Prevent data leaks in SkyConnect with strong security

Overview

SkyConnect has multiple features to prevent data leakages. This topic describes the following:

a. Mail policies to control mail flow which can be used for inbound, internal and outbound mail.

b. Data leak prevention for the Inbound mail flow.

c. Data leak prevention for Outbound mail.

Mail polices

What are mail policies and how do they work?

Mail policies is an advance security feature of SkyConnect which allows you to control mail flow from and to users and groups on your domain.

For example, using mail policies you can allow only a certain set of users to communicate with users on Gmail. Similarly, another set can only communicate with users of your domain. Or you can control who can send out attachments of a certain type and who is allowed to receive attachments.

Types of policies

When defining mail policies, you have to define **sender and recipient policies**. Sender policies are applied when the user is sending mail and Recipient policies are applied when the user or group is receiving mail.

So if you want to stop all communications between a user john@yourdomain.com and a Gmail user jane@gmail.com, then you will have to define a sender and a recipient policy for john@yourdomain.com.

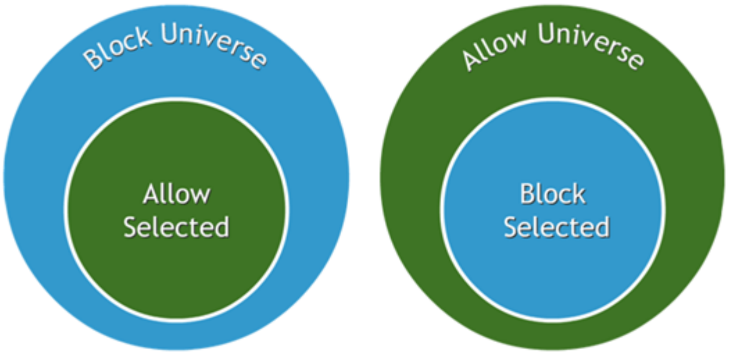
Similarly, if you have a distribution list called all@yourdomain.com which is to be used only for internal purposes and you want to block all external communications to this group id, you will have to define a sender and recipient policy for this id.

If a certain id can only receive mail such as info@yourdomain.com but cannot be used to send out mail, then a sender policy has to be defined for this user and no recipient policy.

Defining a policy

Sender and recipient policies are defined by a **Default** action **and zero or more exceptions** to the default action. The **Default action** can be either **Allow** or **Block**.

Exceptions have an **associated action which is opposite to the default action**. For example, if the Default action is Block, then the exceptions will define all the conditions under which the default action of Block is not applied and the mail flow is allowed. Similarly, if the Default action is Allow, then the exceptions will define all the conditions under which the mail flow is to be blocked.



Mail Policy Definition

The **conditions for the exceptions** are defined using the following parameters:

- Sender for recipient policies and Recipient for sender policies
- Mail size
- Attachment size

Note: After encoding in the MIME format, the size of mail body or attachment increases by 33%. The encoding is required to convert 8 bit data to 7 bit data (suitable for transmission over the network). Hence to block the a mail of size 1 MB or 1024 KB, add a policy for mail size 1024 * 1.33 ~ 1366 KB. In some cases where the mail/attachments may not be encoded, the mail/attachment size limit will be 1.33 MB.

- Attachment count
- Subject text
- Body text
- Attachment type

For each user or group you want to control, define the sender and recipient policies in a table as follows

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy

Sample Mail Policies

Allow users to receive mail but not to send

User ID	Default Sender Policy	Exceptions to the Default Sender Policy	Default Recipient Policy	Exceptions to the Default Recipient Policy
all users of domain	block	none	allow	none

Allow domain users to receive mail but restrict them from sending mail to any external domain

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all users of domain	block	allow when recipient is in domain yourdomain.com	allow	none

Restrict domain users to send and receive mail mail from yahoo.com and gmail.com

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all users of domain	allow	1. block when recipient is in domain yahoo.com 2. block when recipient is in domain gmail.com	allow	1. block when sender is in domain yahoo.com 2. block when sender is in domain gmail.com

Disable all users from sending emails to a particular email id like md@domain.com

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all users of domain	allow	block sending to md@domain.com	allow	none

Allow only domain users to send emails to the group all@yourdomain.com

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all@yourdomain.com	allow	none	block	allow when sender is in domain yourdomain.com

Allow only users in group mgmnt to send emails to the group all@yourdomain.com

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all@yourdomain.com	allow	none	block	allow when sender is in group mgmnt@yourdomain.com

Allow only user md@yourdomain.com to send emails to the group all@yourdomain.com

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all@yourdomain.com	allow	none	block	allow when sender is md@yourdomain.com

Block only users of the group tempstaff@yourdomain.com to send emails to the group all@yourdomain.com

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all@yourdomain.com	allow	none	allow	block when sender is in tempstaff@yourdomain.com

Block users from sending attachments to Gmail

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all@yourdomain.com	allow	block when attachment count is greater than or equal to 1 and recipient is in domain gmail.com	allow	none

Block users from sending more than 5 attachments

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all@yourdomain.com	allow	block when attachment count is greater than 5	allow	none

Block users from sending more than 2 MB of attachments

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all@yourdomain.com	allow	block when attachment size is greater than 2048	allow	none

Block users from sending more mail with Happy Diwali in subject

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all@yourdomain.com	allow	block when subject has Happy Diwali	allow	none

Block users from sending gifs attachments

User ID	Default Sender Policy	Exceptions To The Default Sender Policy	Default Recipient Policy	Exceptions To The Default Recipient Policy
all@yourdomain.com	allow	block when attachment type is gif	allow	none

Configure mail policies for your domain

Mail policies are configurable via the back-end and we request you fill this spreadsheet (https://skyconnect.mithi.com/res/submitting-mail-policies-requests.xls) with the details and raise a ticket to the Mithi Support team (https://docs.mithi.com/home/how-to-access-mithi-help-desk#raising-a-ticket). We will configure the same for you.

Data leak prevention for the Inbound mail flow

In addition to the mail policies which can control inbound, internal and outbound mail flow, you can configure some additional data leak prevention rules for the Inbound mail flow.

Your domain can be configured to **Intercept, Modify or Monitor** the incoming mail flow.

The **Intercept** actions possible are:

- Deliver now
- Delete message
- Quarantine
- Change recipient

The **Modify** actions possible are:

- Clean cleanable malware, delete those that cannot be cleaned
- Stamp the body with a cautionary message.
- Tag the subject with keywords which alert the recipient that the mail is from an external sender
- Delete matching attachments

The way to **Monitor** such Inbound mail would be to:

- Send an email notification to a predefined email id
- Send a bcc of the inbound mail to a predefined email id.

These actions can be taken for mails which match one or more of these **conditions**

- all inbound mail
- all inbound mail for a selected set of users on your domain
- mail from a selected set of senders to any user on your domain
- mail from a selected set of senders to a select set of recipients on your domain
- all mail with certain attachments

Configure the DLP rules for your domain

Inbound data leak prevention rules and mail policies are configurable via the back-end and we request you fill this spreadsheet (https://skyconnect.mithi.com/res/submit-dlp-requests-for-inbound-and-outbound-mailflow.xls) with the details and raise a ticket to the Mithi Support team (https://docs.mithi.com/home/how-to-access-mithi-help-desk#raising-a-ticket). We will configure the same for you.