Validating Mail Flow Before Restricting Access

https://campus.barracuda.com/doc/102888150/

As part of the initial deployment for Email Gateway Defense, you are required to create a new inbound partner connector within Microsoft 365. This connector is used to enforce restrictions on your Microsoft tenant to prevent emails from bypassing your Barracuda Networks gateway defenses.

Prior to enforcing those restrictions, it is important to validate your inbound mail flow to ensure there are no external senders that are sending emails directly.

Create Inbound Connector

To get started, follow the instructions in the deployment guide to create your inbound partner connector.

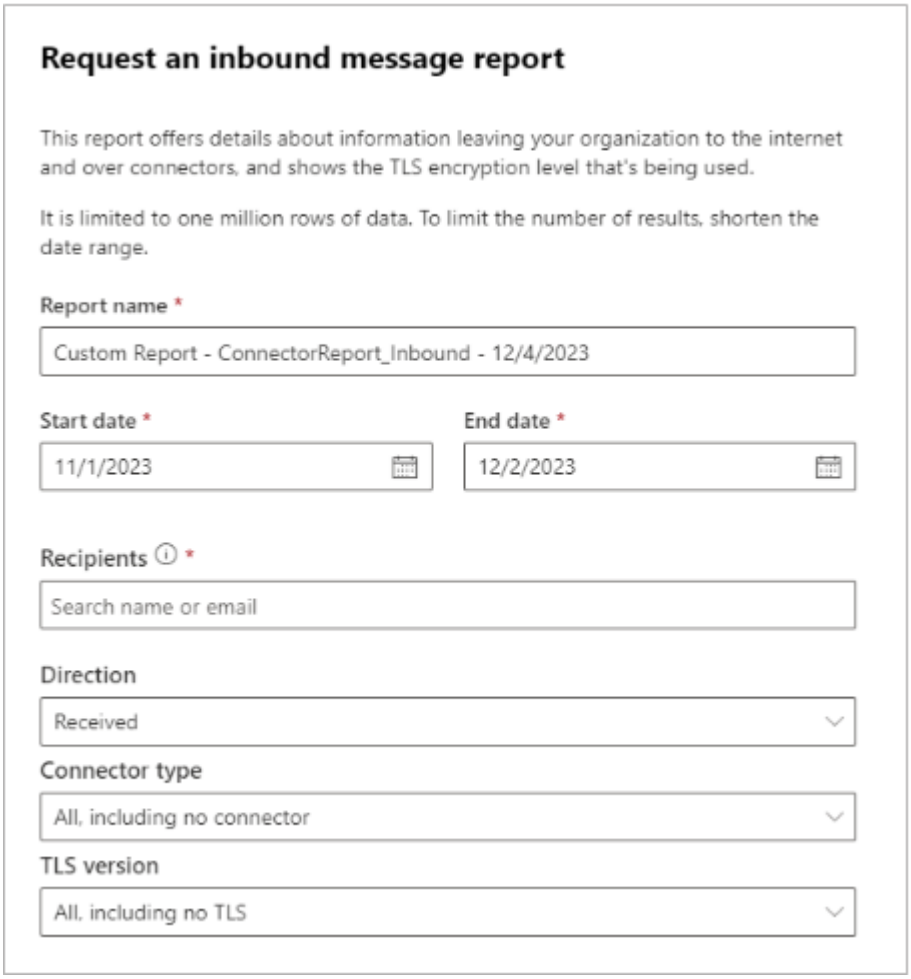
Collect Data

After creating the Barracuda Networks partner connector, let the new data collect over the next few days.

Generate Inbound Report

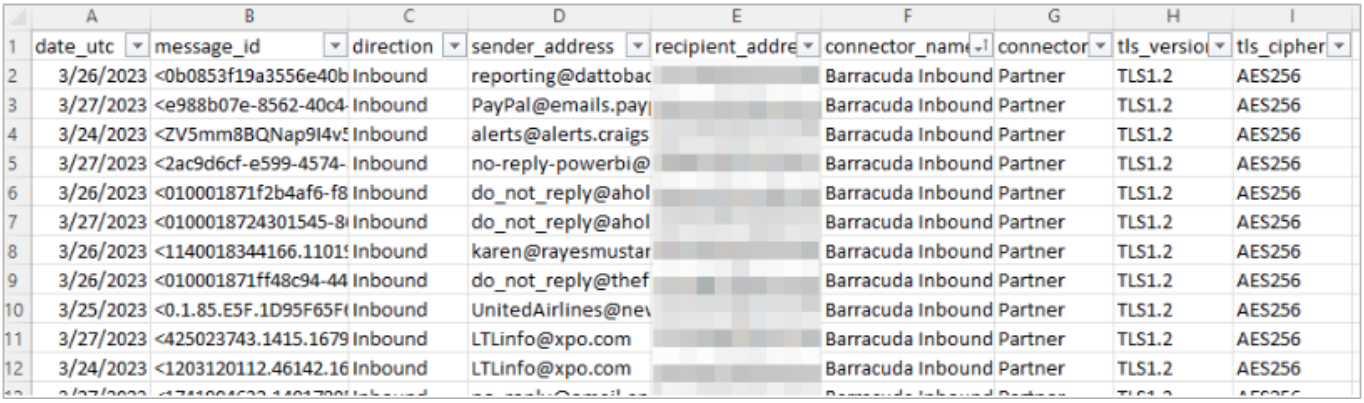
Once you have sufficient data, generate an inbound mail flow report.

1. Log in to your Exchange admin center and navigate to **Reports > Mail flow**.
2. Select **Inbound messages report**.
3. Select **Request report** and fill in the following details:
   - Enter a **Report name**.
   - Fill in the desired **Start** and **End** dates. The start date is when you first enabled the connector, and the end date is the current date or the newest date available to select.
   - Enter an email address for the **Recipients** to receive the inbound message report.
   - Set **Direction** to **Received**.
   - Set **Connector type** to **All, including no connector**.
   - Set **TLS version** to **All, including no TLS**.



4. After the report is generated, you will receive an email from Microsoft with the report attached.
5. Within the report, focus on the entries that do not have a connector associated to them. These are the messages that did not come through Barracuda Networks and will be blocked once the restrictions are enabled.

Run a Microsoft message trace on the message ID from your report to get more information on the message(s).



	A	B	C	D	E	F	G	H	I
1	date_utc	message_id	direction	sender_address	recipient_addre	connector_name	connector	tls_versio	tls_cipher
2	3/26/2023	<0b0853f19a3556e40b	Inbound	reporting@dattobac		Barracuda Inbound	Partner	TLS1.2	AES256
3	3/27/2023	<e988b07e-8562-40c4-	Inbound	PayPal@emails.pay		Barracuda Inbound	Partner	TLS1.2	AES256
4	3/24/2023	<ZV5mm8BQNap9I4v5	Inbound	alerts@alerts.craigs		Barracuda Inbound	Partner	TLS1.2	AES256
5	3/27/2023	<2ac9d6cf-e599-4574-	Inbound	no-reply-powerbi@		Barracuda Inbound	Partner	TLS1.2	AES256
6	3/26/2023	<010001871f2b4af6-f8	Inbound	do_not_reply@ahol		Barracuda Inbound	Partner	TLS1.2	AES256
7	3/27/2023	<0100018724301545-8	Inbound	do_not_reply@ahol		Barracuda Inbound	Partner	TLS1.2	AES256
8	3/26/2023	<1140018344166.1101	Inbound	karen@rayesmustar		Barracuda Inbound	Partner	TLS1.2	AES256
9	3/26/2023	<010001871ff48c94-44	Inbound	do_not_reply@thef		Barracuda Inbound	Partner	TLS1.2	AES256
10	3/25/2023	<0.1.85.E5F.1D95F65F	Inbound	UnitedAirlines@nev		Barracuda Inbound	Partner	TLS1.2	AES256
11	3/27/2023	<425023743.1415.1679	Inbound	LTLinfo@xpo.com		Barracuda Inbound	Partner	TLS1.2	AES256
12	3/24/2023	<1203120112.46142.16	Inbound	LTLinfo@xpo.com		Barracuda Inbound	Partner	TLS1.2	AES256

Emails shown as not coming through a connector will no longer be accepted once the connector restrictions are enforced. Ensure you have the senders use MX records to route mail to your tenant. Alternatively, if the source of the email is a trusted third party, you can create a partner connector within Microsoft.

As long as inbound emails either flow through the Barracuda connector or any of your other inbound (partner) connectors, the mail will not be rejected by the connector restrictions.

Restrict Access

Once you have validated your inbound mail flow, you will need to update the partner connector to enforce the IP restrictions.

Connect to Exchange Online and then run the following PowerShell command:

```
Set-InboundConnector -Identity "Barracuda Inbound Connector" -
RestrictDomainstoIPAddresses $true
```

Figures