JEP(S)

Security perimeter white paper

Configuring a security perimeter around JEP(S) with IIS SMTP

Document control

Document name:	JEP(S) Security perimeter
Author:	Proxmea, Proxmea
Last update:	March 23, 2008

Index

Introduction

Having your mail server directly connected to the internet creates a large security risk for your business. Not only do you risk to have your mail system penetrated by spammers and hackers, but you also run the risk of denial of service attacks (DoS) which can render your mail server or whole mail system unreachable for both external as internal users.

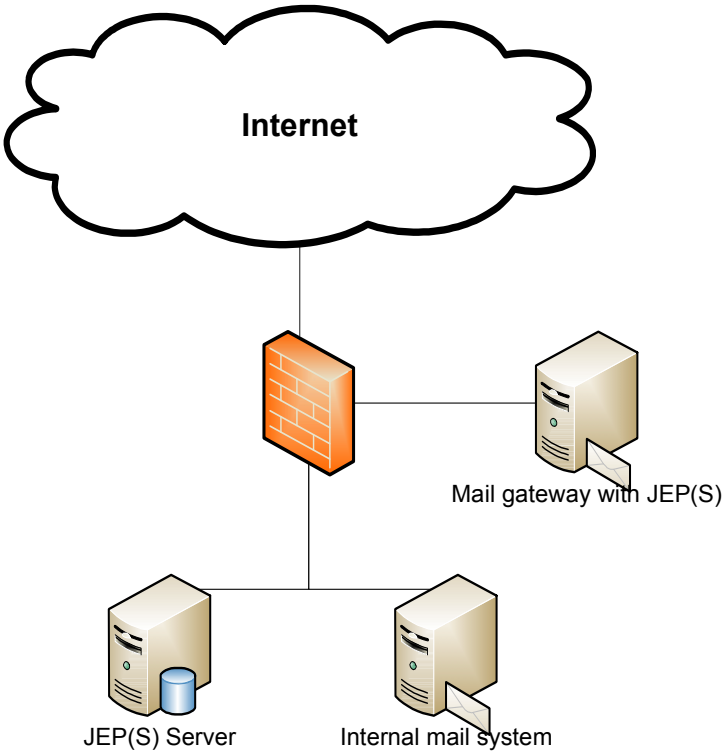
By setting up a security perimeter based on IIS SMTP and JEP(S) which is disconnected from the rest of your network you will move the risk one step away from your critical mail systems. In the case of penetration or a DoS attack of the mail server you will only risk the mail gateway in question and though this will affect the mail flow it won't affect your mail servers.

To set up JEP(S) and a security perimeter network you need:

- A internal server running JEP(S) Server, preferable on a SQL database.
- One or more physical or virtual servers which will be used a mail gateways.
  These servers can run Windows 2000/2003 or Windows XP. (XP comes with IIS SMTP)
  You need .Net framework 2.0 installed on the mail gateway.
- A firewall with a DMZ. (Optional but recommended)
- In most cases you need a JEP(S) license as these connections involve more than one server.

This white paper is intended as a guide into a couple of different setup scenarios for securing your mail network with JEP(S). You might require further knowledge about how firewalls and mail systems work to implement this.

The basics



The above diagram explains the basics of setting up a security perimeter network. This is but one of the many different ways this can be setup and we'll go through many other scenarios later.

The way a mail would be blocked or passed through:

1. A session is initiated from the internet to the firewall on port 25. This session is forwarded to the mail gateway on port 25.
2. JEP(S) intercepts the session and sends a query to the JEP(S) server through the firewall on port 9105.
3. The JEP(S) server inspects the session against its filers and known users (if address sources has been configured) and replies back to the mail gateway with either a pass or block.
4. If the mail gateway receives a block then the session is denied and otherwise the session is accepted. If the session is accepted then it gets delivered to the local mail gateway mail system (IIS SMTP).
5. When the mail has been received by the mail gateway then it delivers it to the internal mail system over port 25.

Outgoing mail goes directly from the internal mail server as this allows us to install the outgoing JEP(S) sink to enable auto whitelisting.

Setting up the basic environment

The JEP(S) Server

Install the JEP(S) server as described in the JEP(S) Administrator guide. You will need to enable listen on all interfaces for the server to accept traffic from the JEP(S) sink on the mail gateway.
To facilitate proper filtration at the mail gateway the email address function of JEP(S) should be used. By using this you give the mail gateway the 'intelligence' of not accepting email if the recipient doesn't exist in your organization.

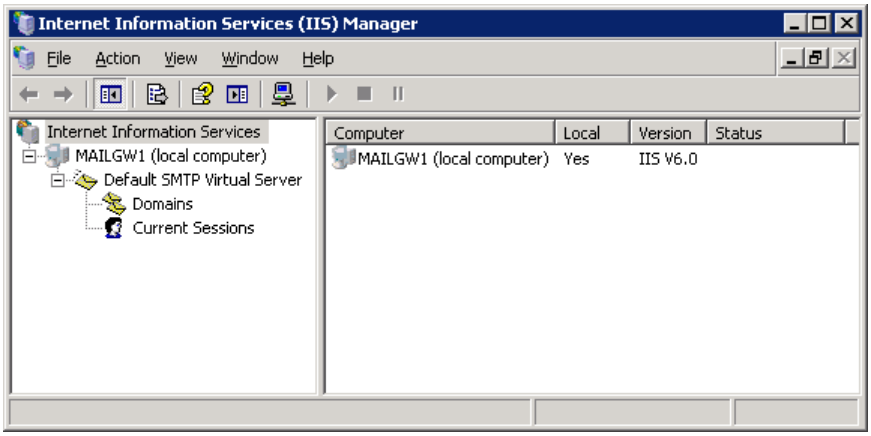
The mail gateway server

You have the choice of running the mail gateway on either Windows 2000,2003 or Windows XP. The reason for XP being in this list is that it does come with the IIS and SMTP components. The only limitation running on XP is that you can only handle 10 concurrent session as default.

Install the SMTP component by opening Add/Remove programs and selecting Add/Remove windows components. Depending on your version of operating system install the SMTP service by either A or B:

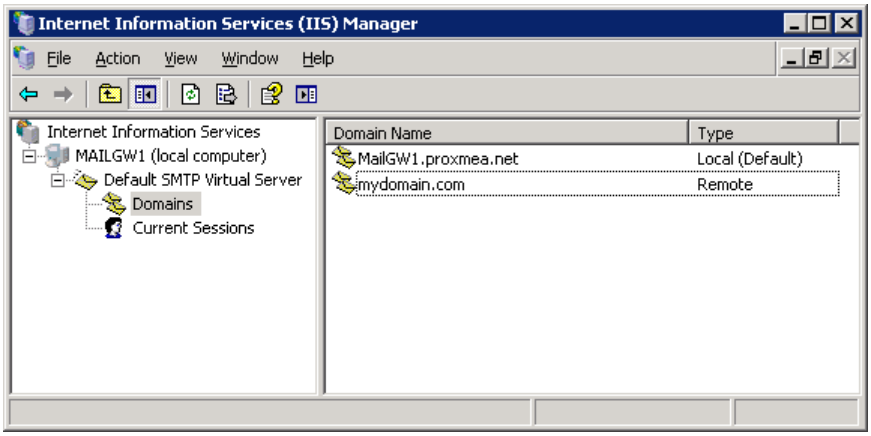
a. Click (not select) Internet Information Services (IIS) and click details
   Select SMTP service and click ok.
b. Click (not select) Application Server and click details.
   Click (not select) Internet Information Services (IIS) and click details
   Select SMTP service and click ok.

1. Open Start menu – Administrative tools - Internet Information Services.

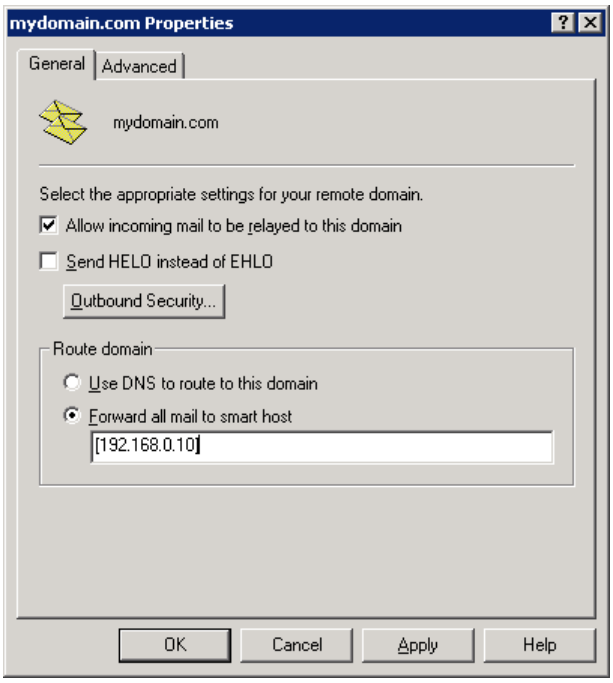


2. Right click Domains and select New – Domain.
3. Select Remote and next.

4. Fill in the domain name you want to receive mail on and press enter.



5. Right click your newly created domain name and select properties.
6. Select Allow incoming mail to be relayed to this domain and fill in the IP number of your internal mail server in the Forward all mail to smart host field.
   Note that you need to enclose the IP within brackets []. When finished press OK.

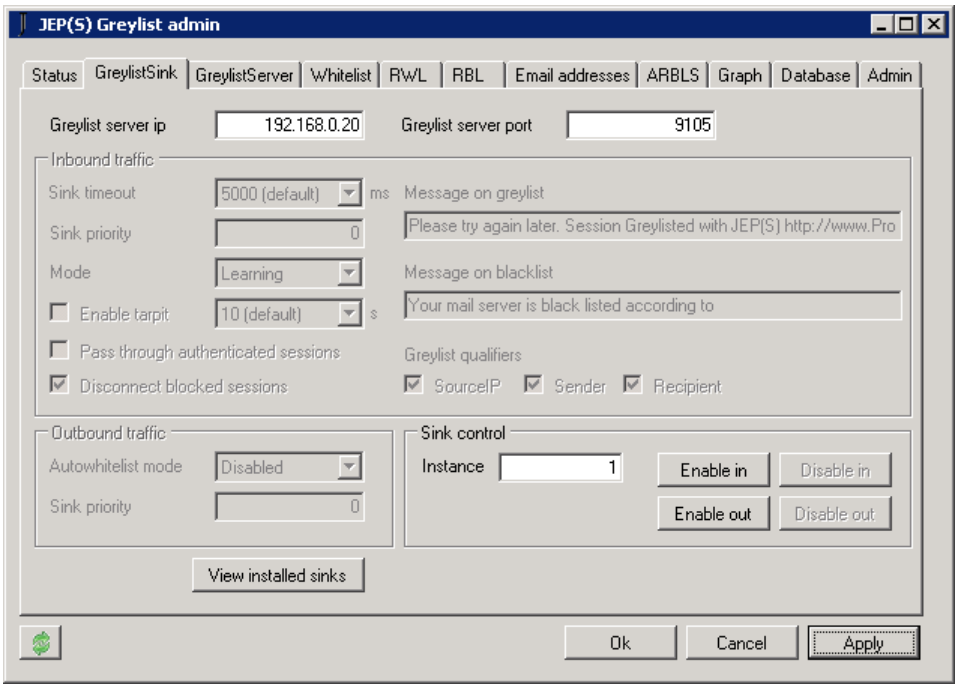


7. If necessary repeat the procedure 2 to 6 for other domain names.

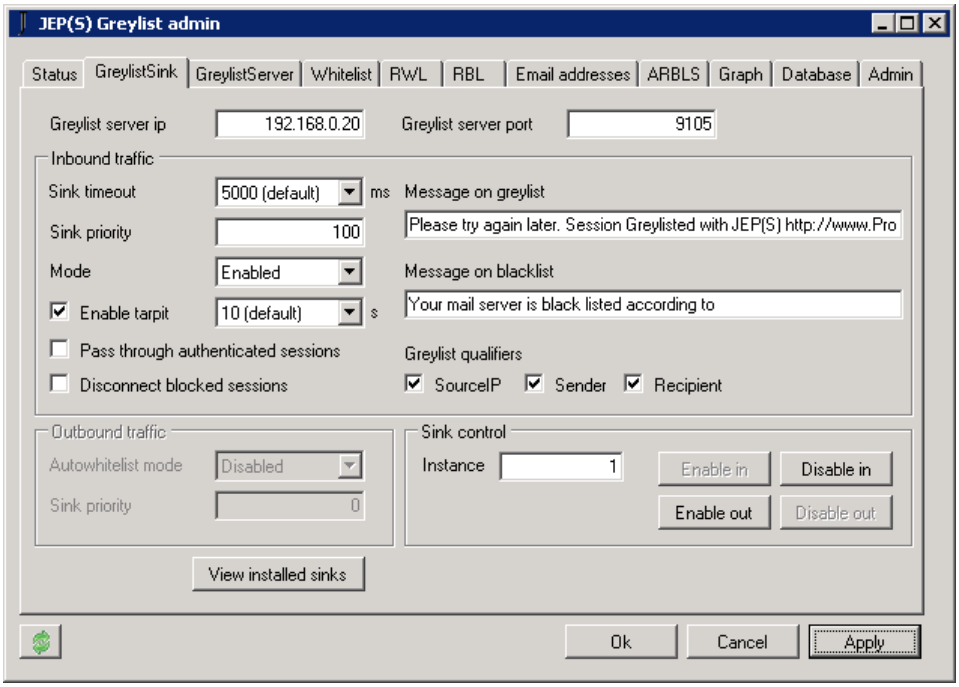
Your mail gateway is now ready to receive mail for your domain but is yet not protected by JEP(S).

8. Extract JEP(S) into a directory of your choice, copy your license file the same directory and then start JEP(S) Admin. Go to the Greylist Sink tab.

9. Change the server IP to the IP of your JEP(S) Server and press Apply.



10. Click Enable in to install the JEP(S) Sink for incoming traffic.
    We won't enable the outgoing sink as this server only handles incoming traffic.
11. Change the following settings and then press Apply:
    a. Mode – Enabled
    b. Disconnect blocked settings – Unchecked
    c. Enable tarpit – Enabled (optional)



The firewall

With the setup just described and assuming that the mail gateway is located in a DMZ you would use the following configuration:

IP's:

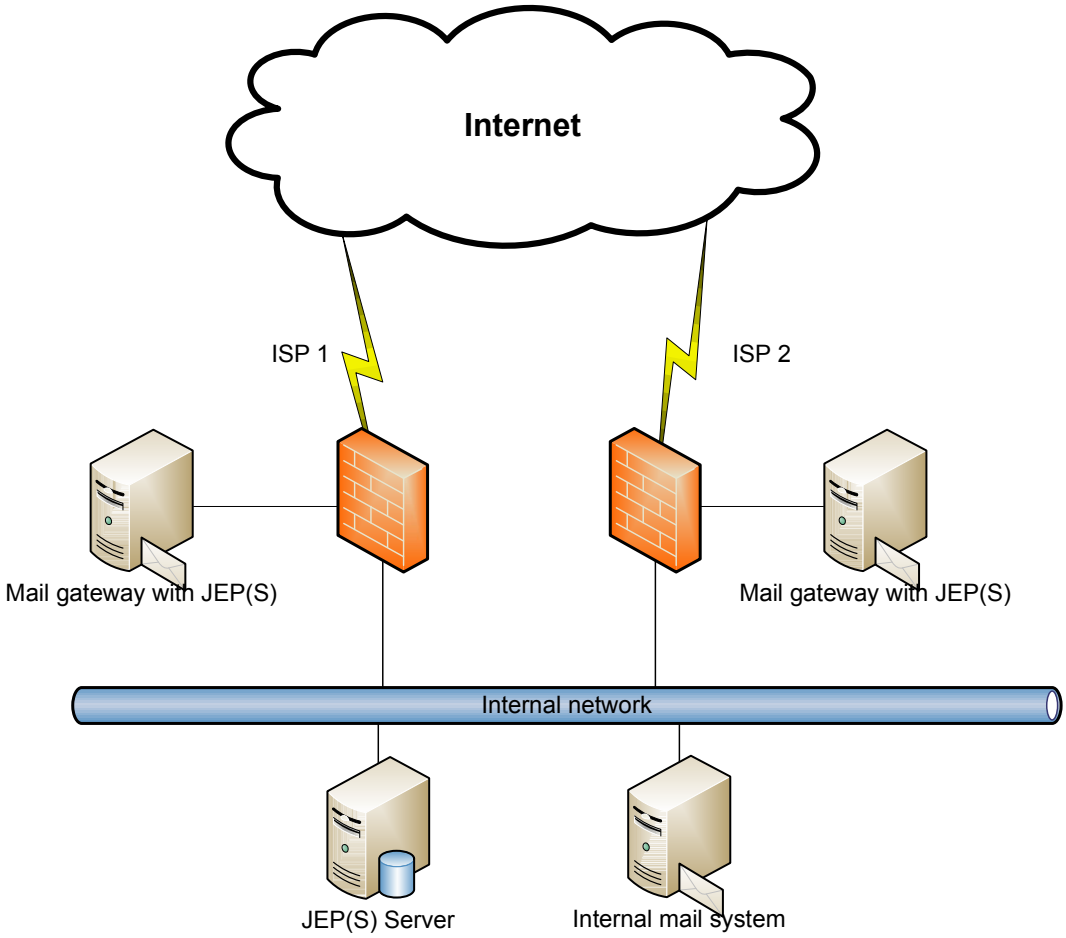
- Mail gateway 10.0.0.100
- Internal mail server 192.168.0.10
- JEP(S) Server 192.168.0.20

Ports that need to be opened:

Any to 10.0.0.100	Port 25 TCP	Incoming mail from the internet to the mail gateway
10.0.0.100 to 192.168.0.10	Port 25 TCP	Mail from the mail gateway to internal mail server
10.0.0.100 to 192.168.0.20	Port 9105 TCP	JEP(S) queries from gateway to JEP(S) server
192.168.0.10 to Any	Port 25 TCP	Outgoing mail from internal mail server to the internet

Scenarios

Redundant mail GW with DMZ

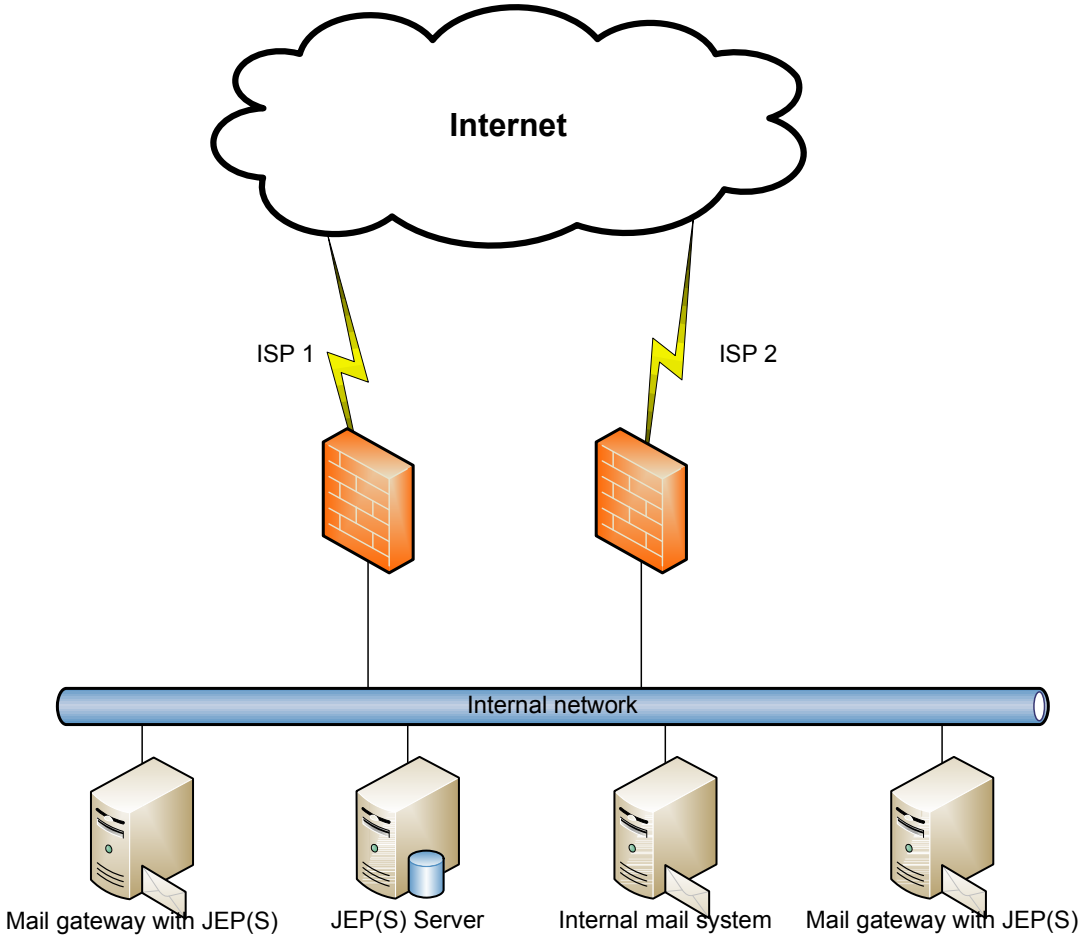


This scenario is suitable if you have two or more internet connections. As both mail gateways are using the same JEP(S) server they can be located virtually anywhere, even across time zones.
The benefit of this setup is that it's secure and redundant.

If you have a failure on either a mail gateway or internet connection you will still receive mail through the other link.

In addition to this you can cluster the JEP(S) Server and use multiple internal mail systems to increase availability. If you have multiple internal mail servers then you would configure the two different mail gateways to connect use different internal mail servers as smart hosts.

Redundant mail gateway without DMZ

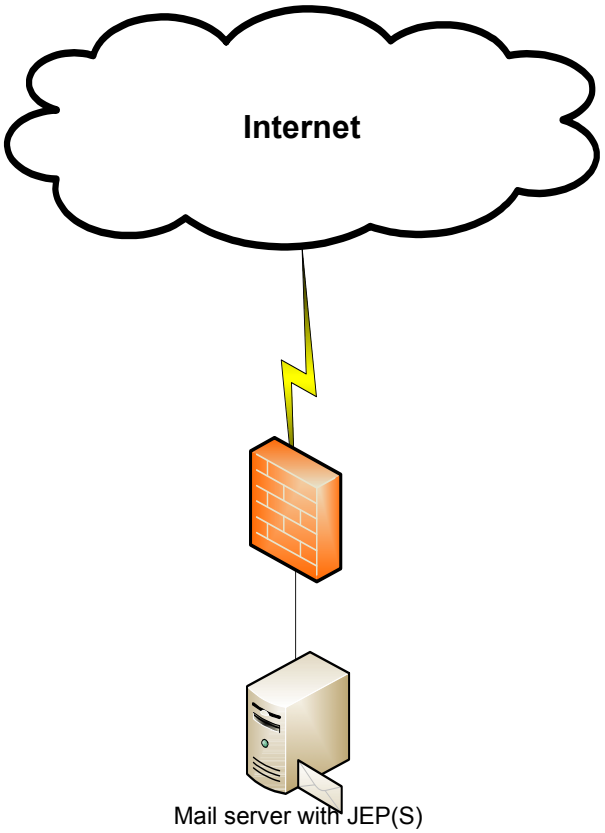


This scenario is suitable if you have two or more internet connections. As both mail gateways are using the same JEP(S) server they can be located virtually anywhere, even across time zones.
The benefit of this setup is that it's relatively secure and redundant. It's still beneficial to place the mail gateways in a DMZ if possible.

If you have a failure on either a mail gateway or internet connection you will still receive mail through the other link.

In addition to this you can cluster the JEP(S) Server and use multiple internal mail systems to increase availability. If you have multiple internal mail servers then you would configure the two different mail gateways to connect use different internal mail servers as smart hosts.

Stand alone mail server setup

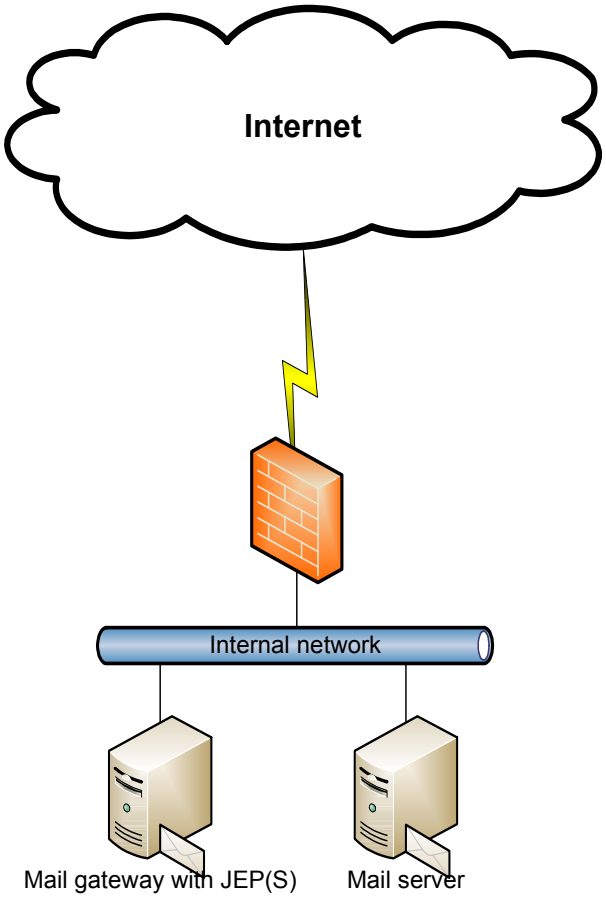


This is a common setup for small companies with Exchange, the JEP(S) server and the JEP(S) sink installed on the same server facing the internet. With a good firewall inspecting the SMTP packets the security achieved can be acceptable.

With this setup you should consider to implement a separate mail gateway as described in the next section.
This way you don't need to expose the Exchange server directly for incoming connections.

This setup can be used with the free (unlicensed) version of JEP(S).

Stand alone mail gateway



With this setup we achieve good security to a low cost. Both the JEP(S) Server and the JEP(S) sink are installed on the mail gateway. While its beneficial to place the mail gateway in a DMZ we do achieve a higher level of security and availability then with the single server setup.

This setup will provide isolation between the incoming mail traffic from the internet and the mail server. In the case of the mail gateway becoming compromised it can be isolated or powered off without affecting the internal mail server.

This setup can be used on the free version of JEP(S) but it's not recommended as the lack of email address filtering can have unwanted affects.