Configuration Example for the D-Link NetDefend Firewall Series

[Case]

Configure SMTP ALG for Anti-Spam

Implement mode: DFL-210/260/260E/800/860/860E/1600/1660/2500/2560/2560G

Firmware: 2.27.01

Why Anti-Spam

SPAM is the abuse of electronic messaging systems broadcasting bulk emails and media. With the popularity of Internet, many people are bothered by SPAM messages everyday. From the system point of view, SPAM messages are a kind of burden for not only system resources but bandwidth. In D-Link NetDefend family, we provide two approaches to filter out SPAM emails – by listing specific SPAM senders in *Blacklist* and by *DNSBL* (DNS Blacklist). In this document, you can find the step by step setting of anti-spam. Before start, please notice:

- The screenshots of the document are retrieved from firmware version 2.27.01. If you are using the firmware version which earlier than this one, the screenshots may not identical to what you see on your browser.
- To prevent existing setting to interfere with the settings in this guides, reset the firewall to factory defaults before starting.

How to configure anti-spam

SUPERSTAR Corporation set up an Anti-Spam service to prevent spam email sending to internal clients. After detail evaluation, Administrators find most of junk mails come from hotmail.com, and therefore decide to block all emails form Hotmail. To filter out junk mails exhaustively, administrators also collect latest spam information from several DNSBLs (DNS Blacklist)..

- Create ALGs for specific services
- Create a service object to associate with the ALG function
- Create IP Rules to associate with service objects

STEP 1: ALG with AV/WCF

Navigate to **Objects> ALG with AV/WCF** and add a new *SMTP ALG* or edit the pre-defined rule *SMTP-inbound.*

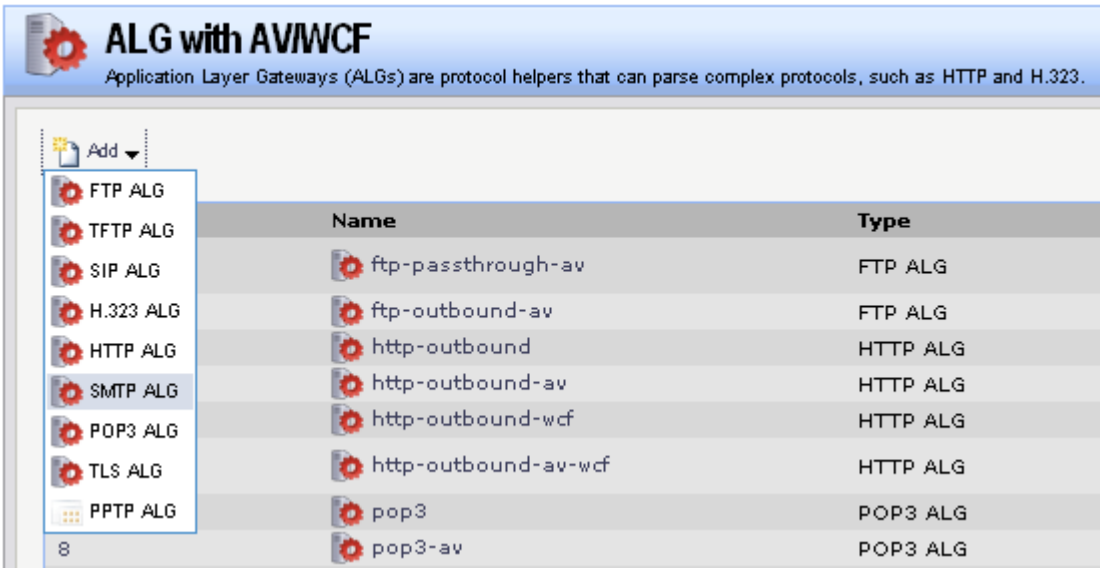

Figure 1: Add SMTP ALG

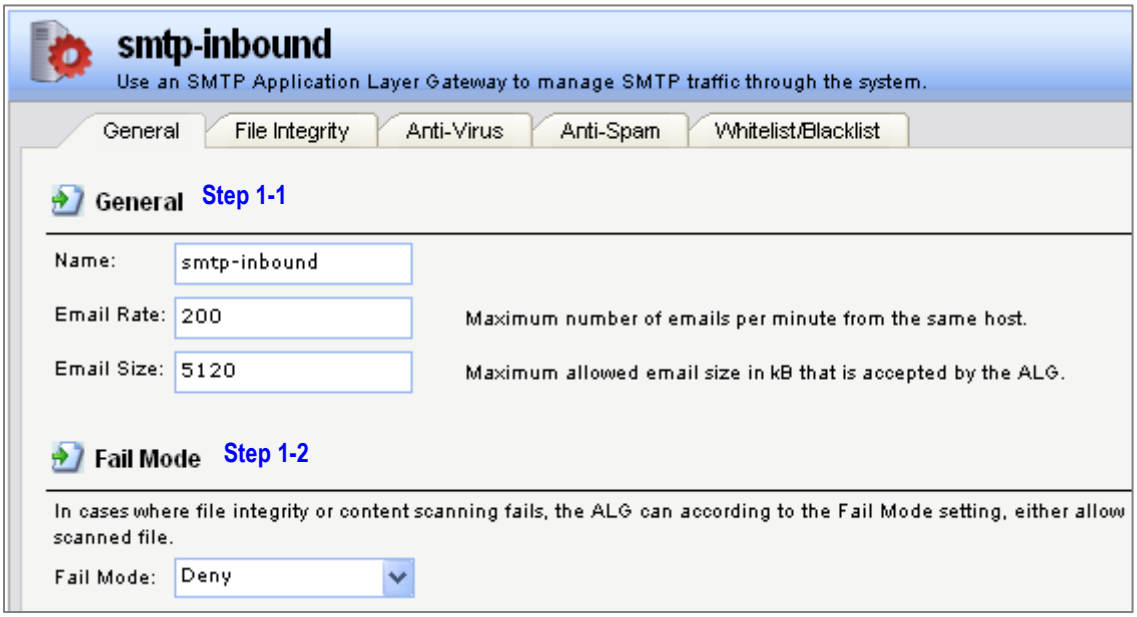

Figure 2: SMTP ALG, General

In General tab (Figure 2), fill in relative information:

Step 1-1: General

Name: smtp-inbound (defined by user)

Email Rate: 200

Email Size: 5120

Step 1-2: Fail Mode

Fail Mode: Deny

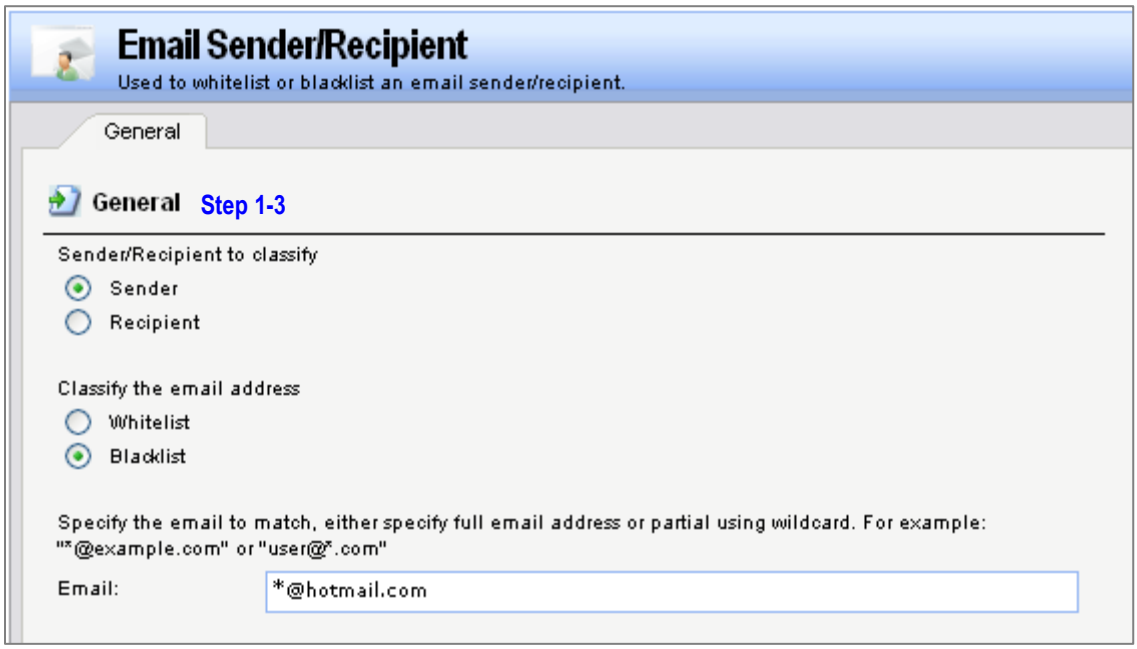

Figure 3: SMTP ALG. Whitelist/Blacklist

In Whitelist/Blacklist tab (Figure 3), add a mail server that you want to block.

Step 1-3: General

Click "Sender"

Click "Blackliast"

Email: *@hotmail.com

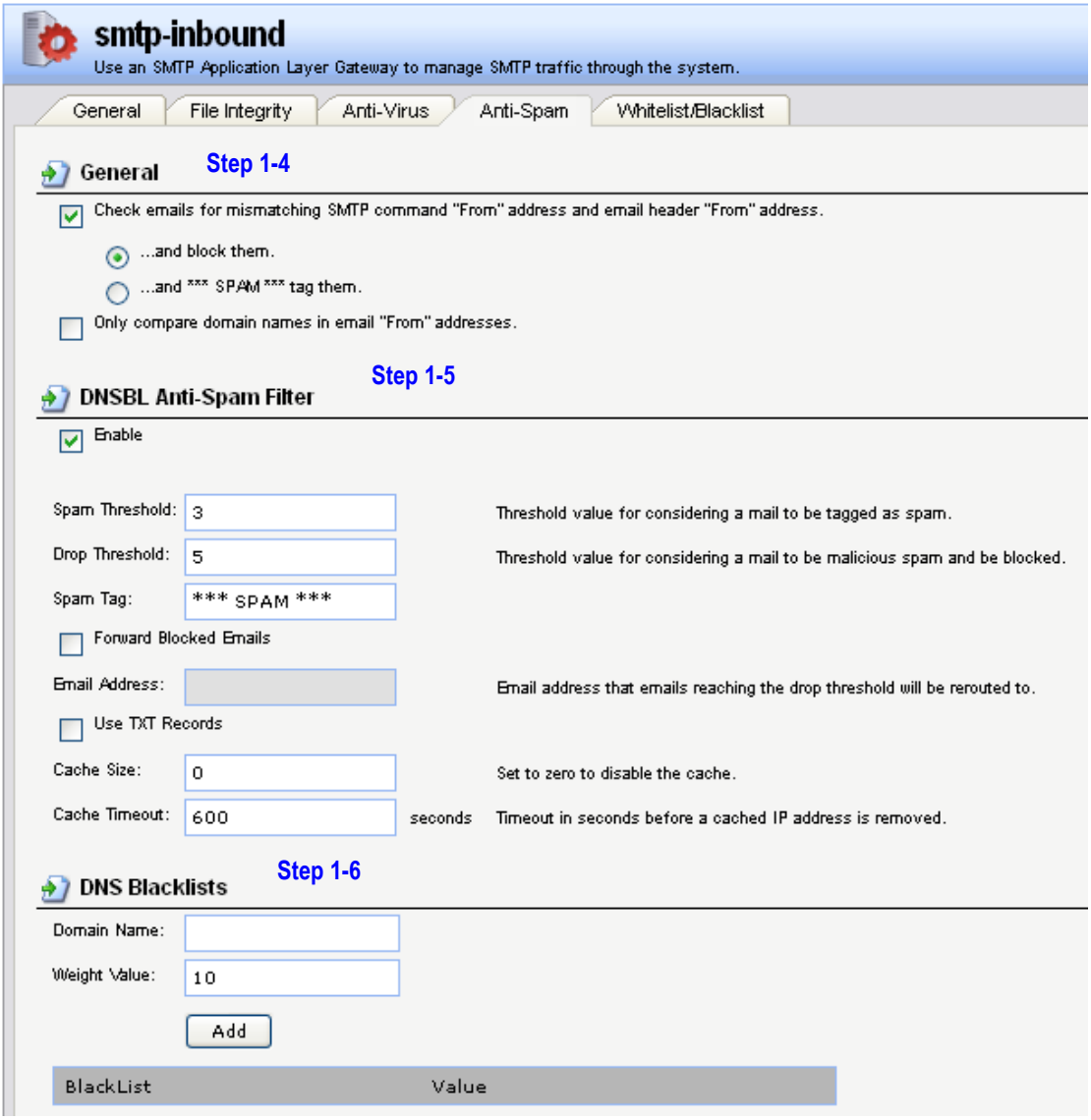

Figure 4: SMTP ALG. Anti-Spam

In Anti-Spam tab (Figure 4), fill in relative information:

Step 1-4: General

Tick box "Check emails for mismatching SMTP command "From" address and email header "From" address"

Choose: "…and block them"

Step 1-5: DNSBL Anti-Spam Filter

Tick box "Enable"

Spam Threshold: 3

Drop Threshold: 5

Cache Size: 0

Cache Timeout: 600

Step 1-6: DNS Blacklist

Add the domain name and weight value of DNS blacklists.

sbl.spamhaus.org (weight value 1)

virbl.dnsbl.bit.nl (weight value 1)

bl.spamcop.net (weight value 1)

list.dsbl.org (weight value 1)

zen.spamhaus.org (weight value 1)

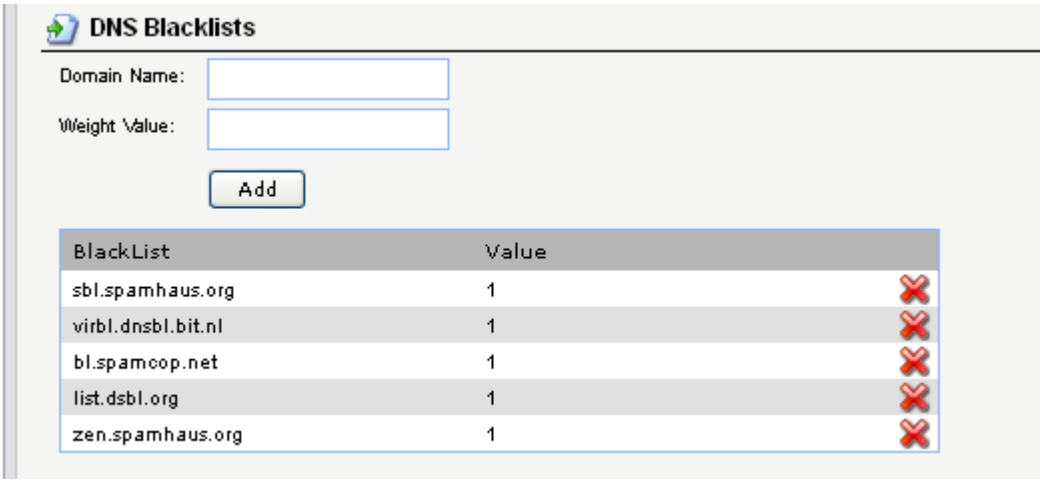

Figure 5: DNS Blacklists

Click OK

When an email sent by Spammers listed on DNS blacklist, the weight value will be calculated accordingly, and then saved in the NetDefend system memory. Referring to the DNS Blacklists, the firewall would sum up relative weight values, and then compares this result with the figure of “Spam Threshold” and of “Drop Threshold” settings. When the sum value is equal to or above the configured figure, the mail will then either be tagged as a spam (*** SPAM ***) in the mail subject and forwarded, or discarded by the ALG directly.

STEP 2: Service

Navigate to **Objects> Services** and add a new *TCP/UDP service* or edit the pre-defined *smtp-inbound* service. The service object will be listed on the *Service* file in IP rules on later step.

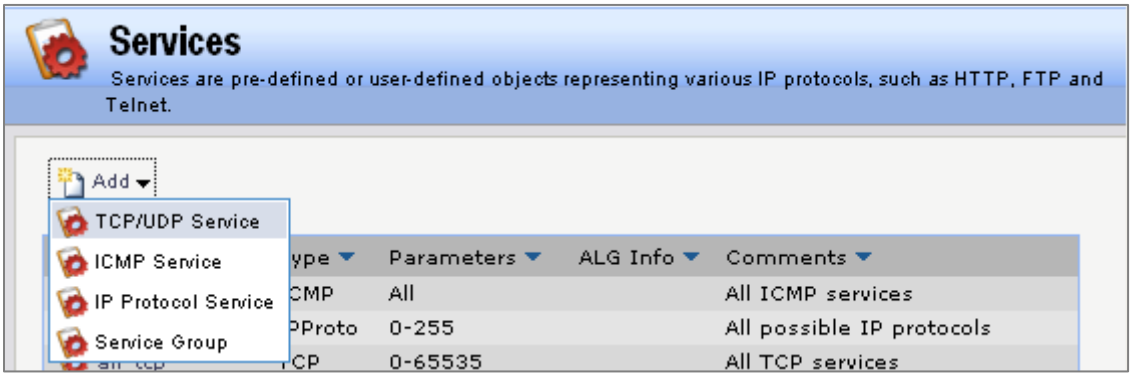

Figure 6: Add TCP/UDP Service

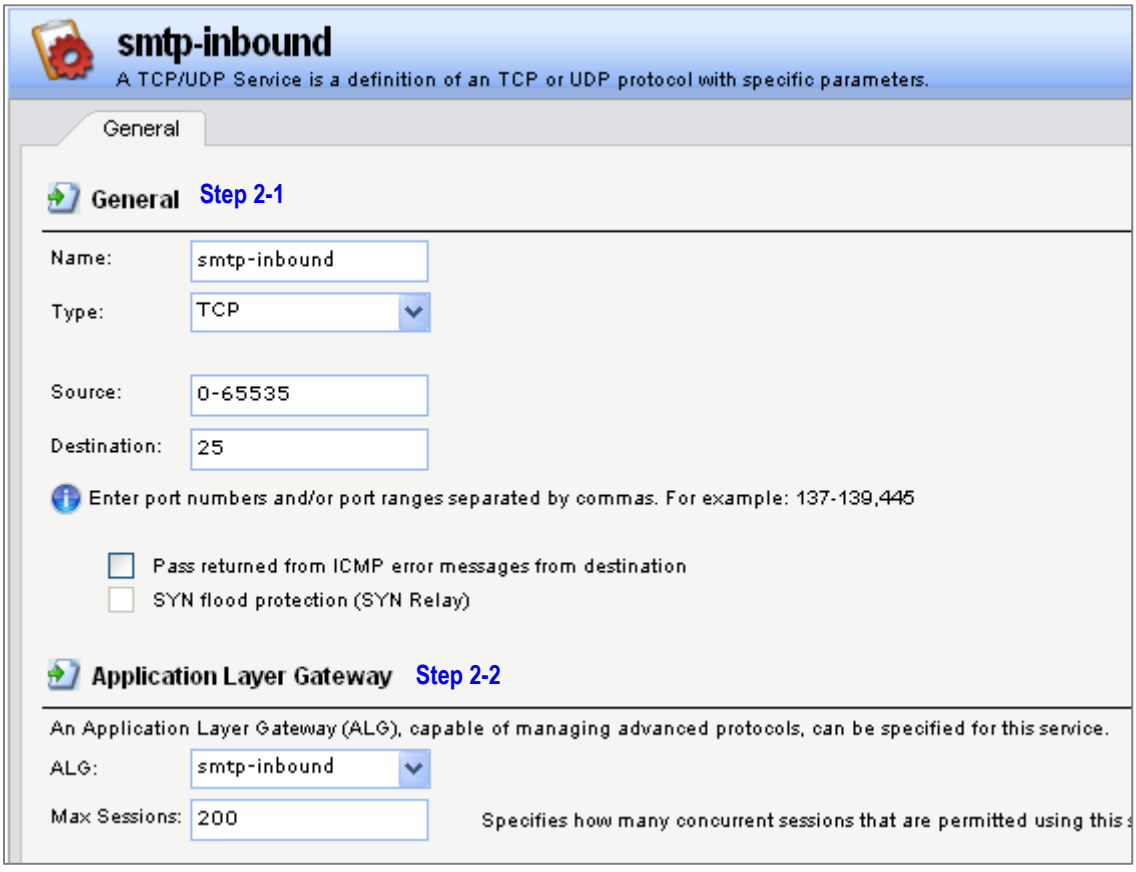

Figure 7: TCP/UDP Service

In General tab (Figure 7):

Step 2-1: General

Name: smtp-inbound

Type: TCP

Source: 0-65535

Destination: 25

Step 2-2: Application Layer Gateway

Select the Application Layer Gateway (ALG), which is created in *ALG with AV/WCF* to specify for this service.

ALG: smtp-inbound

Click OK

STEP 3: Rules

Navigate to **Rules> IP Rules** and add a new *IP Rule*. The first rule defines the connection originating from the external public mail server to internal private mail servicer. Since the internal mail server owns an exclusive private IP and a shared public IP, use SAT to translate the destination IP address between them. The public IP of the mail server is the IP address of wan1. Also remember to add an IP4 object regarding to the private IP of the mail-server in the Address Book.

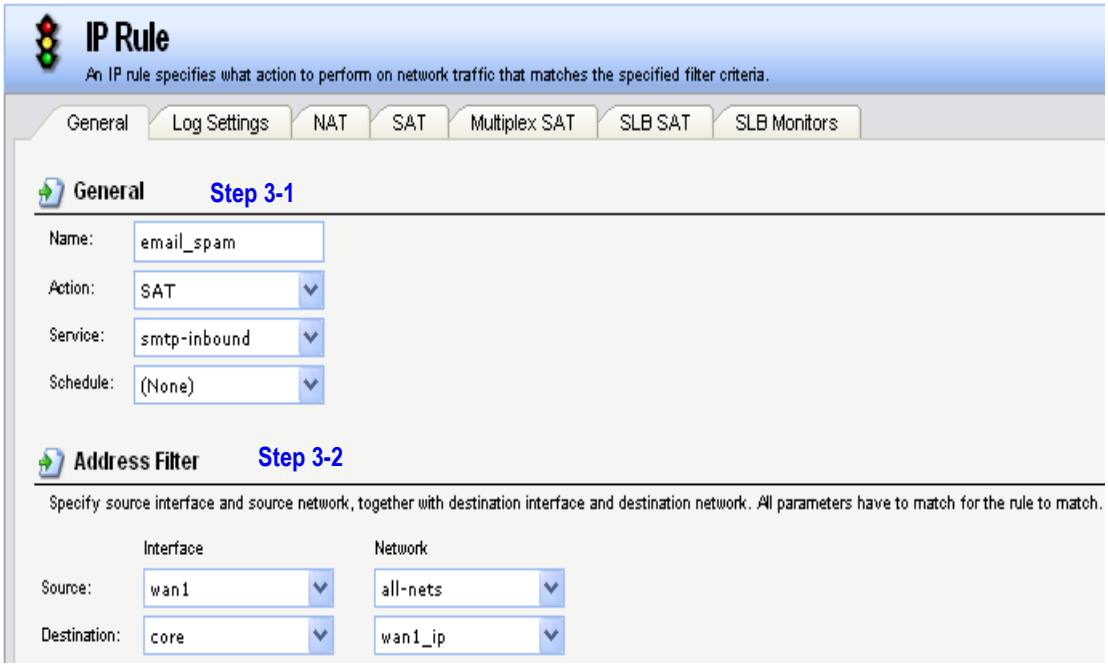

Figure 8: Rules, General

In General tab (Figure 8), fill in relative information:

Step 3-1: General

Name: email_spam (defined by user)

Action: SAT

Service: smtp-inbound

Schedule: (None) (defined by user)

Step 3-2: Address Filter

Source Interface: wan1

Source Network: all-nets

Destination Interface: core

Destination Network: wan1_ip

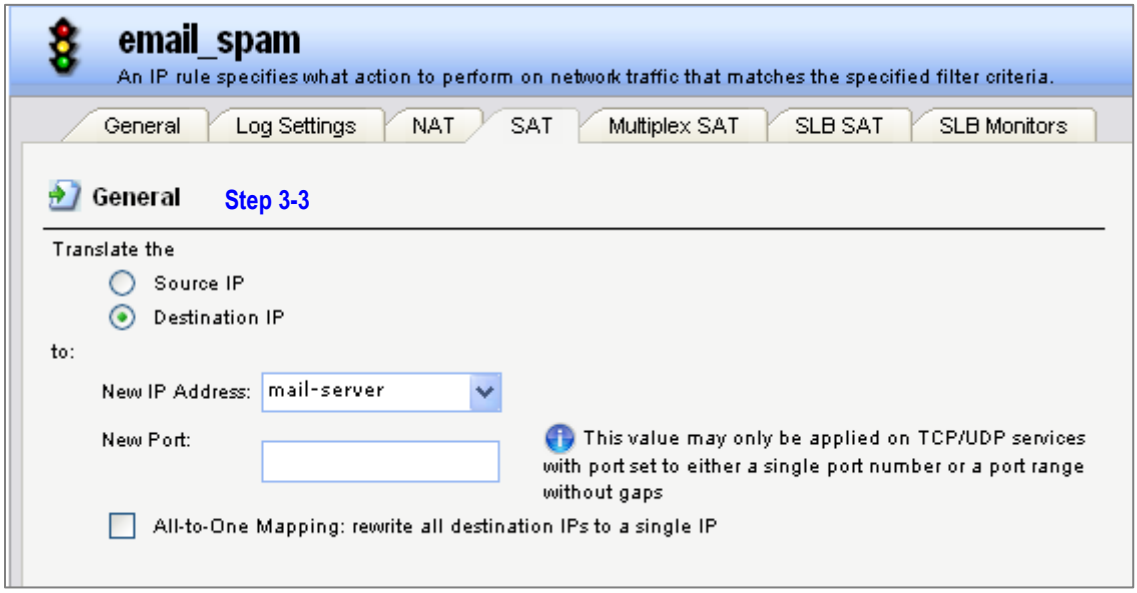

Figure 9: Rules, SAT

In SAT tab (Figure 9):

Step 3-3: General

Click "Destination IP"

New IP Address: mail-server

Click OK

Add the second rule paired to the previous SAT IP rule.

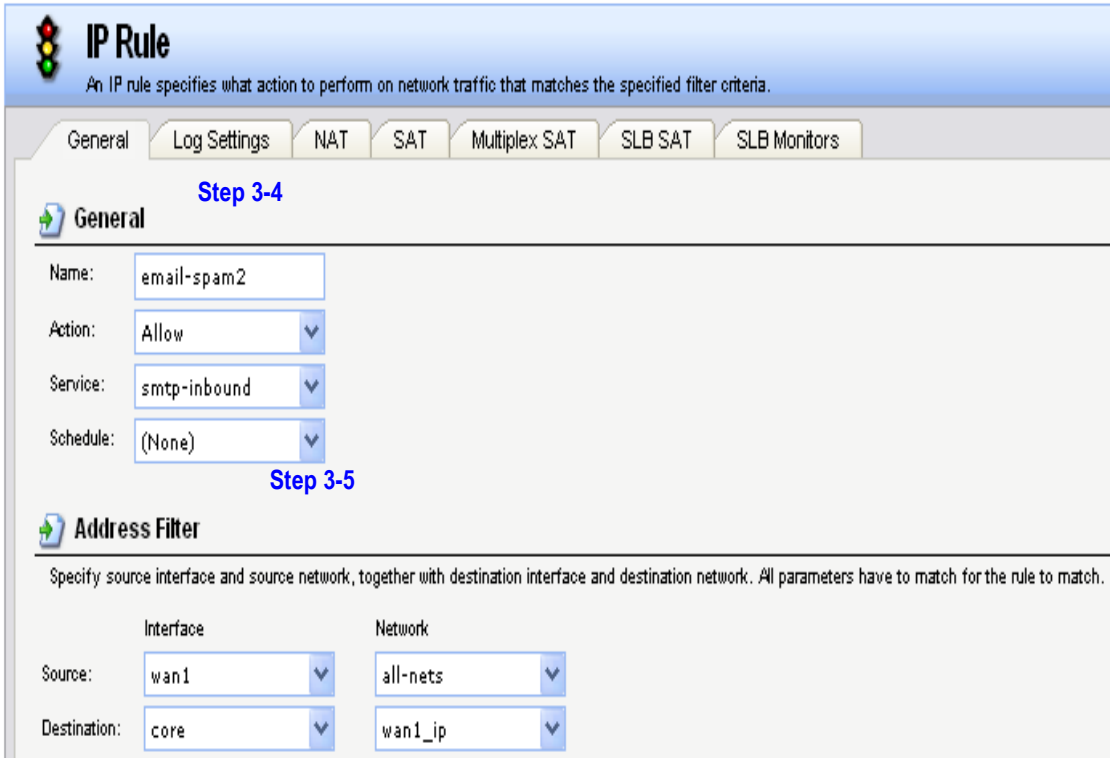

Figure 10: Rules, General

In General tab (Figure 10), fill in relative information:

Step 3-4: General

Name: email_spam2 (defined by user)

Action: Allow

Service: smtp-inbound

Schedule: (None) (defined by user)

Step 3-5: Address Filter

Source Interface: wan1

Source Network: all-nets

Destination Interface: core

Destination Network: wan1_ip

Click **OK**

[[Save and Active the Configuration]]

Extra Information

More discussion about Weight-based calculation:

The NetDefend Firewall adopts weight-based calculation to determine whether an email is a spam or not. On the NetDefend firewall, the administrator could configure the anti-spam filter by checking senders and given the weight values respectively. For example, set the weight value as the below:

In DNSBL Anti-Spam Filter,

Spam Threshold: 3

Drop Threshold: 5

In DNS Blacklist,

sbl.spamhaus.org (weight value 2)

virbl.dnsbl.bit.nl (weight value 1)

dnsbl.sorbs.net (weight value 2)

Example 1:

If the mail is send by all Spammers of DNSBL, the firewall will receive positive return results, 1, 1, 1. The sum value for these positive results will be 2*1 + 1*1 + 2*1, and the total is 5. As the "Drop Threshold" is set as 5, this mail will then be dropped.

2*1 + 1*1 + 2*1=5→ same as Drop Threshold→ Drop the packets.

Example 2:

If the mail is only sent by Spamhaus, the return results will be 1, 0, 0. The weight-based calculation is 2*1 + 1*0 + 1*0 = 2. The NetDefendOS will do nothing with this mail since none of the threshold values are reached.

Example 3:

If the mail is sent by Spamhaus and Sorbs Spammers, the return results will be 1, 0, 1. The weight-based calculation will be 2*1 + 1*0 + 2*1 = 4. As our "Spam Threshold" is 3 and "Drop Threshold" is 5. The mail will be tagged as a spam, and forwarded to client. E.g. If the

original mail subject is "Stock quotes", the subject will be changed to "*** SPAM *** Stock quotes", and forwarded to the client.

Additionally, you can assign higher weight value for specific DNSBL servers, for example if you think the detection rate of Spamhaus is more precise, you can assign higher value for Spamhaus, compared to other servers. Following is the configuration example:

Spamhaus - weight 10

Sorbs - weight 1

Server x - weight 1

Server y - weight 1

Server z - weight 1

Server w - weight 1

Spam Threshold - 5

Drop Threshold – 11

For more information about DNSBL servers, please refer to http://spamlinks.net/filter-dnsbl-lists.htm.