says *Select Traffic Type*, choose *Common Internet Access*
4. In the box below, change the traffic to be *Allowed out of internal network*
5. Leave the rest of the settings as default and click *Next*

These 5 steps have implemented rules for Internet access. The following rules must be implemented for email access, the first set (6a through to 11a) if email is received using POP3, the second (6b through 9b) if email is received using SMTP:

6a. Click on *Add Rule*

7a. Select *SMTP* in the *Select Traffic Type* box. Change the traffic to be *Allowed out of internal network* in the second drop down box, then click *Next*

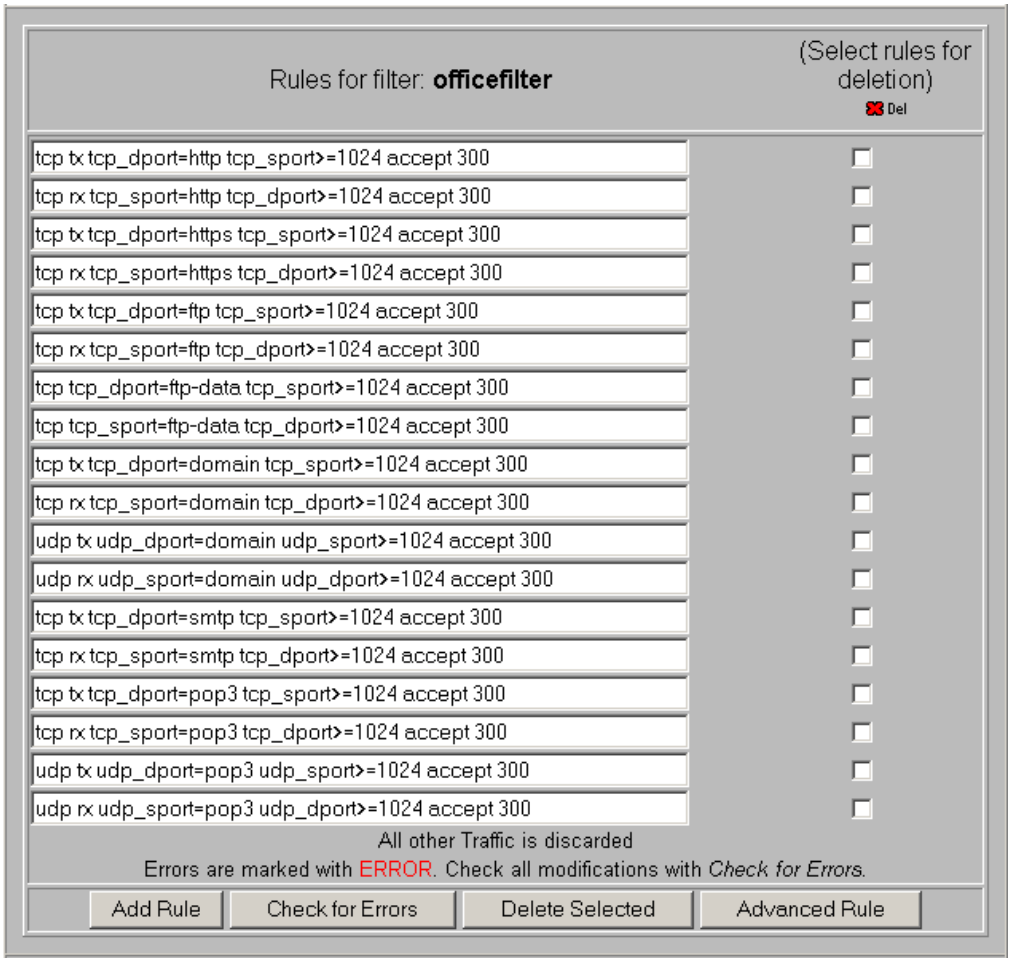
8a. Click on *Add* Rule

9a. Select *POP3* in the *Select Traffic Type* box and choose *Allowed out of internal network*. Click *Next*. The rules for the filter should look like those in Figure 1.

10a. Click on the *Check for Errors* box (even though the rules added here have simply been added using the ePipe Management Assistant, it is a good habit to get into to check the rules for errors).

11a. Configure the changes by clicking on the Configure button on this screen.

Figure 1 – Filter with SMTP and POP3 for email



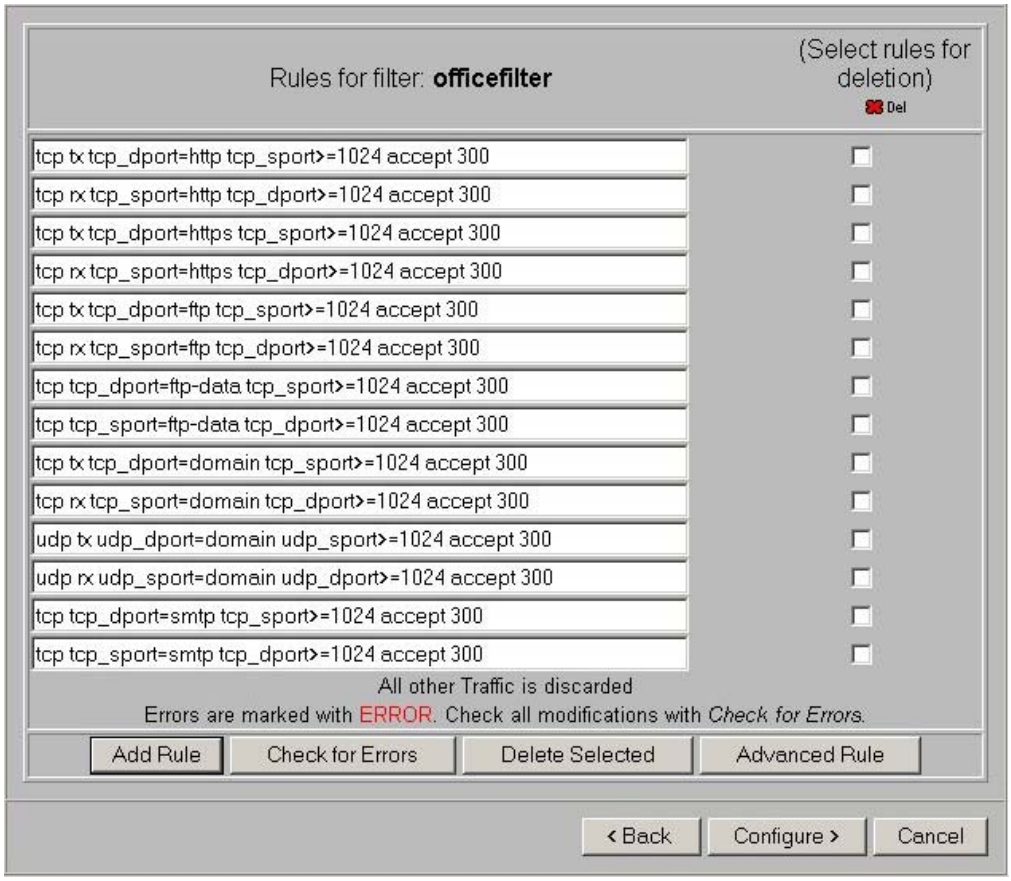
6b. Click on *Add Rule*

7b. Select *SMTP* in the *Select Traffic Type* box. Change the traffic to be *Allowed into/out of internal network* in the second drop down box, then click *Next*. The rules should look like those in Figure 2.

8b. Click on the *Check for Errors* box (even though the rules added here have simply been added using the ePipe Management Assistant, it is a good habit to get into to check the rules for errors).

9b. Configure the changes by clicking on the Configure button on this screen.

Figure 2 – Filter with SMTP allowed both INTO/OUT OF the network



NOTE: If creating a filter by clicking on Filters in the Advanced section of the EPIPE MANAGEMENT ASSISTANT, the filter will need to be associated with the bundle the filter is to be used with. To do this, click on Advanced, then Bundle, then click on the name of the bundle. In this screen, there should be a drop down box below the heading Filter from which the filter that was just created should be selected.

3.3 *Filter 'Rules of Thumb'*

The following list represents some tips or 'rules of thumb' to keep in mind when designing and implementing a filter rule set:

- Make the filter rule set as short as possible – the longer the rule set, the more complex it becomes.
- Order is important. The most used traffic types should always be first in the list. More often than not, this is HTTP, SMTP, DNS and E2B (VPN traffic if a VPN is being used).
- Care should be taken with which traffic types are to be allowed either out of or into the network. Traffic allowed out of the network can still create a security problem – for example the way FTP works means that a filter

allowing FTP out may be able to be exploited by a hacker. It is also worthwhile to be wary of letting other file transfer programs and Internet chat programs through the firewall.
- Extreme care should be taken with all traffic allowed into the network.

4 Testing and Troubleshooting

To test that the filter is working, from a computer on the LAN, attempt to browse to a web site – for example, www.stallion.com. If the filters have been implemented correctly, the ePipe website should appear. This is because HTTP traffic and DNS traffic were allowed out of the network.

If the website doesn't start to load, ensure that there is a connection to the Internet, then remove the filters. This can be done by browsing to the ePipe, clicking on Advanced, then Bundles and the name of the bundle. In the drop down box below the Filters heading, select the "No Filter" option, then configure the bundle. Attempt to browse the web site again.

- If browsing the web site works with the filter removed, compare your filter rules to those in either Figure 1 or Figure 2, make the necessary changes and try to browse the web site again with the filter in place.
- If you cannot browse to the website, try another website. If this also fails, check your Internet connection.

The next step is to test that the filter stops a traffic type that wasn't in the filter list. Ping wasn't included in the list originally so attempt to ping the ePipe website from a command prompt by typing:

ping http://www.ml-ip.com/

If the filter was implemented correctly and the ePipe is currently connected to the Internet, the web address www.ml-ip.com/ should have been resolved to an IP address by DNS (DNS is included in the filter rule list) but the pings time out as in the following example:

```
C:\>ping www.ml-ip.com
Pinging www.ml-ip.com [203.143.238.9] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

This shows that DNS is working but ping, as expected, is not allowed through the firewall, as it was not in the filter rule set.

If the name wasn't resolved to an address, web browsing would not work. Check the Internet connection and DNS settings in both the ePipe and the PCs on the network.

5 Conclusion

A firewall is an important part of any network, likened to an office's front door. Nobody would ever think of leaving their front door unlocked overnight yet many people leave their Internet access unsecured without a second thought. Intrusion using the Internet is stealthy, often un-noticed and potentially more destructive than physical intrusion or break-in. By configuring an appropriate firewall, access to and from the Internet can be locked down at all times, greatly reducing the chance of intrusion or attack.

Care must be taken when allowing traffic into the network, with the realization that a hole is being poked in the firewall. When this is done in combination with a NAT redirect rule, the responsibility for security for that particular port or traffic type is transferred to the device being redirected to. Where possible, avoid allowing any traffic type into the network.

Appendix

Protocol names listed in the ePipe Management Assistant's filter wizard and descriptions:

HTTP

This is the primary protocol used by the World Wide Web. It is used to download HTML pages from servers on the internet.

HTTPS

This protocol is used for secure HTTP access, for example, online banking.

FTP

The File Transfer Protocol is the more traditional method for downloading files on the Internet as compared to HTTP.

PPTP

The Point-to-Point Tunneling Protocol is used to create a client Virtual Private Network to a PPTP server. It is a mechanism to securely connect to another network through the Internet.

SMTP

SMTP is the protocol used for sending e-mail to a mail server. If you wish to send e-mail to an Internet server then you will need to allow this traffic out of your internal network. Likewise, if mail is being sent to a mail server on your LAN, SMTP will need to be allowed into the network.

POP2

This older protocol is now replaced by POP3.

POP3

POP3 is used to retrieve e-mail from a mail server. If you wish to retrieve e-mail from and Internet Service Provider then you may need to allow this traffic out of the network.

IMAP

Internet Message Access Protocol - a method of accessing electronic mail or bulletin board messages that are kept on a mail server.

NNTP

Used to transfer Net News. In order to read News groups you will need to allow this out of your network.

Telnet

Standard terminal style logins across the network.

NetBIOS

The Microsoft networking protocols (Network Neighborhood, etc) – you would not normally want to allow this into the network.

LDAP/ILS

The LDAP (Lightweight Directory Access Protocol.) provides access to X.500 directories.

Microsoft Internet Locator Server (ILS) for NetMeeting expands existing server technology to provide more advanced directory services, higher scalability, and better performance standards (such as LDAP).

DNS

Domain Name Service - this is required to be able to find Internet sites by name, for example 'www.stallion.com'.

RIP

A Routing protocol, you do not normally want to allow this traffic onto the internet.

Ping

A useful method for testing your connections, it sends a message to another computer, which in turn sends a reply to confirm it received the message.

E2B (Port 2000)

This rule allows the default E2B VPN connection traffic to operate. You need to allow this traffic out of your network to establish an E2B VPN connection. If you have customized your E2B Server Port then you will need to create an Advanced Rule to allow this traffic through.

ESP (IPSec)

The encapsulation protocol for IPSec. ESP should be allowed into and out of the network when using IPSec transport for E2B tunnels (TCP is the default). If you are filtering the traffic on a VPN then it is advisable to set the "up-time" for this kind of traffic to zero (0) so that spurious redials do not occur as part of the VPN shutdown process.

IKE (ISAKMP)

Internet Key Exchange (TCP port 500). IKE should be allowed into and out of the network when configuring a VPN using IKE.

Lotus Notes

Using TCP port 1352, this is for use with Lotus Notes Messaging.

MS Netmeeting

Microsoft Netmeeting uses a number of TCP ports – these being ports 389, 522, 1503, 1720 and 1731. To use the audio features of MS Netmeeting, you will need to pass through secondary UDP connections on dynamically assigned ports (1024-65535). Information on how to do this will be in a following section.

Citrix Winframe/Metaframe

Citrix Winframe/Metaframe, otherwise known as ICA, uses port 1494. Allow this through your firewall when using Citrix Winframe on your network.

RealPlayer

Allows RealPlayer through the firewall.

VDOLive

Japanese streaming video player using port 7000.

AOL

Uses TCP port numbers 5190 to 5193. This allows the user to utilize AOL Instant Messenger as well as other features offered by AOL.

PC-Anywhere

Uses TCP port number 5631and UDP port number 5632 – useful for remote PC administration.

L2TP

Layer 2 Tunneling Protocol - Uses TCP port 1701. Used in some VPN devices, particularly Windows 2000.

SSH

Secure Shell, a method for logging into another computer over a network. Uses TCP port 22.

Network Time Protocol

A protocol for synchronizing the time on multiple machines using TCP port 123.

IRC

Internet Relay Chat is a program which is used to participate in discussion groups on the Internet, using TCP port 194.

IP/IP

IP over IP needs to be enabled for any E2B/VPN Bundles that are using a cipher of *NONE*. If you are filtering the traffic on a VPN then it is advisable to set the "up-time" for this kind of traffic to zero (0) so that spurious redials do not occur as part of the VPN shutdown process.

Common Internet Access

Common Internet Access includes HTTP, HTTPS, FTP and DNS. It is designed purely for browsing of the web.

Document Number: AN-EP-007
Keywords: filter firewall security hack intrusion

First Edition: February, 2002
This revision: September, 2002