

If you have evaluated different centralized Anti-Spam & Anti-Virus Solutions you mostly stuck with one criteria. Email delivery has to be done via SMTP and MX Records. So far so good, but what to do, when having ISP taking care of all your email routing and your company is not big enough to maintain an own Email Service, like Lotus Domino or an Exchange environment. This works only, when your ISP is able to catch all in one single mailbox. When running a different environment, you may consider another POP3 Download Proxy, which is able to forward internally via SMTP.

## A typical environment looks like this:



In this scenario, all client retrieves their emails via POP3 from an external Email Server, hosted by an ISP. Anti-Spam can only work, if they are located on each client and this to be administered could cause nightmares. There are good solutions out there, like McAfee Security's WebShield Appliance with Anti-Spam and Anti-Virus, but solutions like that works only when SMTP delivery is in place. This won't be the way in this environment.

To make this run, I've added another service and McAfee Security WebShield Appliance.



The Red Server hosts now a kind of POP3 Retriever and SMTP Forwarder. The Grey Server has been added with a freeware SMTP Server. Between them, McAfee Security WebShield Appliance is scanning for Anti-Virus, Anti-Spam & Email Content Filtering.



There are several products out there, doing the Email Retrieval Job. In this scenario I used following products, which may be easily copied for your demands.

**ISP hosting Emails:** 

EMAIL RETRIEVA	L: EFS Standard Email Forwarding System by http://www.chimeracomputing.com/
Local SMTP Serve	r: Mail Enable Standard Edition by http://www.mailenable.com
ANTI-Virus & Anti <u>h</u>	-Spam: McAfee Security WebShield Appliance tp://www.nai.com/us/products/mcafee/antispam/spk_webshield_appliances.htm
Email Client:	Microsoft Outlook Express

#### Installation Steps

EFS Standard Email Forwardung System

Download Product from http://www.chimeracomputing.com/ and run efs3full.exe



Click on NEXT

License Agreement will show up







Click on **NEXT** – Here you can change Default Directory. I recommend to leave default settings



#### Click on **NEXT**

Once confirmation windows appears, you have the last change to stop the installation. To continue, you have to click **INSTALL** 



# Centralized Anti-Spam with POP3 Downloads



After a short moment, when installation has been performed you'll get a notification, that EFS has successfully installed. Now, it's time to view the readme.txt



When having Launch E.F.S. be marked, the application will start automatically.



Launch EFS by right click on 🥦

at the taskbar



# Centralized Anti-Spam with POP3 Downloads page 5 of 5

🐸 Email Forwarding System - STANDARD 📃 🗆 🗙
Aliases Headers Firewall Pre Check Post Check / Alert
Log POP3 SMTP Domains Schedule Advanced
POP3 Server pop.hotpop.com IP
Username demoroom@hotpop.com Port 110
Password ****** Timeout 60
Leave a Copy of Messages on Server
POP3 Messages Before Send Initiated:
Strip POP3 Account Prefix:
Max download
<u>?</u> <u>Apply</u> <u>Save</u>
IN: Disconnected OUT: Disconnected

Add following minimum values:

**Configure E.F.S** 

#### POP3 Server Username Password

Verify by clicking on IP, if DNS Lookup works.

Setup POP3 (incoming mail) settings and test mail downloads correctly and Enter the domain you accept mail for under the Domains tab

🛤 Email Forwardi	ng System - STANDARD	_ 🗆 🗙			
Aliases Header	s   Firewall   Pre Check   Post C	heck / Alert			
Log POP3	SMTP Domains Schedule	Advanced			
• Eorward					
SMTP Server	128.203.210.108	<u>I</u> P			
Port	25 Timeout 30 ES				
Postmaster	postmaster_internal@hotpop.com	<u>T</u> est			
Always CC Postmaster  Always CC Postmaster  Message Limit Per Send: 500  Dont Send 'Error' Messages					
C Do NOT Forwa	rdApply	<u>S</u> ave			
IN: Disconnected	OUT: Disconnected				

This SMTP Server is the IP Address of my McAfee Security Webshield Appliance, where all POP3 retrieved Emails will be forwarded. How WebShield has been configured, you will find later on this document.



## page 6 of 6

If your WebShield is already be setup, you should verify, if you can reach McAfee WebShield Appliance via Telnet on Port 25 (for SMTP)

C:\WINNT\system32\cmd.exe - telnet 128.203.210.108 25					_ 🗆 🗵					
220 W -	lelcome	to	Rainer	Bemsel's	Anti-Spam	Solution	via	WebShield	Appliance	▲ ▼

The disclaimer for SMTP has been modified, so you might have a different disclaimer. Now, you should enter the Primary Domain.

👪 Email F	orwarding System -	STANDARD	
Aliases	Headers Firewall	Pre Check	Post Check / Alert
Log	POP3 SMTP	Domains Sche	edule Advanced
Primary	Domain hotpop.com		⊻dA
Accept m	hail for these secondary	domains: maximum	n O
Add	Delete	Ap	ply <u>S</u> ave
IN: Disconn	nected	OUT: Disconne	ected

Change to LOG tab and click on CHECK. If there are any emails already with your ISP, you should get a retrieval

😂 Email Forwarding System - STANDARD					
Aliases Headers Firewall Pre Check Post Check / Alert					
Log POP3 SMTP Domains Schedule Advanced					
Click here to Register EFS Advanced!					
12/23/2003 09:44 < retrieving email 1 (3,975 bytes)					
Scheduled Today at 09:59 AM					
Progress In:  6 0ut:  6 6					
Clear Check Send 2 OK					
IN: Disconnected OUT: Disconnected					











## Mail Enable Standard Edition

Start the installation by double-click on mailenablestandard.exe. You should **not** install this mail server not on the same server as E.F.S has been installed.



#### Click on NEXT

Get Installation Settings		×
	Please enter the name and company of the registered owner of MailEnable Messaging Services for Windows NT/2000 into the fields below. All fields must be filled in to proceed. Name: Rainer Bemsel Company: private NOTE: It is recommended that you read the Quick Start installation guide before installing MailEnable. This is available at: http://www.mailenable.com/support	
	< <u>B</u> ack Next> Cancel	-

#### Type your name and Company. Click on **NEXT**













Read the terms and conditions and click on NEXT



You can change the folder by clicking on **BROWSE**. However, I recommend to keep default settings. Click on **NEXT** 



Again, keep default settings and click on **NEXT** 



#### Click on NEXT



Get Postoffice Details			×
	MailEnable requires and from. You typics company that you an Post Office you are r something that repre You will also need to mailbox for the Post Post Office Name: Password: Note: The Post Offic characters and shou characters "@:[]*	at least one Post Office to di ally configure one Post Office te hosting mail for. Because te egistering under Mail Enable- sents your company or busin supply a password for the F Office. demolab	eliver mail to for each this is the first it should be tess unit name. 'ostmaster ostmaster ess than 20 y of these
	<	<u>B</u> ack <u>N</u> ext>	Cancel

This is where you can add your own domain. I've added another Post Office later on at MailEnable Administrator. Click on **NEXT** 



Change the values to meet your requirements and click on NEXT



To start the installation click on **NEXT** and progress bar will appear.



MailEnable Read	Me			×
MailEnable Read	vle.txt			
	 . ,			
This README File	e provides r	elease ni	otes for MailEnable.	
Revision History	==			
Date 30-Apr-031.703	Version	Fixes	Explanation	
22-Apr-031.702 17-Apr-031.701		Fixes, a Fixes	ddition	
24-Mar-03	1.7		Update	
RELEASE NOTES	5			_
1				
OK			Cancel	

You will get a readme. Click on OK



Installation is complete. Click on FINISH and allow PC to restart. When PC has been restarted, logon again and start Mailenable





#### Create a new Post Office, if necessary

🚡 MailEnable - [MailEnable\MailEn	able Management\Messenging Manager\Post Offices	]		
Console <u>W</u> indow <u>H</u> elp			🗅 🗳 🖬   🎫 💷	I X
🗍 Action View Eavorites 🗍 🖨	→ 🗈 🔃 🕏 🖏 😫			
Tree Favorites	PostOffice A	Status		
MailEnable MailEnable Management Messenging Manager Post Off New View New Window New Window New Taskpa Bad Mail Bad Mail Servers Dicalhosi Help Diagnose Services	V from Here	Enabled		
Creates a new object in this container.				

Type a New post office name (incl. Domain extension)

📲 New Post Office	×					
MailEnable requires post offices to deliver mail to and from. A post office is typically named to represent the company or business unit that will use it to store e-mail.						
Note: The post office na should not contain space	me should typically be less than 20 characters and es or any of these characters "@ : []*?/\''.					
New post office name:	hotpop.com					
When a new post office created. This is the admi supply a password for thi	is created, a default mailbox called "Admin" will be nistrators mailbox for the post office. You need to is mailbox.					
Password:	*****					
Confirm Password:	жжжж					
	OK Cancel					

The password is for the administrator's mailbox, also knows as postmaster.

Similar to Post Office, create mailboxes if necessary.



## **Outlook Express Configuration**

Because EFS is a POP3 Download Service only, you will have to use to different server for routing emails in and out.

In my example, incoming Mail Server is located on "grey server" (based on my network layout on page one). For Outgoing mail, you may have to send emails directly to your ISP.

😪 pop.hotpop.com Properties	<u>?</u> ×
General Servers Connection Security Advanced	
Server Information	-
my incoming mail server is a server.	- 1
	- 11
Outgoing mail (SMTP): smtp.hotpop.com	_
Incoming Mail Server	-
Account name: demoroom	
Password:	
Remember password	
Log on using Secure Password Authentication	
Outgoing Mail Server	-
My server requires authentication Settings	
	-
OK Cancel Apr	du d
	<u>v</u>

On the next pages, you'll find some screenshots, where to add parameters to have appliance be able to scan for Spammails.



# McAfee Security WebShield Appliance

1. Connect WebShield Appliance on LAN 2 with your Administration Computer. https://10.1.2.108



- Default User Name: webshield Default Password: webshieldchangeme
   If you have Java Runtime Version other than 1.31\_04, please uninstall Java Runtime first, and let
   WebShield serve you with the proper Java Runtime Version. Allow installation and grant access.
- Assign Basic Settings: As I decided to run WebShield Appliance in Proxy Mode, you only need to change IP Address for LAN 1. LAN 2 is used for administration only and can be deactivated after basic settings have been configured.
- 4. Reboot WebShield Appliance and log on again by using new assigned IP Address and reconnected to LAN 1
- 5. Under SMTP, click on Anti-Spam.

E-mail (SMTP)
Postmaster
▶Anti-Relay
▶Anti-Spam
▶Delivery
Content Scanning
▶Quarantine
Attachments
▶Disclaimers
▶Configuration

6. E-Mail Anti-Spam pane will open.



<ul> <li>Permit Sender</li> <li>Deny Sender</li> <li>Real Time Anti-Spam Check</li> </ul>	<ul> <li>Inbound Anti-Spam Policy</li> <li>Outbound Anti-Spam Policy</li> <li>Anti-Spam Rules List</li> </ul>	
Rear time And-Spann Check	Ана-эраннкаез цэс	

When running a configuration from scratch, click on **EVALUATE** and Anti-Spam Policy

- 7. Now, click on Delivery
- E-mail (SMTP) Postmaster Anti-Relay Anti-Spam Delivery Content Scanning Quarantine Attachments Disclaimers Configuration

Click on Local Domains. If you haven't added any local domains, now it's time to do.

<ul> <li>Methods Used</li> <li>Local Domains</li> <li>Fallback Relays</li> <li>Deferred Messages</li> </ul>	
Local Domains Specify the local do most common doma Dom hotpo xylan.	nains to which messages for specific hosts are sent. List the ins first because they are tried in order: ain Hosts .c 192.168.0.123 om 128.203.210.250 Modify Delete Move up Move down

Click on Add and enter the values for Domain and internal SMTP Server

Add		×
Enter the inbou	ind domain and list of hosts	
	Domain	
	hotpop.com	
	Hosts	
	192.168.0.123	
	OK Cancel	

That's pretty much for the basics. I've sent a couple of caught spam mails to my demoroom Pop Account and run this scenario all the way through. On the next pages, you will see some screenshots of the positiv result.



# **Outlook Express Inbox View**

👙 Inbox - Outlook Express				IX
Eile Edit <u>V</u> iew <u>T</u> ools <u>M</u>	lessage <u>H</u> elp			<b>E</b>
New Mail Reply Repl	ly All Forward	Print Delete Send/Recv	► Addresses Find	
🔅 Inbox				
Folders	× ! 0 ?	From	Subject	Rec
🞲 Outlook Express	<b>_</b>	MailEnable Administrator	New E-Mail Account Notification	12/2
🗄 🧐 Local Folders		🖾 Rainer_Bemsel@NAI.com	FW: Congress, Yahoo! Slam Spam	12/
🙀 Inbox (7)		🖾 Rainer Bemsel	[spam] FW:	12/
		🖾 Rainer Bemsel	[spam] FW: I saw your profile p¥3cT8oab	12/
		🖾 Rainer Bemsel	[spam] FW: Buy your medications Discretely	12/
💮 🗑 Deleted Items	-	🖾 Rainer Bemsel	[spam] FW: everyone should be big - this is ho	12/
Contacto 💌	~	🖾 Rainer Bemsel	FW: Rainer - Software Sale-PROTECT YOUR PC	12/
Quintacts		🖾 Rainer Bemsel	FW: Rainer, do u want to see Filthy Sluts From	12/
	<b>▼</b>   •			►
8 message(s), 7 unread			💻 Working Online	_/_

Picking one of the emails, marked with SPAM. By verifying the properties, I could see all X-Headers, added by Spamkiller

[spam] FW: Buy your medications Discretely
General Details
Internet headers for this message:
MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="=_NextPart_000_0019_01C3C951.CE! X-Priority: 3 (Normal) X-MSMail-Priority: Normal X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.116 Importance: Normal Disposition-Notification-To: "Rainer Bemsel" <rainer@bemsel.cc X-Provags-ID: kundenserver.de abuse@kundenserver.de auth: X-HotPOP-Delivered-To: demoroom@hotpop.com To: <demoroom@hotpop.com To: <demoroom@hotpop.com X-Forwarder: Redirected by EFS, http://www.chimeracomputin; X-NAI-Spam-Score: 8.0 X-NAI-Spam-Level: ******** X-NAI-Spam-Level: ********* X-NAI-Spam-Level: *********</demoroom@hotpop.com </demoroom@hotpop.com </rainer@bemsel.cc 
Message Source
OK Cancel

With a setup similar to this, you can use a global Anti-Spam Solution, based on SMTP.

