Пример настройки межсетевых экранов D-Link NetDefend

Настройка SMTP ALG для борьбы со спамом

Применимо к моделям: DFL-210/260/260E/800/860/860E/1600/1660/2500/2560

Прошивка: 2.27.01 и выше.

Почему антиспам?

Спам – это злоупотребление электронными системами обмена сообщениями при рассылке электронной почты и другой медиа информации. С ростом популярности интернета множеству людей докучают ежедневные спам сообщения. С системной точки зрения, спам сообщения являются нагрузкой не только для системных ресурсов, а и для полосы пропускания каналов связи. В семействе межсетевых экранов D-Link NetDefend мы обеспечиваем два метода для фильтрации спам сообщений – при помощи списка определённых спам отправителей в *Blacklist* и через *DNSBL* (DNS Blacklist). В этом документе вы можете найти пошаговую инструкцию по настройке антиспама. Перед началом, пожалуйста, учтите, что скриншоты в документе получены с прошивки версии 2.27.01. Если вы используете другую прошивку, то скриншоты могут отличаться от вашего интерфейса.

Как настроить антиспам

Предположим, что SUPERSTAR Corporation настраивает антиспам для блокировки спам сообщений, посылаемых локальным пользователям. После детального анализа, администраторы определили, что большинство спам сообщений приходят с hotmail.com, и поэтому они решили заблокировать все сообщения с Hotmail. Для более тщательной фильтрации спама, администраторы также используют последнюю информацию о спамерах с нескольких баз DNSBL (DNS Blacklist).

Для реализации данной задачи необходимо:

- Создать ALG для определённых служб
- Создать объект необходимой службы и привязать к нему соответствующий ALG
- Создать правила (IP Rules) и использовать в них, созданные объекты служб

ШАГ 1: ALG с AV/WCF

Перейдите в **Objects> ALG with AV/WCF** и добавьте новый *SMTP ALG* или отредактируйте существующий *SMTP-inbound.*

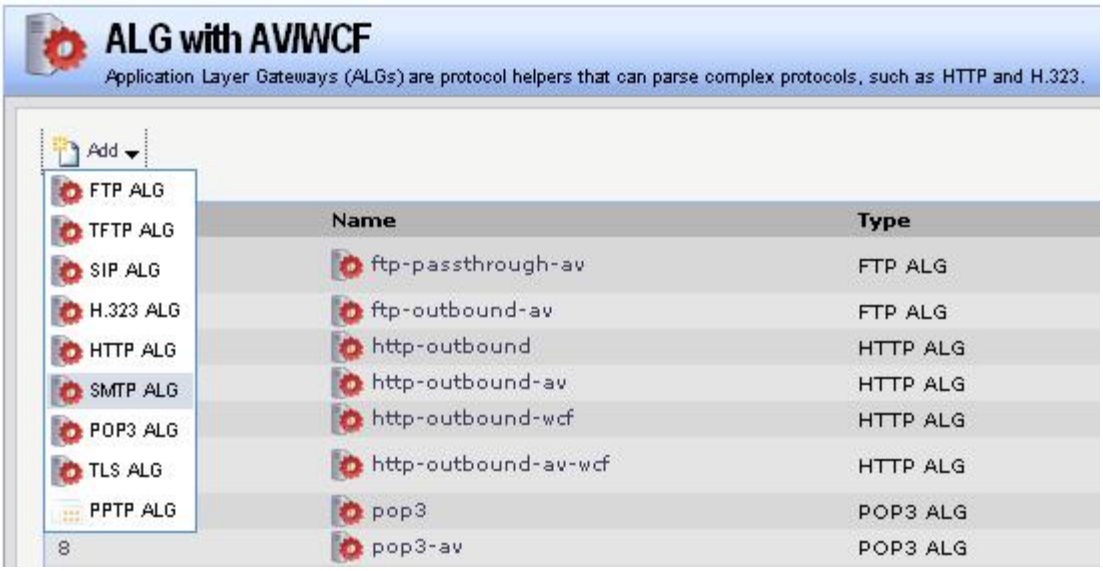

Рис 1: Добавление SMTP ALG

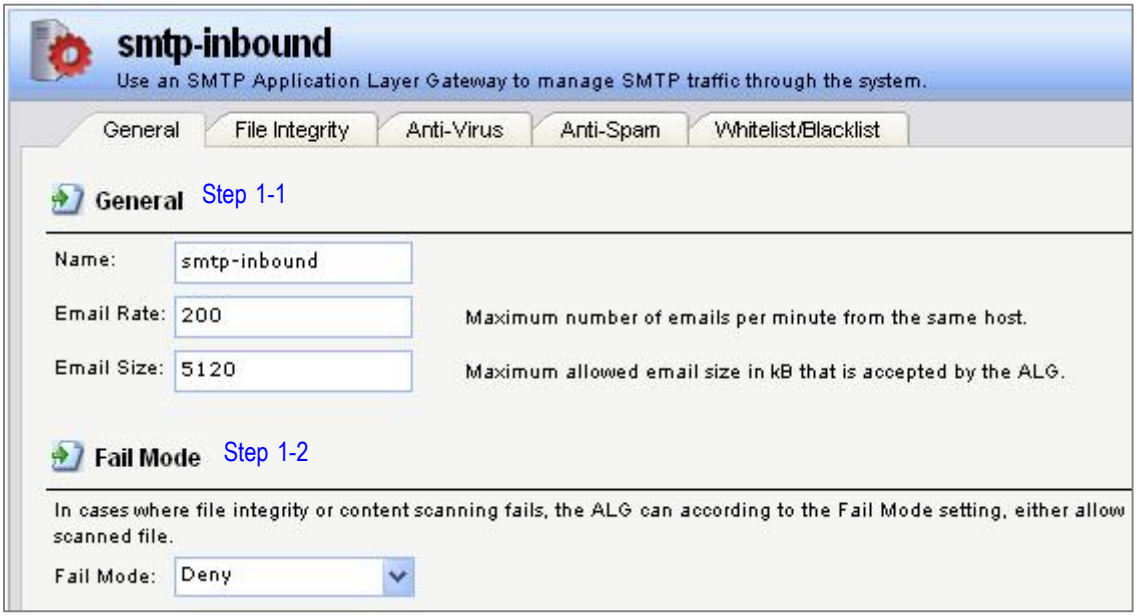

Рис 2: SMTP ALG, General

На вкладке General (Рис 2), заполните соответствующие поля:

Шаг 1-1: General

Name: smtp-inbound (может быть любое название, указанное пользователем)

Email Rate: 200

Email Size: 5120 (максимальный размер сообщения можно указать другой, но желательно не оставлять данное поле пустым, а ввести определённые ограничения)

Шаг 1-2: Fail Mode

Fail Mode: Deny

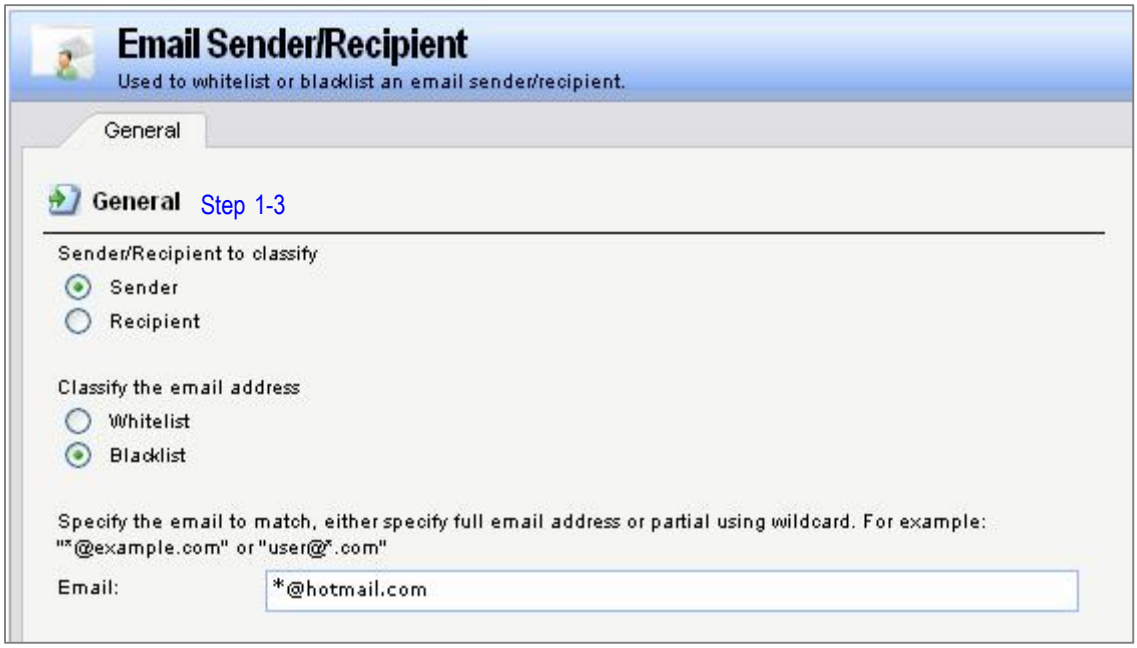

Рис 3: SMTP ALG. Whitelist/Blacklist

На вкладке Whitelist/Blacklist (Рис 3), добавьте домен, который вы хотите заблокировать.

Шаг 1-3: General

Выберите “Sender”

Выберите “Blacklist”

Email: *@hotmail.com

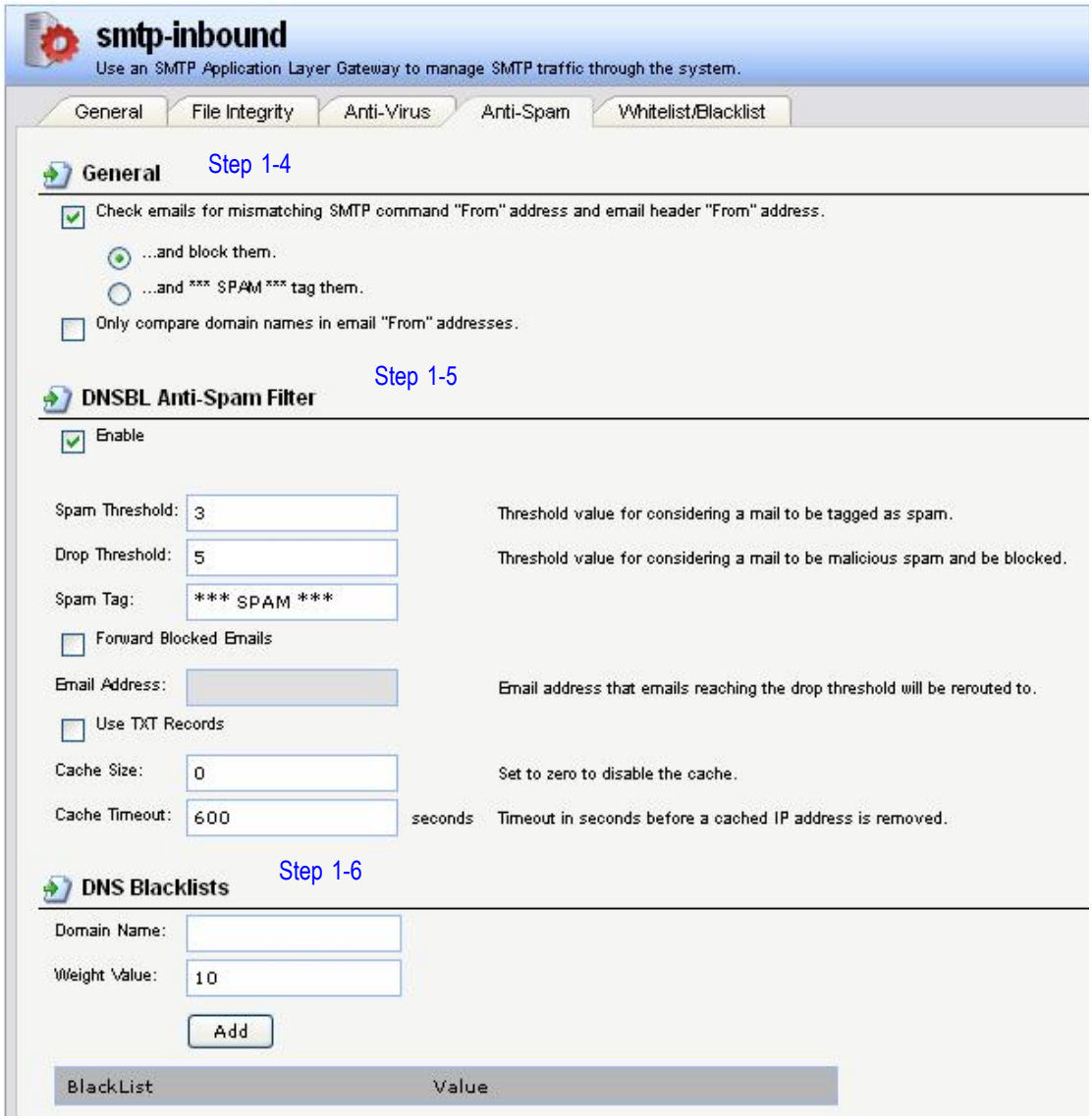

Рис 4: SMTP ALG. Anti-Spam

На вкладке Anti-Spam (Рис 4), заполните соответствующую информацию:

Шаг 1-4: General

Установите галочку в поле “Check emails for mismatching SMTP command “From” address and email header “From”address”

Выберите: “…and block them”

Шаг 1-5: DNSBL Anti-Spam фильтр

Установите галочку в поле “Enable”

Spam Threshold: 3

Drop Threshold: 5

Cache Size: 0

Cache Timeout: 600

Шаг 1-6: DNS Blacklist

Добавьте доменные имена и значения весов чёрных списков DNS.

sbl.spamhaus.org (вес = 1)

virbl.dnsbl.bit.nl (вес = 1)

bl.spamcop.net (вес = 1)

list.dsbl.org (вес = 1)

zen.spamhaus.org (вес = 1)

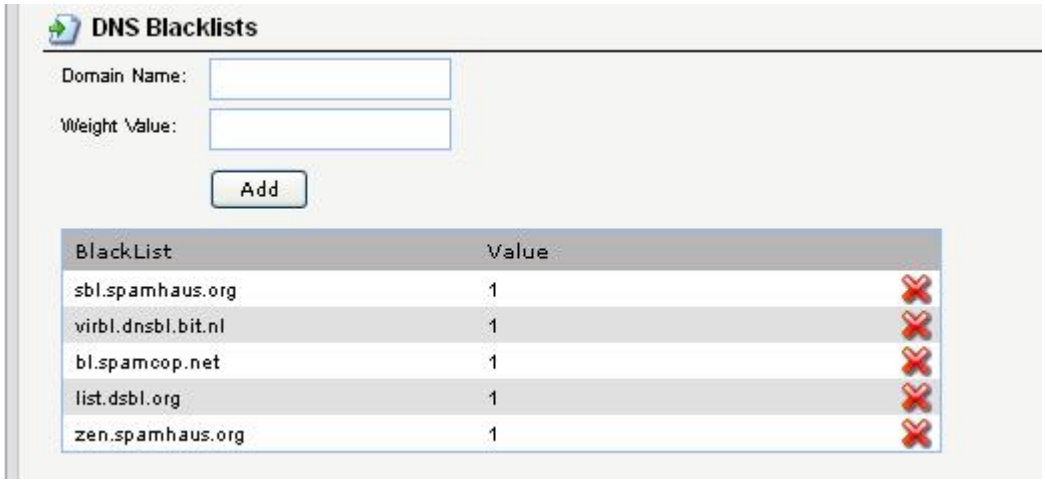

Рис 5: Чёрные списки DNS

Щёлкните OK

Когда доменное имя электронного сообщения, посланного спамером будет обнаружено в каком-либо чёрном списке DNS, то значение веса этого списка будет сохранено в системной памяти NetDefend. Потом межсетевой экран просуммирует соответствующие значения весов всех чёрных списков, в которых было обнаружено доменное имя спамера, и после этого сравнит результат со значениями, указанными в полях “Spam Threshold” и “Drop Threshold” настроек DNS Blacklists. Если суммарное значение будет эквивалентно или выше, этих значений, то электронное сообщение будет, или помечено как спам (*** SPAM ***) в поле "тема" данного сообщения и отослано, или отброшено.

Шаг 2: Service

Перейдите в **Objects> Services** и добавьте новую службу TCP/UDP service или отредактируйте существующую smtp-inbound. Объект данной службы появится в списке служб в правилах (IP rules) в следующих шагах по настройке межсетевого экрана.

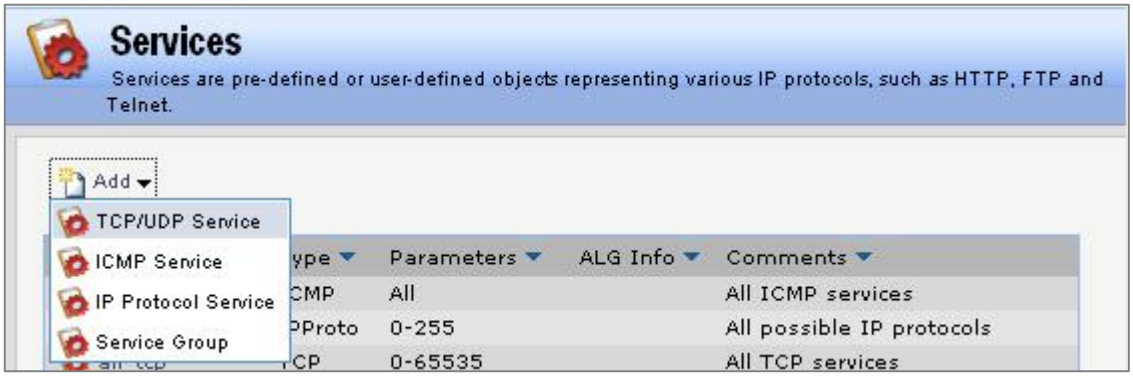

Рис 6: Добавление TCP/UDP службы

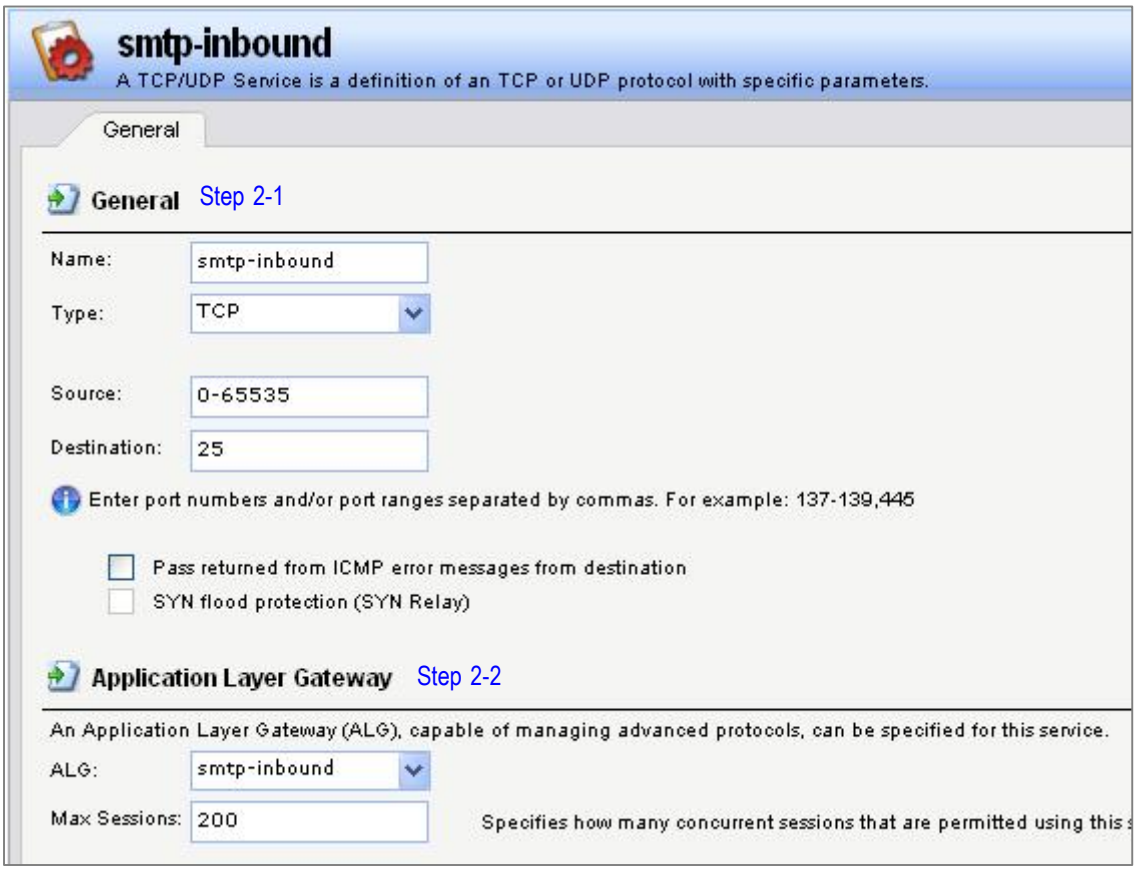

Рис 7: TCP/UDP Служба

На вкладке General (Рис 7):

Шаг 2-1: General

Name: smtp-inbound

Type: TCP

Source: 0-65535

Destination: 25

Шаг 2-2: Application Layer Gateway

Выберите Application Layer Gateway (ALG),который был создан в *ALG with AV/WCF* для этой службы.

ALG: smtp-inbound

Щёлкните OK

Шаг 3: Rules

Перейдите в **Rules> IP Rules** и добавьте новое правило (add *IP Rule)*.
Первое правило описывает установление соединения с внешнего публичного почтового сервера к внутреннему частному серверу, установленному в локальной сети. Так как внутренний почтовый сервер имеет собственный частный (серый) IP адрес и общий публичный IP, то необходимо использовать SAT для трансляции IP адреса назначения между ними. В качестве публичного IP адреса почтового сервера будет выступать IP адрес интерфейса wan1. Также, не забудьте добавить IP4 объект "серого" IP адреса почтового сервера в адресную книгу (Address Book).

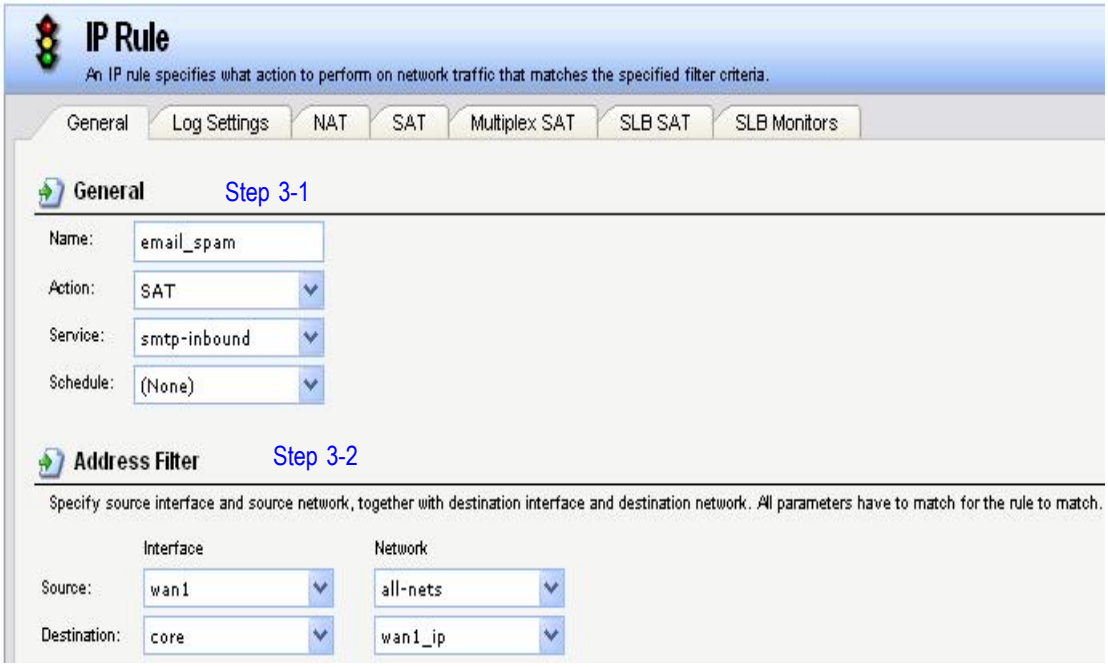

Рис 8: Rules, General

На вкладке General (Рис 8), заполните соответствующую информацию:

Шаг 3-1: General

Name: email_spam (может быть любое название, указанное пользователем)

Action: SAT

Service: smtp-inbound

Schedule: (None) (или любое другое расписание, заданное пользователем)

Шаг 3-2: Address Filter

Source Interface: wan1

Source Network: all-nets

Destination Interface: core

Destination Network: wan1_ip

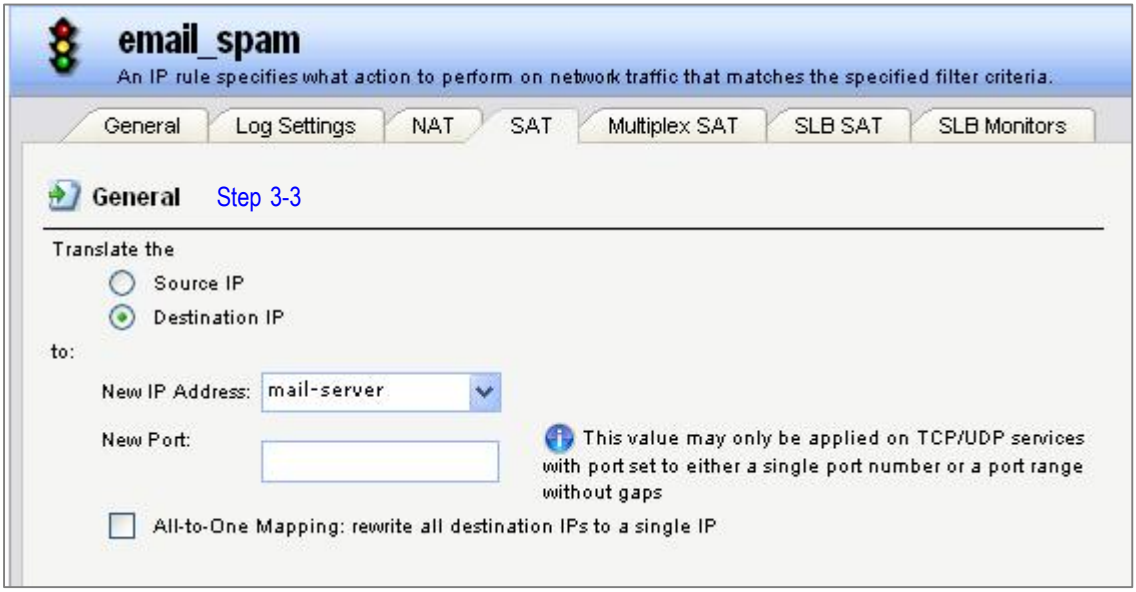

Рис 9: Rules, SAT

На вкладке SAT (Рис 9):

Шаг 3-3: General

Выберите “Destination IP”

New IP Address: mail-server

Щёлкните OK

Для продвижения пакетов, к предыдущему правилу SAT необходимо добавить второе правило с действием Allow. В списке правил, правило Allow должно находиться ниже правила SAT.

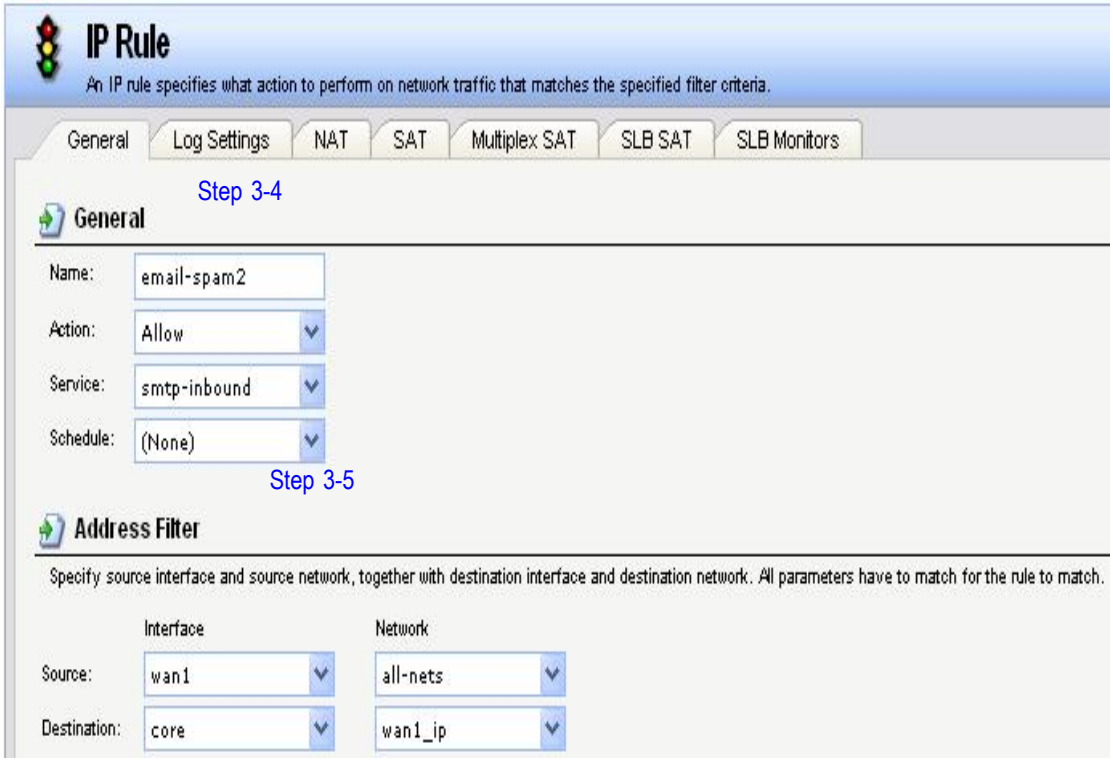

Рис 10: Rules, General

На вкладке General (Рис 10), укажите соответственно:

Шаг 3-4: General

Name: email_spam2 (определяется пользователем)

Action: Allow

Service: smtp-inbound

Schedule: (None) (определяется пользователем)

Шаг 3-5: Address Filter

Source Interface: wan1

Source Network: all-nets

Destination Interface: core

Destination Network: wan1_ip

Щёлкните OK

[[Сохраните и активируйте конфигурацию]]

Дополнительная информация.

Дополнительные примеры по расчету весов:

Межсетевые экраны NetDefend используют систему подсчёта весов для определения, является ли электронное сообщение спамом или нет. На межсетевых экранах NetDefend администратор может настраивать антиспам фильтр, проверяя отправителей и выставляя им соответствующие веса. Например, веса установлены, как указано ниже:

В DNSBL Anti-Spam фильтре,

Spam Threshold: 3

Drop Threshold: 5

В DNS Blacklist,

sbl.spamhaus.org (вес = 2)

virbl.dnsbl.bit.nl (вес = 1)

dnsbl.sorbs.net (вес = 2)

Пример 1:

Если отправитель почтового сообщения будет находиться во всех базах DNSBL, то межсетевой экран получит обратный позитивный результат = 1, 1, 1. Конечное значение позитивного результата будет 5= 2*1+1*1+2*1. Так как значение "Drop Threshold" выставлено в 5, то это почтовое сообщение будет отброшено.

Пример 2:

Если отправитель почтового сообщения будет находиться только в базе Spamhaus, то межсетевой экран получит обратный позитивный результат = 1, 0, 0. Конечное значение позитивного результата будет 2= 2*1+1*0+2*0. NetDefendOS не будет выполнять никаких действий над этим сообщением и просто перешлёт его почтовому серверу, так как значения триггеров не достигнуты.

Пример 3:

Если отправитель почтового сообщения будет находиться в базах Spamhaus и Sorbs Spammers, то межсетевой экран получит обратный позитивный результат = 1, 0, 1. Конечное значение позитивного результата будет 4= 2*1+1*0+2*1. Так как достигнуто значение "Spam Threshold" = 3 и не достигнуто значение "Drop Threshold" = 5, то

почтовое сообщение будет помечено, как спам и отправлено почтовому серверу. Т.е. если оригинальная тема почтового сообщения была, например, "Лучшие цены", то она будет изменена на "*** SPAM *** Лучшие цены", после чего сообщение будет отправлено получателю.

Вы можете присвоить любые значения весов определённым DNSBL серверам. Например, если вы считаете, что определение спама сервером Spamhaus является более точным, то вы можете присвоить более высокое значение веса для Spamhaus по сравнению с остальными серверами. Например:

Spamhaus – вес = 10

Sorbs – вес = 1

Server x – вес = 1

Server y – вес = 1

Server z – вес = 1

Server w – вес = 1

Spam Threshold - 5

Drop Threshold – 11

Для получения дополнительной информации о DNSBL серверах обращайтесь по следующей ссылке http://spamlinks.net/filter-dnsbl-lists.htm.