Configuration Examples for the D-Link NetDefend Firewall Series

Scenario: How to configure Anti-Spam on NetDefend Firewall

Platform Compatibility: All NetDefend Firewall Series

Last update: 2008-08-01

Overview

In this document, the notation *Objects->Address book* means that in the tree on the left side of the screen **Objects** first should be clicked (expanded) and then **Address Book**.

Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 have more than one lan interface, the lan interfaces are named lan1, lan2 and lan3 not just lan.

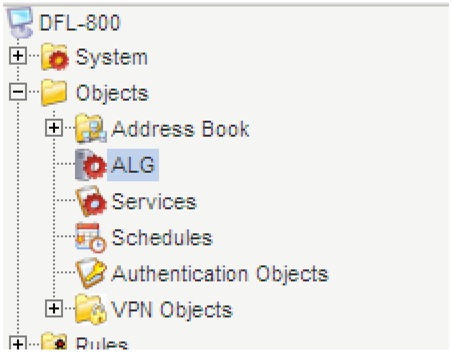
The screenshots in this document is from firmware version 2.20.00. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

To prevent existing settings to interfere with the settings in these guides, reset the firewall to factory defaults before starting.

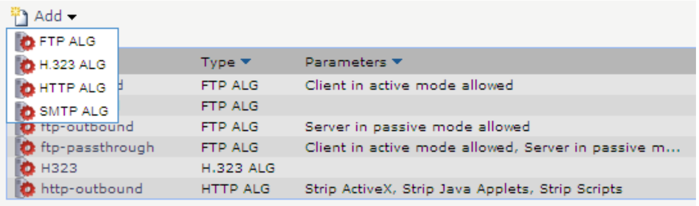
How to configure SMTP ALG for Anti-Spam

This scenario shows how to configure a NetDefend firewall to enable Anti-Spam feature for filtering incoming spam mails.

Step 1: Go to *Objects ->ALG*



Step 2: Add a new SMTP ALG, or edit the pre-define rule SMTP-*inbound*



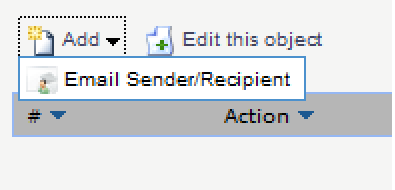
	Type	Parameters
	FTP ALG	Client in active mode allowed
	FTP ALG	
ftp-outbound	FTP ALG	Server in passive mode allowed
ftp-passthrough	FTP ALG	Client in active mode allowed, Server in passive m...
H323	H.323 ALG	
http-outbound	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts

In this case, let's use the pre-defined SMTP ALG, and modify it.

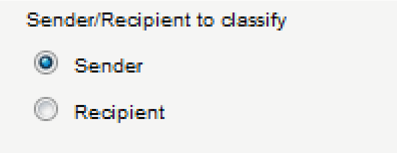
Step 3: Click *SMTP-inbound*

The SMTP ALG supports Email address/Email domain filtering, you can manually add blacklist/whitelist to customize address filtering.

Step 4: If you would like to block emails from a specific Sender, add *Email Sender/Recipient*



Select: *Sender*

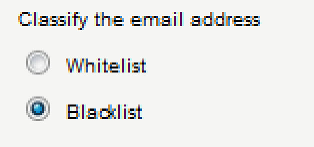


Sender/Recipient to classify

● Sender

○ Recipient

Select *Blacklist*

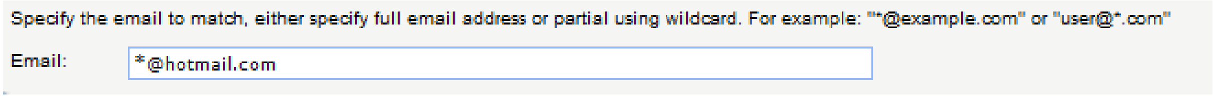


Classify the email address

○ Whitelist

● Blacklist

Assume that you would like to block a specific email server, e.g. *@hotmail.com, enter the email domain or account that you want to block as following:

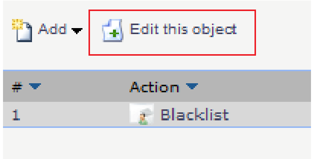


Specify the email to match, either specify full email address or partial using wildcard. For example: "*@example.com" or "user@*.com"

Email: *@hotmail.com

Click *OK*

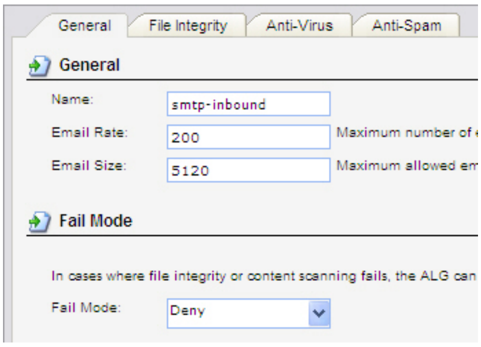
Step 5: Click *Edit this object* for advance setting



#	Action
1	Blacklist

Step 6: In *General* tab, provide the following information:

Name: *smtp_inbound*
Email Rate: *200*
Email Size: *5120*
Fail Mode: *Deny*
Click tab *Anti-Spam*



General

Name: smtp-inbound

Email Rate: 200 Maximum number of

Email Size: 5120 Maximum allowed em

Fail Mode

In cases where file integrity or content scanning fails, the ALG can

Fail Mode: Deny

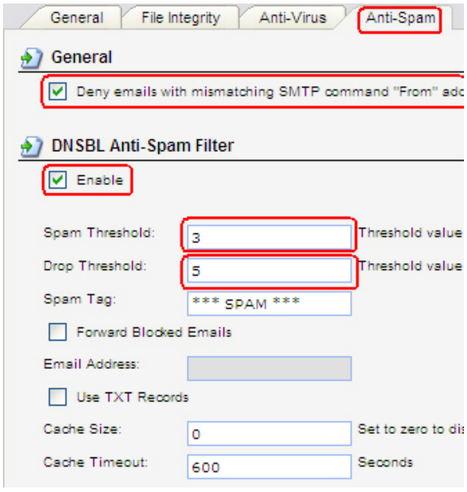
Note for Settings:

Email Rate:
It represents the maximum number of emails allowed per minute from the same host

Email Size:
It represents the maximum allowed email size in KB that is accepted by the ALG.

Step 7: In *Anti-Spam* tab, provide the following information:

General: *Enable* “Deny emails with…”
DNSBL Anti-Spam Filter: Select *Enable*
Spam Threshold: *3*
Drop Threshold: *5*
Cache Size: *0*
Cache Timeout: *600*



General

☑ Deny emails with mismatching SMTP command "From" adc

DNSBL Anti-Spam Filter

☑ Enable

Spam Threshold: 3 Threshold value

Drop Threshold: 5 Threshold value

Spam Tag: *** SPAM ***

□ Forward Blocked Emails

Email Address:

□ Use TXT Records

Cache Size: 0 Set to zero to dis

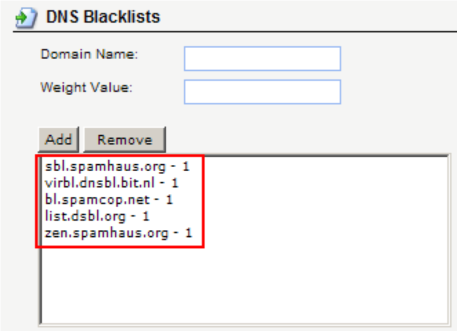
Cache Timeout: 600 Seconds

Step 8: Specify specific DNS Blacklists Servers and respectively assign Weight Value for these servers, so that the NetDefend firewall can send queries to the servers.

Below is the configuration example:

DNS Blacklists
Add the blacklists you want to use, i.e.

- 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)


DNS Blacklists
Domain Name:
Weight Value:
Add Remove

sbl.spamhaus.org - 1
virbl.dnsbl.bit.nl - 1
bl.spamcop.net - 1
list.dsbl.org - 1
zen.spamhaus.org - 1

Click *OK*

Note for Settings:
Weight Value:
When a mail is marked as a spam by the specified blacklist server, the weight value is then stored in the NetDefend system memory. After all blacklist servers have returned the query results to the NetDefend firewall, the NetDefend firewall will then sum up the values according to the mails tagged as “SPAM” by the blacklist servers.

Then, the sum value is compared to the value in “Spam Threshold” and “Drop Threshold” setting. When the value is equal to or above the configured value, the mail will then either be tagged as a spam (*** SPAM ***) in the mail subject and forwarded, or discarded by the ALG.

Further discussion about Weight-based calculation:

The NetDefend Firewall adopts weight-based calculation to determine if an email is a spam or not. On the NetDefend firewall, considering the administrator configured the public blacklist servers and respective weight values as the followings:

The Spamhaus DNSBL:

- ➢ sbl.spamhaus.org (Weight value 2)

The VIRBL DNSBL:

- ➢ virbl.dnsbl.bit.nl (Weight value 1)

The SORBS DNSBL:

- ➢ dnsbl.sorbs.net (Weight value 2)

Also, the "Drop Threshold" is configured as 5, and the “Spam Threshold" is as 3.

Example 1:

Saying each DNSBL server regards the mail sender as a spam sender; this will give us positive returned results, 1, 1, 1 from the servers. Thus, 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.

Example 2:
Saying if only Spamhaus regards the sender is a spam sender, the returned results from these servers will be 1, 0, 0. The weight-based calculation then is 2*1 + 1*0 + 1*0 = 2; the NetDefendOS will do nothing with regard to the mail, since none of the threshold values are reached.

Example 3:
Saying that Spamhaus and Sorbs DNSBL servers both regard that the mail is a spam. The returned results from the servers will be 1, 0, 1. Thus, 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 then tagged as a spam, and forwarded. E.g. If the original mail subject is "Stock quotes", the subject will be changed to "*** SPAM *** Stock quotes", and forwarded. Therefore, the mail will be sent to the receiver still, since the "Drop Threshold" is 5, compared to the sum result, which is only 4.

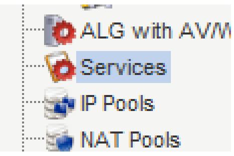
Additionally, you can configure 1 DNSBL server only instead of 3, or you can even configure more than 3 servers. You can assign higher weight value for some specific DNSBL servers, for example if you regard that the detection rate of Spamhaus is more precise and trustworthy, in such case you can assign 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

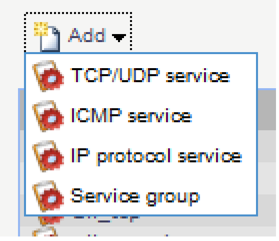
Spam Threshold - 5
Drop Threshold - 11

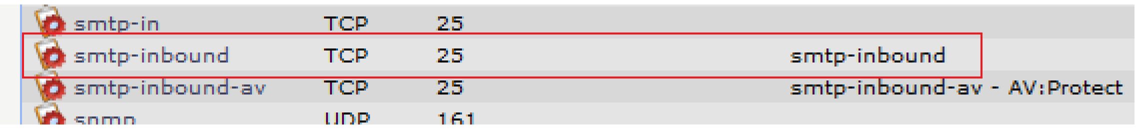
Note:
The DNSBL servers for querying and their respective weight value assignment are up to the administrator. For more information about DNSBL servers, please refer to http://spamlinks.net/filter-dnsbl-lists.htm.

Step 9: Go to *Services*



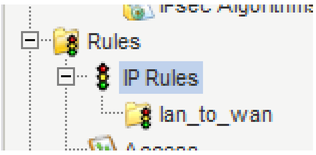
Add *TCP/IP service* Object to include SMTP ALG for Anti-Spam, or *use the predefined smtp-inbound* object, if you already configure the predefined SMTP ALG for Anti-Spam as mentioned in previous steps.

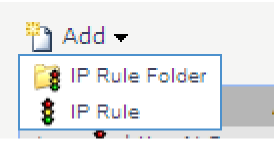




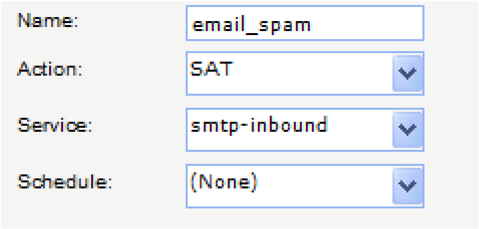
smtp-in	TCP	25	
smtp-inbound	TCP	25	smtp-inbound
smtp-inbound-av	TCP	25	smtp-inbound-av - AV:Protect
snmp	UDP	161	

Step 10: Go to *Rules > IP Rules*,
Add an *IP Rule*





Step 11: In General tab, provide the following information,
Name: email_spam
Action: *SAT*
Service: *smtp-inbound*

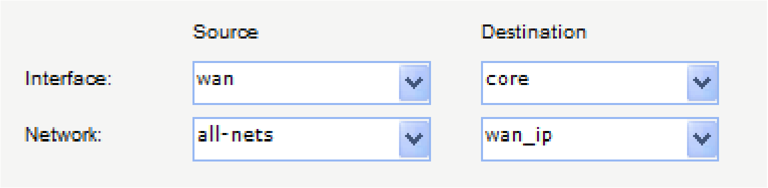


Name:	email_spam
Action:	SAT
Service:	smtp-inbound
Schedule:	(None)

Note:
Select smtp-inbound service object since it includes SMTP ALG.

Source Interface: wan
Source Network: *all-nets*

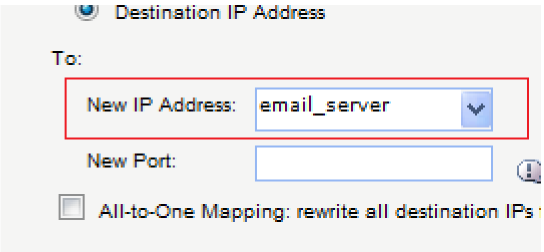
Destination Interface: core
Destination Network: *wan_ip*



	Source	Destination
Interface:	wan	core
Network:	all-nets	wan_ip

In SAT tab,

Select email_server object, or enter email server ip address



● Destination IP Address

To:

New IP Address:	email_server
New Port:	

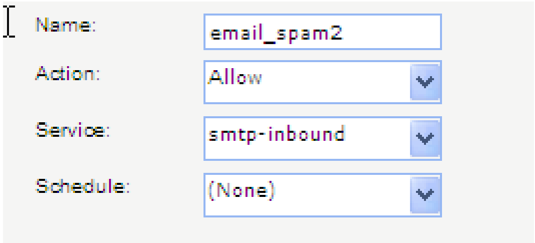
□ All-to-One Mapping: rewrite all destination IPs

Note:
This “email_server” object is just an example in this document; you may need to create an IP address object for it, as by default NetDefend firewalls don’t have this pre-defined object.

Click *OK*

Step 12: Add a rule
In General tab

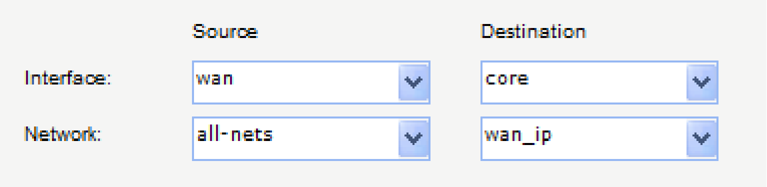
Name: email_spam2
Action: *Allow*
Service: *smtp-inbound*



Name:	email_spam2
Action:	Allow
Service:	smtp-inbound
Schedule:	(None)

Source Interface: wan
Source Network: *all-nets*

Destination Interface: core
Destination Network: *wan_ip*



	Source	Destination
Interface:	wan	core
Network:	all-nets	wan_ip

Step 13: Click *Save and Active*