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: 2008-03-13

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 has more than one lan interface, the lan interfaces are named lan1, lan2 and lan3 not just lan.

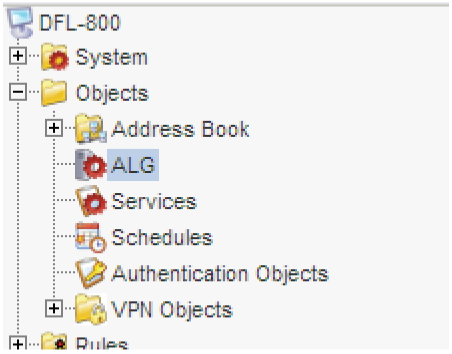
The screenshots in this document is from firmware version 2.20.00. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

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

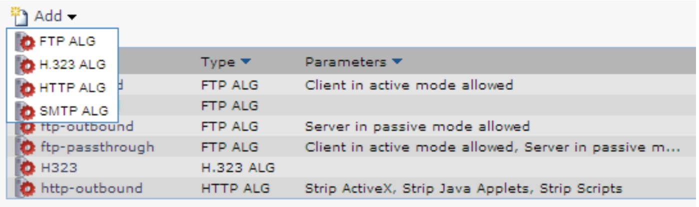
How to configure SMTP ALG for Anti-Spam

This scenario shows how a firewall can filter incoming email if it is spam or not.

Step 1: Go to *Objects ->ALG*



Step 2: Add a new SMTP ALG
Or edit pre-define rule SMTP-*inbound*



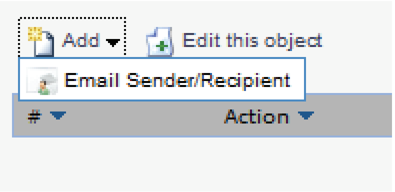
	Type ▾	Parameters ▾
d	FTP ALG	Client in active mode allowed
	FTP ALG	
ftp-outbound	FTP ALG	Server in passive mode allowed
ftp-passthrough	FTP ALG	Client in active mode allowed, Server in passive m...
H323	H.323 ALG	
http-outbound	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts

In this case, let's modify pre-defined SMTP ALG

Step 3: Click *SMTP-inbound*

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

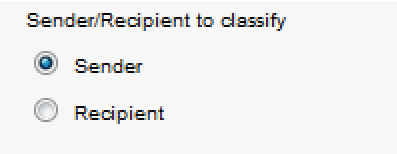
Step 4: Add *Email Sender/Recipient*
Select: *Sender*



If you would like to block email from specific Sender

Select *Blacklist*

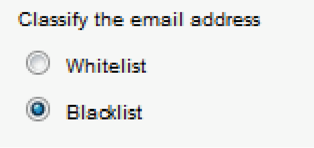
If you would like to block a specific email server



Sender/Recipient to classify

● Sender

○ Recipient

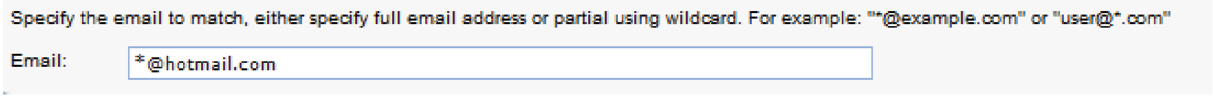


Classify the email address

○ Whitelist

● Blacklist

Enter the specific email domain or account that you want to block

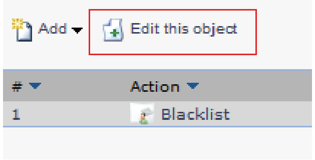


Specify the email to match, either specify full email address or partial using wildcard. For example: "*@example.com" or "user@*.com"

Email: *@hotmail.com

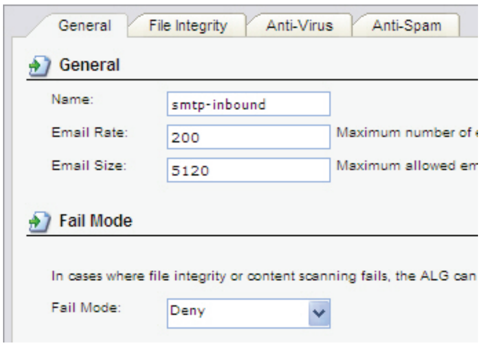
Click *OK*

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



#	Action
1	Blacklist

Step 6: In *General* tap
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

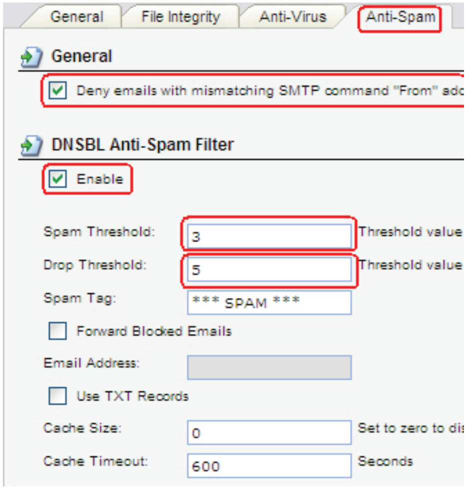
Fail Mode

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

Fail Mode: Deny

Settings explained:
Email Rate: Maximum number of emails per minute from the same host
Email Size: Maximum allowed email size in kB that is accepted by the ALG.

Step 7: In *Anti-Spam* tap
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

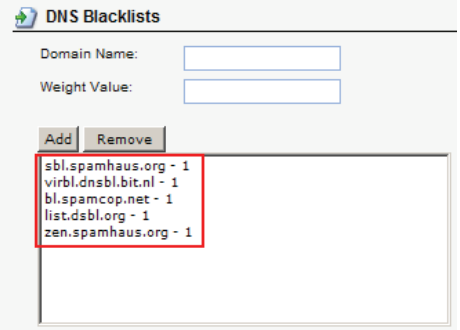
Email Address:

□ Use TXT Records

Cache Size: 0 Set to zero to dis

Cache Timeout: 600 Seconds

Step 8: Enter *specific anti-spam server and Weight Value* for firewall querying



DNS Blacklists

Domain Name:

Weight Value:

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

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)

Settings Explained:
Weight value: When a mail is marked as spam by the blacklist you've entered, the weight value is stored in memory. When all blacklists have reported back to the firewall if the mail is spam or not, the values of the blacklists that returned "SPAM" will be added together. The total value is matched against the "Spam Threshold" and "Drop Threshold" value. When the value is equal or more then the values set, the mail will either be marked as spam (*** SPAM ***) or dropped by the ALG.

Click *OK*

Regarding Weight-based calculation introduction

NetDefend Firewalls is weight-based to calculate and determine each email that is Normal or Spam, like following example,

Example 1:
Lets say that each server think the sender of the email is a spam sender. This will give us a result of 1, 1 and 1 from the servers. The total sum will be 1*1 + 2*1 + 2*1 and the total result is 5. Since the "drop threshold" is set to 5, this mail will be dropped.

Example 2:
Lets say that only SpamHaus think that this is a spam mail. The results from the servers will be 0, 1, 0. With the weights the results is 1*0 + 2*1 + 1*0 = 2. Nothing will be done to the mail, since the none of the thresholds were reached.

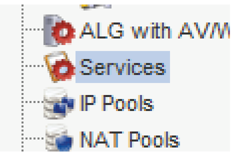
Example 3:
Lets say that SpamHaus and Sorbs thinks that this is a spam mail. The results from the servers will be 0, 1, 1. With the weights the results will be 1*0 + 2*1 + 2*1 = 4. Our "spam threshold" is 3 and "drop threshold" is 5. The mail will be tagged as spam (if the subject was "Stock quotes" it will be changed to "*** SPAM *** Stock quotes". The mail will still be sent to the receiver, since the "drop threshold" is 5 and our sum is only 4.

You can also choose to configure only 1 server instead of 3, like this example. You can also choose to configure even more than 3 servers. The difference in weight can be higher. If you for example think that SpamHaus is more trusted than the others you can use the following settings:
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

How many servers you configure and how you weight them is up to the user.

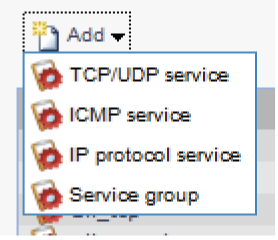
Note: Please refer to http://spamlinks.net/filter-dnsbl-lists.htm for more DNSBL server information.

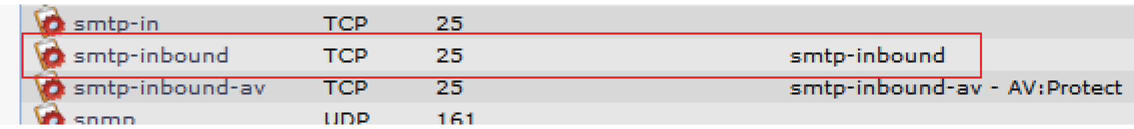
Step 9: Go to *Services*



Add *TCP/IP service* Object to include SMTP ALG for anti-spam

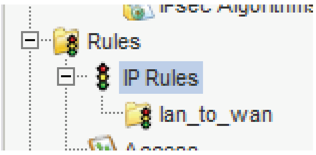
Or use predefine smtp-inbound object if you already configure predefine SMTP ALG for anti-spam as previous step mentioned

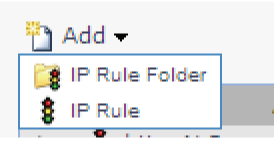




smtp-in	TCP	25	
smtp-inbound	TCP	25	smtp-inbound
smtp-inbound-av	TCP	25	smtp-inbound-av - AV:Protect
snmp	UDP	161	

Step 10 Go to *Rule> IP Rule*, Add *IP Rule*

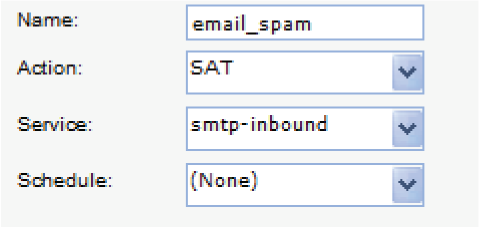




Step a:
In General tab

Name: email_spam
Action: *SAT*
Service: *smtp-inbound*

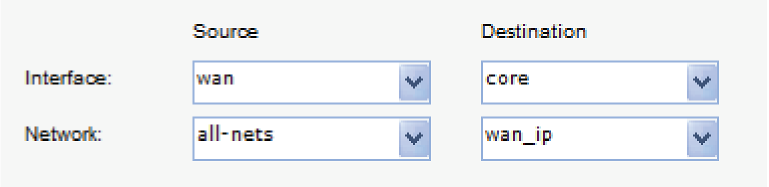
Note: Select smtp-inbound service object due to it includes SMTP ALG



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

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

Destination Interface: core
Destination Network: *wan_ip*

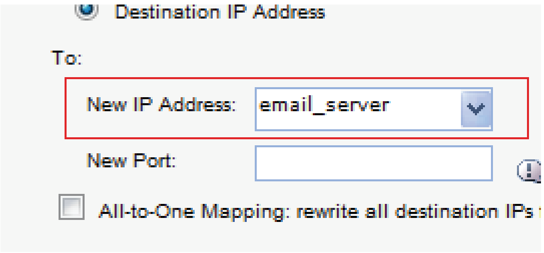


	Source	Destination
Interface:	wan	core
Network:	all-nets	wan_ip

In SAT tab

Select email_server object, or enter email server ip address

Note: This “email_server” object is just an example in this document. NetDefend firewalls don’t have this pre-defined object by default.



● Destination IP Address

To:

New IP Address: email_server

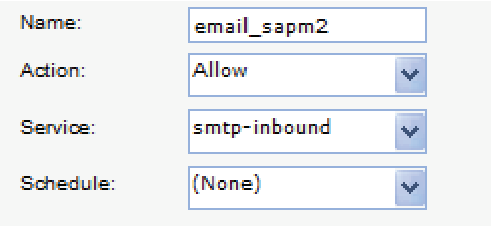
New Port:

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

Click *OK*

Step b: Add a rule
In General tab

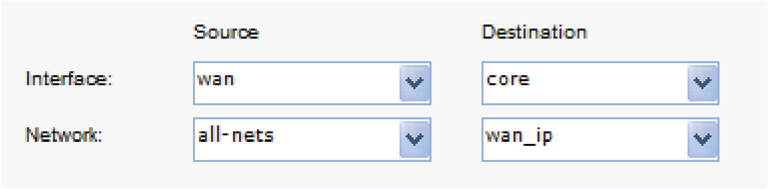
Name: email_spam2
Action: *Allow*
Service: *smtp-inbound*



Name:	email_sapm2
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 12: Click *Save and Active*