# How to Configure Custom Mail Gateway Rules

https://campus.barracuda.com/doc/53248821/

It is highly recommended that you contact Barracuda Networks Technical Support for help with these expert settings to configure custom rules for the Mail Gateway service.

The following article provides information and examples on how to configure custom mail gateway rules. For the Mail Gateway service of the Barracuda NextGen Firewall F-Series, you can configure the following types of rules:

- **Pre Settings** – These rules are processed before all other mail gateway settings.
- **Post Settings** – These rules are processed after all other mail gateway settings.

## Configure Custom Rules

To configure custom rules for the mail gateway, complete the following steps.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Mail-Gateway > Mail Gateway Settings**.
2. In the left menu, click **Advanced Setup**.
3. Click **Lock**.
4. In the **Expert Settings** section, configure your custom rules. In the following table, complete the steps for the type of rules that you want to configure.

| Task | Steps |
|---|---|
| To configure Pre Settings. | 1. From the **Enable Pre Settings** list, select *yes*.<br>2. Next to **Pre Settings**, click **Set** or **Edit**.<br>3. In the **Pre Settings** window, configure your custom rule. |
| To configure Post Settings. | 1. From the **Enable Post Settings** list, select *yes*.<br>2. Next to **Post Settings**, click **Set** or **Edit**.<br>3. In the **Post Settings** window, configure your custom rules. |

The custom rules can be added to all five levels of an SMTP mail transmission. For more information, see RFC 2821 at http://www.ietf.org/rfc/rfc2821.txt.

| Level | Type | Description |
|---|---|---|
| **1** | Connect | This is the connection level of the mail gateway server (like that banned hosts rule will affect the connect level). |
| **2** | Helo | This is the SMTP greeting level (SMTP "helo" or "ehlo" command). |
| **3** | Sender | In this level, the sender of a mail is announced (SMTP "mail from:" command. For example, banned sender rule will affect the sender level). |

| | | |
|---|---|---|
| **4** | Recipient | The recipient of a mail is announced in this level (SMTP "rcpt to:" command. For example, banned recipient or rewrite recipient rule will affect the recipient level). |
| **5** | Data | In the last level of a SMTP transmission, the mail body (data) is transmitted. For example, the subject is part of the mail body (banned subjects rule will therefore affect the data level). |

   - For more information on the abstract rule language that should be used when configuring custom rules, see the following Abstract Rule Language section.
   - For examples of custom rules, see the following Example Custom Rules section.

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

## Abstract Rule Language

The following sections provide information on the syntax and commands that can be used when configuring custom rules.

#### General Syntax

- Comment lines are ignored by the abstract rule parser. Format comment lines as follows: `// Comment line`
- Separate expressions with spaces. For example, a double-slash (`//`) must be followed by a space.
- Quote string variable values. For example: `"string"`
- Separate parameters with a comma (`,`).

#### Expressions

An expression assigns a value to an variable. You can combine multiple expressions with logical operators.

| Usage | Example |
|---|---|
| `<variable> <operator> <value>` | `fromdomain <> "sample.com"` |

You can use the following variables and operators:

### Operators

| Operator | Description |
|---|---|
| = | Text Operator. Equality. |

| | |
|---|---|
| **<>** | Text Operator. Inequality. |
| **" "** | Numerical Operator |
| **AND** | Logical Operator |
| **OR** | Logical Operator |

### Variables

| Variable | Type | Level | Description | Special Value |
|---|---|---|---|---|
| **result** | integer | all | The return code of rule parser. | - |
| **peerip** | string | connect (1) | The IP address of peer (client). | - |
| **peername** | string | connect (1) | The hostname of peer (client). | - |
| **inbound** | boolean | connect (1) | 0=outbound; 1=inbound (that is mail reception on internal IP). | - |
| **helo** | string | helo (2) | The SMTP greeting name (ehlo/helo). | - |
| **from** | string | sender (3) | The sender email address after rewriting. | **null** |
| **fromuser** | string | sender (3) | The local part of the sender email address after rewriting. | - |
| **fromdomain** | string | sender (3) | The domain of the sender email address after rewriting. | - |
| **to** | string | rcpt (4) | The recipient email address after rewriting. | **postmaster** |
| **touser** | string | rcpt (4) | The local part of the recipient email address after rewriting. | - |
| **todomain** | string | rcpt (4) | The domain of the recipient email address after rewriting. | - |
| **orig_[…]** | string | sender (3)<br>rcpt (4) | Adds **orig_** to the email address variable. For example:<br>`orig_fromdomain`<br>Reflects the email address before rewriting. | - |
| **subject** | string | data (5) | The subject of the mail body. | - |

### ACTION Command

The `ACTION` command specifies the actions to be performed by the Mail Gateway service. Lines with the `ACTION` command require a semicolon (`;`) at the end of the line. Expressions with the `ACTION` command are space-delimited.

| Usage | Examples |
|---|---|
| `ACTION ("<action>", "<parameters>");` | `ACTION ("rewrite", test@sample.com);`<br>`ACTION ("event", "1, Event has been triggered!");` |

Even if there are no parameters required for an action (such as the **Quit** action), you must still enter the second set of quotation marks. For example:

```
ACTION ("quit, "");
```

You can use the following actions:

| Action | Description | Level | Parameters |
|---|---|---|---|
| **ruledebug** | View rule debug messages in logs. | All | - |
| **smtpdebug** | View SMTP debug messages in logs. | All | - |
| **deliverdirect** | When specified in level 3, it affects the whole mail object. Otherwise, it affects the current rcpt. | > 2 | Target IP address. |
| **bind** | When specified in level 3, it affects the whole mail object. Otherwise, it affects the current rcpt.<br>• **extern** – Use first configured external bind IP address.<br>• **intern** – Use first configured internal bind IP address.<br>• To specify an **Explicit Service IP** [inbound-flag is either **0** (default, outbound) or **1** (inbound)]. | > 2 | • extern<br>• intern<br>• bind IP<br>• [inbound-flag] |
| **quit** | Close the connection. | All | - |
| **deny** | Deny mail delivery of current mail. | > 2 | Description. |
| **drop** | Drop current recipient. | 4 | - |
| • **rewrite**<br>• **rewriteuser**<br>• **rewritedomain** | If specified in level 3, rewrite sender (-part). Otherwise, rewrite current recipient (-part) | > 2 | Mailboxes, local-parts, or domains. |
| • **clone**<br>• **cloneuser**<br>• **clonedomain** | Clone current recipient (-part). | 4 | List of mailboxes, local-parts, or domains. |
| **priority** | Assign scheduling priority. Allowed parameters:<br>• low<br>• normal<br>• high<br>• urgent | > 2 | Priority. |

| | | | |
|---|---|---|---|
| **event** | Trigger an event. Allowed parameters:<br>• **0** – Info<br>• **1** – Notice<br>• **2** – Error description of event; will be displayed in **Events** if the event is triggered. | All | Event type and description. |
| **none** | Do nothing. | All | - |

#### IF Statements

An IF statement is comprised of the following:

- A test expression that specifies conditions to be met.
- A statement that declares actions to be performed when the conditions are met.

| Usage | Example |
|---|---|
| `IF (<test-expressions>) THEN <statement>; ENDIF` | `IF (fromdomain = "sample.com") OR (fromuser = "spammer") THEN ACTION ("deny", "Banned Sender"); ENDIF` |

You can use the following statements:

| Statement | Description |
|---|---|
| **IF** | Begin IF test block. |
| **ELSE** | Begin ELSE block. |
| **ELSEIF** | Begin ELSEIF block. |
| **ENDIF** | END IF block. |
| **THEN** | THEN statement for IF tests. |

#### RETURN Command

The RETURN command exits the current level function, so subsequent instructions will no longer be performed.

### Usage

Lines with the RETURN command require a semicolon (;) at the end. Expressions with the RETURN command are space-delimited; this is also valid for the semicolon after the command**:**

**RETURN ;**

## Example Custom Rules

The following sections provide examples of the custom rules that you can configure for the Mail Gateway service.

### Denying mail with a specific greeting name

Mail delivery from mail servers that send "spam" as the greeting name should be denied. Enter the following rule language code into the **Helo** field of the Pre or Post Settings:

```
IF (helo = "spam") THEN ACTION ("quit", ""); RETURN; ENDIF
```

### Changing the priority of an email

The priority of emails arriving from a specific address should be changed to "high". Enter the following rule language code into the **Sender** field of the Pre or Post Settings:

```
IF (from = "boss@company.com") THEN ACTION ("priority", "HIGH"); ENDIF
```

### Cloning an email from a specific address

Emails arriving from a specific address should be cloned and distributed to multiple recipients. Enter the following rule language code into the **Recipient** field of the Pre or Post Settings:

```
IF (from = "sender@company.com") THEN ACTION ("clone", "rcp1@company.com,
rcp2@company.com,rcp3@company.com"); ENDIF
```

### Redirecting spam

Spam emails should be redirected. The following rule language code can be entered in any expert Pre Settings. The following syntax applies:

```
ACTION ("redirect", "/opt/phion/bin/spam_redirect.sh");
```

For this example, the referenced `spam_redirect.sh` script that is required for email redirection could read as follows:

```
#!/bin/bash # $1 ... path to mail files # $2 ... spoolid ## this script
redirects mails with "[SPAM]" within subject # to an archive mail account
DSTMAILBOX=mailboxname DSTDOMAIN=domainname DSTIP=serverip
BODY_FILE=$1$2".body" ENV_FILE=$1$2".env" TMP_FILE="/tmp/"$2".env"
```

```
SUBJECT=`cat $BODY_FILE | formail -c -x subject | grep "[SPAM]" | sed -e
's/.*\[SPAM\].*/[SPAM]/g'` if [ "_$SUBJECT" = "_[SPAM]" ]; then # redirect to
spam mail box # 1. remove lines that start with "rcpt" # 2. insert infos for
delivery to spam archive # (assumption: $DSTIP is an internalmailserver) mv
$ENV_FILE $TMP_FILE cat $TMP_FILE | grep -v -e "^rcpt" -e"^recipient" -
e"^numrcpts" > $ENV_FILE echo "numrcpts 1" >> $ENV_FILE echo "recipient" >>
$ENV_FILE echo "rcpt id 0" >> $ENV_FILE echo "rcpt user $DSTMAILBOX" >>
$ENV_FILE echo "rcpt domain $DSTDOMAIN" >> $ENV_FILE echo "rcpt status 0" >>
$ENV_FILE echo "rcpt deliverdirect $DSTIP" >> $ENV_FILE echo "rcpt bindtype
1" >> $ENV_FILE echo "rcpt bind intern" >> $ENV_FILE rm -f $TMP_FILE fi echo
"0"
```

This script must be made executable. Enter: `chmod 777 /opt/phion/bin/spam_redirect.sh`