# 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 Outbound Email (Microsoft 365 mailbox > SecurityGateway > Internet)

### 1. Create connectors in Microsoft 365 to relay to SecurityGateway

A. Log in to the Microsoft 365 admin center.

B. Click **Admin | Admin Center | Exchange | Exchange Admin Center.**

C. Select **Mail flow | Accepted domains.**

D. Edit your domain and switch your accepted domain type from ‘Authoritative’ to ‘Internal Relay’ which is important until account synchronization is done with SecurityGateway. (You will need to switch back to Authoritative once all available accounts in Microsoft 365 have been added in SecurityGateway.)

E. To create a connector, select **Mail Flow | Connectors.**

F. Click on the plus symbol (**+**) to add a new connector.

**Note:** If any connectors already exist for your organization, you can see them listed here.

G. Under **Select your mail flow scenario**, select the following:

- From: Microsoft 365
- To: Your organization’s email server

H. Click **Next.**

I. Type a name and description for the new connector - ie “SMTP- Outbound”.

J. Check the options **Turn it on** and **Retain internal Exchange email headers.**

K. Click **Next.**

L. Select the first option **Only when I have a transport rule set up that redirects messages to this connector** and click **Next.**

M. In the **Routing Method** section, enable the option to **Route email through these smart hosts.**

N. Click the plus sign (**+**). The **Add smart host** dialogue box appears.

O. Type the fully-qualified domain name (FQDN) of your SecurityGateway server. The FQDN is typically in the format of hostname, domain. com or the static IP address.

P. Click **Save**, and then click **Next.**

Q. Choose whether you want to have all emails use TLS when sending to SecurityGateway, and then click **Next.**

R. To validate the connector, type a recipient email address on a domain outside of your organization.

S. Once the connector is successfully validated, click **Save.**

T. If the connector does not validate, double-click the message displayed to get more information and see **About fixing connector validation errors** for help resolving issues.

### 2. Create a rule to route all outgoing emails using the above connector

A. In Exchange Admin Center, select **Mail flow** | **Rules.**

B. Click on the plus symbol (**+**) and select **Create a new rule**.

C. Give an appropriate name to the rule.

D. Click the **More Options** link.

E. Under **Apply this rule if**, select **The recipient** | **is external/internal** | select **Outside the organization** | **OK.**

F. Under **Do the following,** select **Redirect the message to** | **the following connector** | select the connector which you created in the above section | **OK.**

G. Click **Save** to save the rule.

You now have all outgoing mail from Microsoft 365 redirected to SecurityGateway for filtering prior to delivery to the recipient address.

## PART 2: Configure Incoming Email (Internet > SecurityGateway > Microsoft 365 Mailbox)

### 1. Create a new connector in Microsoft 365 to relay from SecurityGateway

A. Log in to the Microsoft Microsoft 365 admin center.

B. Click **Admin | Admin Center | Exchange | Exchange Admin Center.**

C. To create a connector, select **Mail Flow | Connectors.** All currently existing connectors for your organization are displayed.

D. Click on the plus symbol (**+**) to add a new connector.

E. Under **Select your mail flow scenario**, select the following:
**From**: Your organization's email server
**To**: Microsoft 365

F. Click **Next.**

G. Type a name and description for the new connector.

H. Check **Turn it on** and **Retain internal Exchange email headers**, and then click **Next.**

I. To identify your SecurityGateway server, either enter the domain name by selecting the first option, or if the SecurityGateway server has a static IP (recommended) then add the IP by selecting the second option.

J. Click **Next.**

K. Confirm what you entered and click **Save.**

# PART 3: Setup SecurityGateway

## 1. Add Domain

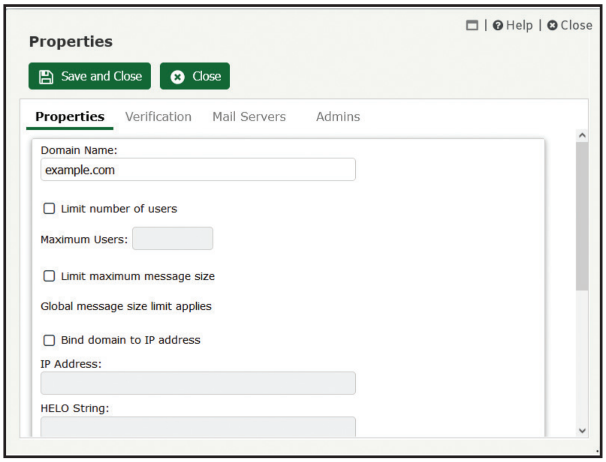
A. Log into SecurityGateway with your Global Administrator account.

B. Click **Setup/Users | Accounts | Domains and Users.**

C. Under the Domain List, select **New.**

D. Enter the domain name and click on **Save and Close.**

[Figure 3-1]



Domain Name: example.com

□ Limit number of users

Maximum Users:

□ Limit maximum message size

Global message size limit applies

□ Bind domain to IP address

IP Address:

HELO String:

Figure 3-1

## 2. Configure a User Verification Source

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

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

**Note:** To allow SecurityGateway to access the Microsoft 365 tenant, the Microsoft 365 plan requires Exchange Online. Please make sure the Microsoft 365 plan includes this feature.

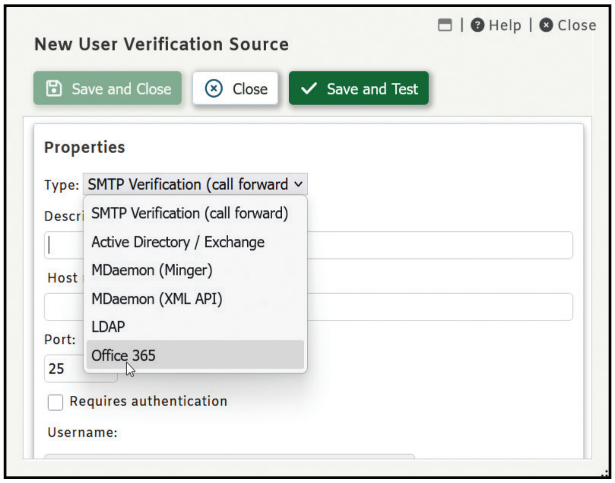
- SecurityGateway requires a service principal that has been granted permission to access the Microsoft 365 tenant. This makes it possible for SecurityGateway to utilize Microsoft 365 as a user verification source.
- Microsoft 365 uses Azure Active Directory as its directory service. A PowerShell module must be installed first. PowerShell 5.1 or higher is required on a 64-bit operating system in order to operate correctly. PowerShell 5.1 is the default build for Windows 10 and Windows Server 2016. On servers running previous operating systems, it will need to be installed from the Windows Management Framework.
- Install and Configure Windows Management Framework (WMF) 5.1.
- Connect to Microsoft 365 PowerShell.

**When the PowerShell module has been installed, follow the steps below to create a service principle for SecurityGateway.**

1. Open PowerShell.
2. Use one of the following commands to connect to the AD Azure tenant:
   - Microsoft 365 Worldwide (+GCC): **Connect-MsolService -AzureEnvironment AzureCloud**
   - Microsoft 365 Germany: **Connect-MsolService -AzureEnvironment AzureGermanyCloud**
   - Azure China Cloud: **Connect-MsolService -AzureEnvironment AzureChinaCloud**
3. Enter the Microsoft 365 administrator credentials when prompted.
4. Enter the following command to review a list of existing service principals: **Get-MsolServicePrincipal**
5. Enter the following to create a new service principal:
   - **$principal = New-MsolServicePrincipal -DisplayName ‘SecurityGatewaySP’ -ServicePrincipalNames @(“SecurityGatewaySP”) -Type Password -Value ‘use_a_password_of_your_choice_here’ -StartDate (Get-Date) -EndDate (Get-Date).AddYears(1)**
     - The service principal object will be created and stored in the $principal variable.
     - The service principal’s password is valid for one year from its create date by default.
6. The Directory Readers role must be assigned for the service principal to be able to read information from the Azure AD tenant. Enter the following command to do this:
   - **Add-MsolRoleMember -RoleName “Directory Readers” -RoleMemberType ServicePrincipal -RoleMemberObjectId $principal.ObjectId**

**Configure a User Verification Source in SecurityGateway.**

1. Click **Setup/Users | Accounts | User Verification Sources**.
2. Under **User Verification Sources**, select **New**.
3. Under **Properties**, select **Office 365** under the **Type** drop-down menu. [Figure 4-1]
4. Enter a description for your new user verification source.
5. Enter a Domain Name, for example: example.com.
6. Select the appropriate **Cloud Type** (Global, U.S. Government, Germany, China). [Figure 4-2]
7. Enter the **Service Principal** name and password which you entered in the PowerShell (step 5 in the previous section).
8. Under the 'Type' section, select the name of your Microsoft 365 domain from the **Available Domains** list and use the arrow button to move it to the **Selected Domains** list.
9. Click on **Save and Close.**
10. On the **User Verification Sources** page, select your new user verification source, and then click on **Verify Users** to add all Microsoft 365 users to SecurityGateway.



New User Verification Source

Properties

Type: SMTP Verification (call forward)

Descri

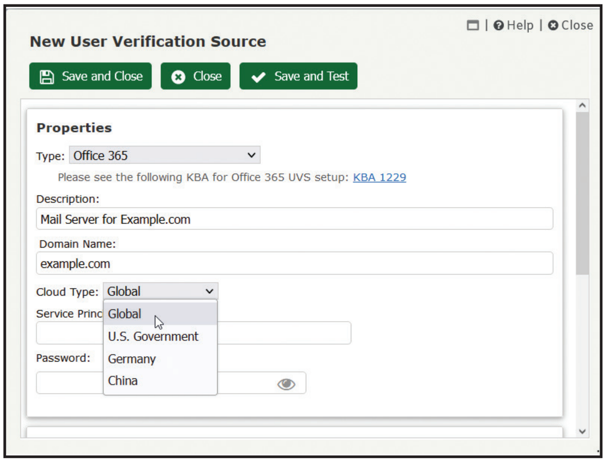
Host

Port: 25

□ Requires authentication

Username:

Figure 4-1



New User Verification Source

Properties

Type: Office 365

Please see the following KBA for Office 365 UVS setup: KBA 1229

Description: Mail Server for Example.com

Domain Name: example.com

Cloud Type: Global

Service Princ

Password:

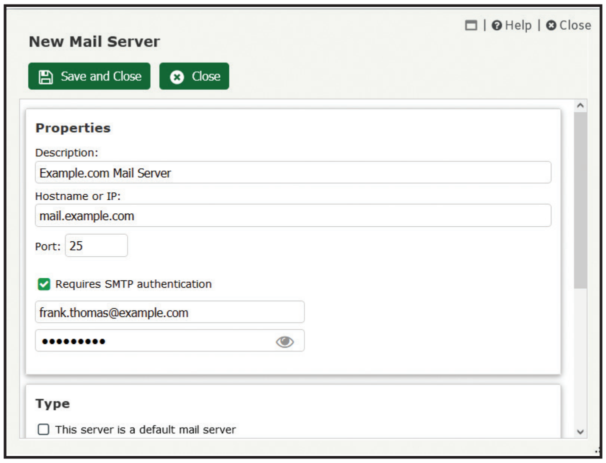
Figure 4-2

## 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.*

1. Click on **SETUP/USERS | Mail Configuration | Domain Mail Servers**
2. Under **Domain Mail Servers**, select **New**
3. Under the **Properties** section, insert a description, along with the hostname or IP address, and the SMTP port (25 is the default). If this server requires SMTP authentication, then check the box and enter the appropriate username and password in the blanks provided. [Figure 4-3]
4. Click **Save and Close**

At this point, you can now test your outbound email configuration by sending a message from one of your Microsoft 365 accounts to any outside domain. The message must pass through SecurityGateway and the Call Forward Verification will automatically add the new account in SecurityGateway as the first user.



New Mail Server

Properties

Description: Example.com Mail Server

Hostname or IP: mail.example.com

Port: 25

☑ Requires SMTP authentication

frank.thomas@example.com

•••••••••

Type

□ This server is a default mail server

Figure 4-3

## PART 4: 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 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.