SecurityGateway

Protecting Microsoft 365 with SecurityGateway

SecurityGateway protects businesses against inbound threats such as spam, phishing, viruses, and spyware, and outbound threats such as leaks of sensitive information. It works with any mail server or hosted mail service, including Microsoft Exchange and Microsoft 365.

This guide provides businesses using Microsoft 365 with step-by-step instructions for filtering inbound and outbound mail using SecurityGateway for Email.

Overview

PART 1: Configure Microsoft 365 to Route Outbound Mail Through SecurityGateway

Follow the steps below to configure Microsoft 365 to route outbound mail through SecurityGateway

1. Log in to the Microsoft 365 admin center.
2. Click **Admin/Exchange/Exchange Admin Center.**
3. Select **Mail Flow > Connectors.** All currently existing connectors for your organization will appear.
4. Click on the plus symbol (**+**) to add a new connector.
5. Under **Select your mail flow scenario**, select the following:

   From: Microsoft 365
   To: Partner organization
6. Click **Next.**
7. Type a name and description for the new connector.
8. Check **Turn it on** and click **Next.**
9. Ensure **Only when email messages are sent to these domains** is checked, and then click the plus (**+**) icon.
10. In the **Add Domain** dialog box, type a single asterisk (*) to use as a wildcard, and then click **OK**. This forwards your outbound email to SecurityGateway.
11. Select **Route email through these smart hosts**, and then click on the plus (+) icon.

    The add smart host dialog box appears
12. Type the fully-qualified domain name (FQDN) of your SecurityGateway server (Example: hostname.domain.com).
13. Click **Save**, and then click **Next.**
14. Choose if you want to have all emails use TLS when sending to SecurityGateway, and then click **Next.**
15. To validate the connector, type a recipient email address on a domain outside of your organization.
16. Once the connector is successfully validated, click **Save.**

PART 2: Configure SecurityGateway

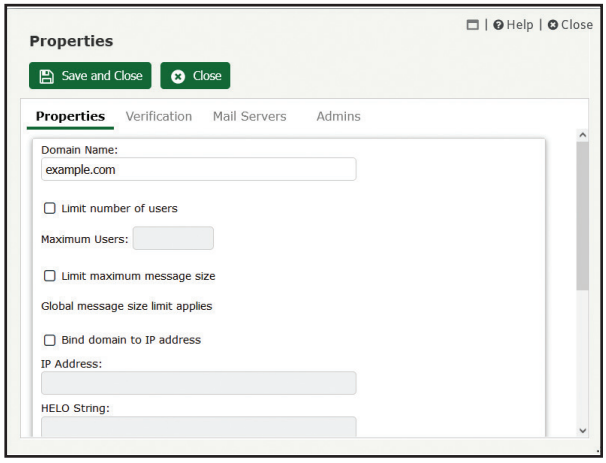

Figure 2-1

1. Add Domain in SecurityGateway

A. Log into SecurityGateway with your Global Administrator account.
B. Click **Setup/Users | Accounts | Domains and Users.**
C. Under the Domain List, select **New.**
D. Enter the domain name and then click on **Save and Close.**
[Figure 2-1]

2. Configure a User Verification Source

This option is used to verify accounts on Microsoft 365 during incoming and outgoing email transfer.

Follow the steps below to allow SecurityGateway to utilize Microsoft 365 as a user verification source.

In Azure Active Directory:

1. Navigate to the **App Registrations** page in Azure AD.
2. Select **New Registration.**
3. Enter an application name in the Name field.
4. Select **Register.**
5. Make note of the Application ID.
6. Select **API Permissions.**
7. Select **+ Add a permission.**
8. Select **Microsoft Graph.**
9. Select **Application Permissions.**
10. Select **Group.Read.All** and **User.Read.All.**
11. Select **Add permissions.**
12. Click the **Grant admin consent for...** button.
13. Click **Yes.**
14. Select **Certificates & Secrets.**
15. Click **+ New Client Secret.**
16. Enter a description in the description field.
17. Select the radio button to determine how long the password will be valid.
18. Make note of the generated password in the Value field as this password will not be viewable again.

In SecurityGateway:

1. Login to SecurityGateway as a global administrator.
2. Select **Setup/Users.**
3. Select **Accounts.**
4. Select **User Verification Sources.**
5. Click on **New.**

6. Select **Office 365** in the **Type** drop-down menu. [Figure 3-1]
7. Enter a description.
8. Enter the Microsoft 365 domain name in the **Domain Name** field.
9. Select the **Cloud Type** in the drop-down menu. For most configurations, the option will be set to **Global**. [Figure 3-2]
10. Enter the Application ID from Azure AD in the **Service Principle** field. This can be found on the Overview page of the app registration in Azure AD.
11. Enter the password generated in Azure AD in the **Password** field.
12. Click **Save and Close.**

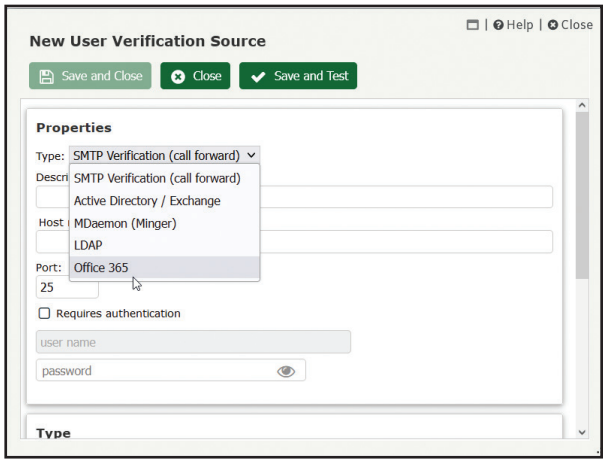

Figure 3-1

3. Configure Domain Mail Servers

These are the servers on which your users have their email accounts and where their messages are stored (in this case it is Microsoft 365). When SecurityGateway receives a message for a verified user of one of your domains, it will attempt to deliver the message to the mail servers associated with that domain.

Follow the steps below to add a Microsoft 365 server as a Domain Mail server in SecurityGateway.

1. Log into SecurityGateway.
2. Select **Setup/Users.**
3. Select **Mail Configuration.**
4. Select **Domain Mail Servers.**
5. Click on **New.**
6. In the **Properties** section, enter the Domain Mail Server description.
7. In the **Hostname or IP** field, enter the host name, following the example below:

   If the Microsoft 365 domain is domain.com use the following:

   domain-com.mail.protection.outlook.com

8. Enter the port number for SMTP connections (default 25).
9. Select **Requires SMTP Authentication** if required and enter the Username and Password. [Figure 3-3]
10. In the **Type** section, click **This server is a default mail server** if you would like this mail server to be used for any domains that have not been assigned their own mail server. Domains that do not have a defined domain mail server will use this server to route mail.
11. Use the **Available Domains** section to specify which domains will use this mail server for routing mail. Click on the domain name and use the right arrow button to move it to the **Selected Domains** column.
12. Click **Save and Close.**

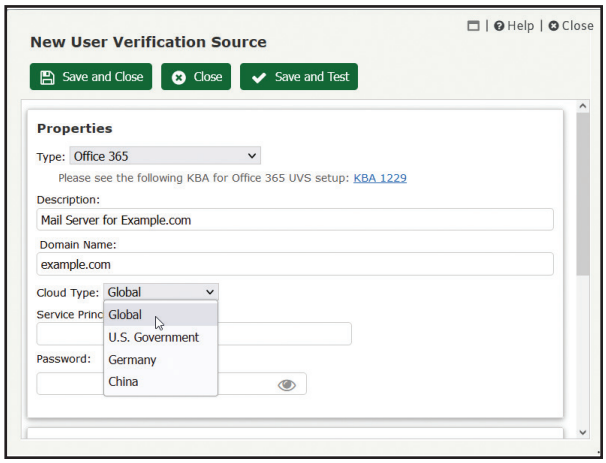

Figure 3-2

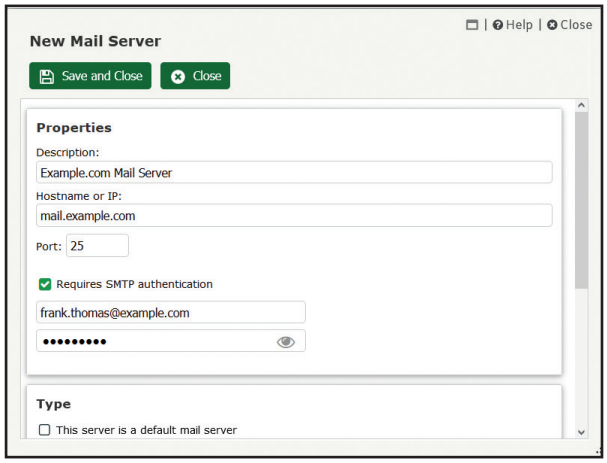

Figure 3-3

PART 3: Change DNS Settings

The final step is to configure your DNS records to route your domain's mail to your SecurityGateway server.

1. Add an 'A' record in your DNS settings to point your host name (ie. sg.example.com) to the static IP address of the SecurityGateway server.
2. Configure your MX record to direct inbound mail to your SecurityGateway server.

Host/Sub-domain	MX Server	Priority
example.com	sg.example.com	10

3. Create an SPF record for your Microsoft 365 domain. An SPF record can be added to the TXT Records in DNS.

Name	Value	
example.com	v=spf1 a mx a:sg.example.com	include:spf.protection.outlook.com- all

4. Validate your DNS settings and wait for the approval from your provider which can take up to 2 days.

If everything is set up correctly then you are ready to use SecurityGateway in front of Microsoft 365 for both incoming and outgoing mail filtering.