Step 2 - Configure Email Gateway Defense for Exchange Server 2007 and 2010

https://campus.barracuda.com/doc/96022766/

Use this article to deploy Email Gateway Defense for Exchange Server 2007 and 2010 in your environment.

Step 1. Ensure Connectivity and Redundancy

- Open your firewall ports to allow the IP address ranges based on your Barracuda Networks instance; see Email Gateway Defense IP Ranges Used for Configuration for a list of ranges based on your Barracuda Networks instance.
- Where relevant, verify your network subnet is granted access in the ACL on your mail server (and LDAP server, for that matter).
- Block all port 25 traffic except for that originating from Email Gateway Defense IP Ranges Used for Configuration based on your Barracuda Networks instance.

Step 2. Launch the Email Gateway Defense Setup Wizard

Alternatively, you can manually set up Email Gateway Defense using the web interface.

Configure Domain

1. Log into Email Gateway Defense, and go to the **Domains** page.
2. Enter the primary Exchange domain name you want to filter, for example: `corpdomain.com`
3. Enter the mail server hostname (FQDN) or IP address for the domain entered in the previous step, for example: `corpdomain-com.mail.protection.outlook.com`
4. Click **Add** in the **Actions** column; the **Domains > Domain Settings** page displays. If you are adding multiple mail servers, assign a priority level, and click **Add**.

1. Log into Email Gateway Defense, and click the link to launch the Email Gateway Defense Setup wizard.
2. Select the **Region** for your Data Center. Then click **Get Started**.
   After you select your region, you cannot change it.

3. The **Specify Primary Email Domain** page displays. Enter the primary domain you want to filter, for example: `corpdomain.com`
4. Click **Next**. The **Specify Email Servers** page displays. Enter the mail server hostname (FQDN) or IP address for the domain entered in the previous step.

   If Email Gateway Defense Setup wizard has already identified your mail server IP based on the MX record, the **Mail Servers** field pre-populates.
5. Click **Add**. Enter an email address to test the server configuration, and click **Test All Mail Servers**.
6. Once the mail server is verified, the **Verified** ( ) icon displays in the status column and a confirmation message displays at the top of the page.
7. Click **Next**. The **Configure Settings** page displays. Select from the following options:
   1. **Virus Protection** – Set to **On** to direct Email Gateway Defense to detect and block viruses on inbound email.
   2. **Spam Protection** – Set to **On** to direct Email Gateway Defense to evaluate inbound mail for spam based on a score assigned to each processed message. When set to **Off** inbound mail is not scanned for spam.
   3. **Spam Scoring** – Set **Spam Protection** to **On** to enable **Spam Scoring**. Scoring ranges from 1 (definitely not spam) to 10 (definitely spam). Setting a score of '1' will likely block legitimate messages while setting a score of '10' will allow more messages through the system. Based on this score Email Gateway Defense blocks messages that appear to be spam and logs these messages in the user's Message Log with **Score** as the reason for the block.

      The following features, configured on the **Inbound Settings > Anti-Spam/Antivirus** page, are enabled when **Spam Protection** is set to **On**:
      • **Barracuda Reputation Block List (BRBL)** – Database of IP addresses manually verified to be a noted source of spam.
      • **Barracuda Real-Time System (BRTS)** – Advanced service to detect zero-hour spam and virus outbreaks even where traditional heuristics and signatures to detect such messages do not yet exist. Each quarantined message has a reason of **BRTS** in the Message Log.
      • **Sender Policy Framework (SPF)** – Block Fail is disabled.
      • **Barracuda Anti-Fraud Intelligence** – Barracuda Networks anti-phishing detection which uses a special Bayesian database for detecting Phishing scams.
      • **Intent Analysis** – Blocking based on intent analysis.
      • **CloudScan Scoring** – A cloud-based spam scanning engine which assigns a score to each message processed ranging from 0 (definitely not spam) to 10 (definitely spam).
8. Click **Next**. The **Outbound** page displays.
9. To verify your domain, replace your current MX records with Email Gateway Defense Primary and Backup MX records displayed on the page.

   During the evaluation period, to complete the verification process but allow your legitimate mail to continue using your current mail server, you can add the MX records with a low priority, for example, *99*.
   Some mail may appear in the Message Log after making this MX record change as spammers routinely send mail to all MX records for a domain.
   Once you have made the change to your MX records, return to the **Route Email**

Through Barracuda page and click **Verify MX Records**. Email Gateway Defense should see the changes made and verify your domain. If the domain does not verify correctly, verify that your MX changes are live. You can do this by using the following sites that return your MX information:
http://mxtoolbox.com/
https://toolbox.googleapps.com/apps/dig/ (select the MX option)
If your domain's MX records do not display in Email Gateway Defense MX records, you must wait until they display before your domain can be verified.
Note that after verifying your domain, any mail sent to your domain from another Barracuda Email Gateway Defense customer will be processed normally by your Email Gateway Defense account and not delivered via MX records.

10. If you only want to route your inbound mail through Email Gateway Defense and not your outbound mail, select **I do not want to route my e-mail through Barracuda at this time**, and select the verification option:
    1. **CNAME Records** – To use the CNAME records method to verify the domain ownership:
        1. Log into your DNS Server and, under this domain, create a subdomain whose name is created by concatenating 'barracuda' and the CNAME token shown in the **Route Email Through Barracuda** page. For example: `barracuda30929916985.corpdomain.com`
        2. Point the CNAME record of that subdomain to **ess.barracuda.com**

           Allow the DNS propagation to take effect before proceeding.
        3. Click **Confirm Validation** in the **Route Email Through Barracuda** page.
    2. **Email to Technical Contact** – This method sends a verification email to the technical contact email address, if it exists, listed on your domain's WHOIS entry.

       This verification option is not available if Email Gateway Defense cannot find your domain's WHOIS entry. If there is not a technical contact, then only the **MX Records**, **CNAME**, and **Email to the Postmaster** options displays on this page.
    3. **Email to the postmaster** – This method sends a verification email to the postmaster email address for your domain. The confirmation email includes a link that the recipient must click to verify the domain.

       This option is available if Email Gateway Defense can find your postmaster in your domain’s WHOIS records. This method sends a verification email to the postmaster email address for your domain. The confirmation email includes a link that the recipient must click to verify the domain.
11. Click **Next**, and click **Next** once again.
12. On the **Select Data Center Region** page, select the data center for your locale, and click **Get Started**.
13. Complete the wizard pages.
14. The **Confirmation** page displays. Confirm domain ownership, and then click **Done**.
15. Go to the **Domains** page and verify your settings.

Step 3. Set Up User Accounts

You can add users manually, or use your organization's LDAP server or Microsoft Entra ID service to automatically synchronize Email Gateway Defense with your active directory server. To create a few test accounts during the evaluation period, use the **Manually Add Users** steps below.

Decide how you want to use quarantine:

- **Global quarantine** – When selected, the administrator monitors the **Message Log** for quarantined mail and decides whether or not it is spam.
- **Per-user quarantine** – When selected, users have quarantine accounts and can decide whether or not mail is spam. Set up several users for the evaluation and test the results. This option requires more initial effort to set up user accounts, possibly with sync to your active directory server, but less work for the administrator over time since users manage their quarantined mail.

Quarantine Type	Create User Accounts	Manages Quarantine?	User can Create Sender Allow List/Block List
Global	No	Admin	No
Per-user	Yes	User	Yes

1. If you select **Global quarantine**, there is no need to create user accounts.
2. If you select **Per-user quarantine**, manually add a few test accounts on the **Users > Add/Update Users** page, and set **Enable User Quarantine** to **Yes**. The first time Email Gateway Defense receives an email for that user and the message is quarantined, the user receives a quarantine notification email at the scheduled quarantine notification interval. Depending on how you configure the quarantine notification interval on the **Users > Quarantine Notification** page, the user receives a quarantine digest at a specified time.

Manually Add Users

1. Go to **Users > Add/Update Users**:

2. In the **User Accounts** field, enter each user email address for the domain on a separate line, and then select from the following options:
   1. **Enable User Quarantine** – All emails for the user which meet the configured block policy go to the user's quarantine account.

      Depending on how you have configured the quarantine notification interval on the **Users > Quarantine Notification** page, the user receives a quarantine digest at a specified time. From the **Users > Quarantine Notification** page you can also allow the user to set their own quarantine notification interval.

   2. **Notify New Users** – When set to **Yes**, users receive a welcome email when the account is created.
3. Click **Save Changes**. The users are added to the **Users > Users List** table where you can select from the following actions:
   1. **Edit** – Click to specify domains this user can manage.
   2. **Reset** – Click to send the user an email with instructions on how to reset their account password.
   3. **Log in as this user** – Click to view or change the user's settings (for example, quarantine notifications), v iew/manage the domains this user manages, and v iew/search/manage the user's Message Log.
   4. **Delete** – Click to remove the user account.
4. Click **Save Changes**; the **Users List** displays.

The first time Email Gateway Defense receives an **Allowed** email for a non-existent user at a domain configured for the service, if that same recipient receives a second email 1-6 days later, a new user account is created. This method of new account creation does not use LDAP lookup, and the user receives an email from Email Gateway Defense with their login information so they can access their quarantine account.

Automatically Add Users

You can configure user authentication via your organization's LDAP server or Microsoft Entra ID service. For complete setup details, see the following articles:

- How to Configure User Authentication with Microsoft Entra ID
- How to Configure User Authentication Using LDAP

Step 4. Configure Outbound Mail Scanning

1. Log into Email Gateway Defense, and go to **Outbound Settings > Sender IP Address Ranges**.
2. Enter the IP Address and Domain Name (logging domain) and optional **Comment** for IP address ranges allowed to send outgoing email from your domains, and click **Add**.

   Note that Barracuda Networks policy requires all outbound IP addresses to have a rDNS (PTR) record.
   This requirement is for the security of our service and your email. This policy stops spammers from signing up to our service, adding hundreds of outbound IP addresses, and using our service to send out massive spam attacks. For security reasons, there are no exceptions to this policy.
   If you are using an IP or ISP that does not provide a rDNS (PTR) record for your IP, Barracuda Networks recommends either moving to a different ISP, or routing your mail through another ISP/Service that does provide an rDNS (PTR) record. For example,

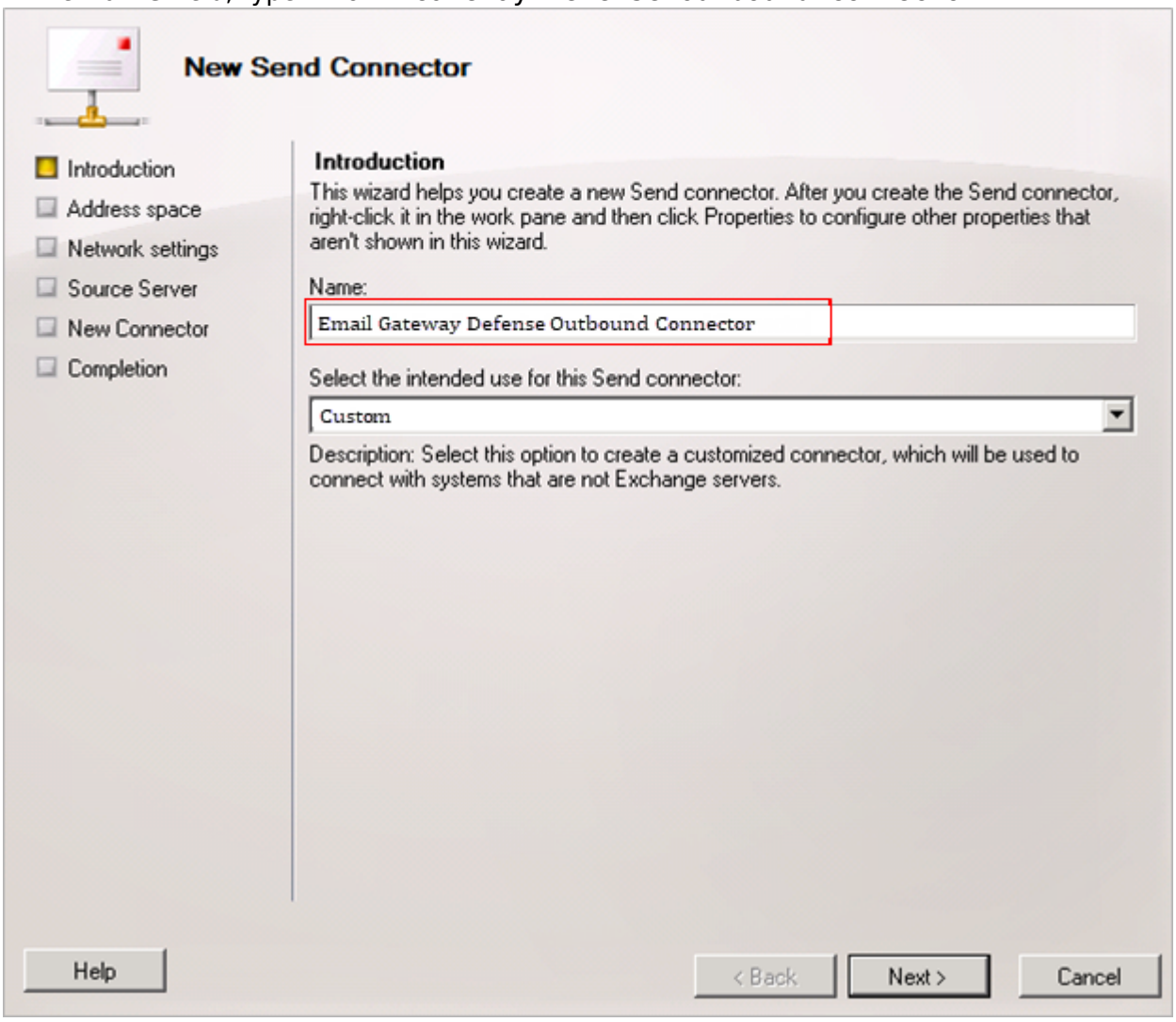
Microsoft 365.

3. Add all IP addresses from which outgoing mail is allowed to flow through Email Gateway Defense. The **Logging Domain** is the domain name that appears in the **Message Log** as the sending domain for the associated IP address.

Step 5. Set Up Email Gateway Defense Outbound Scanning

Complete the following steps for each domain from which you are relaying outbound mail:

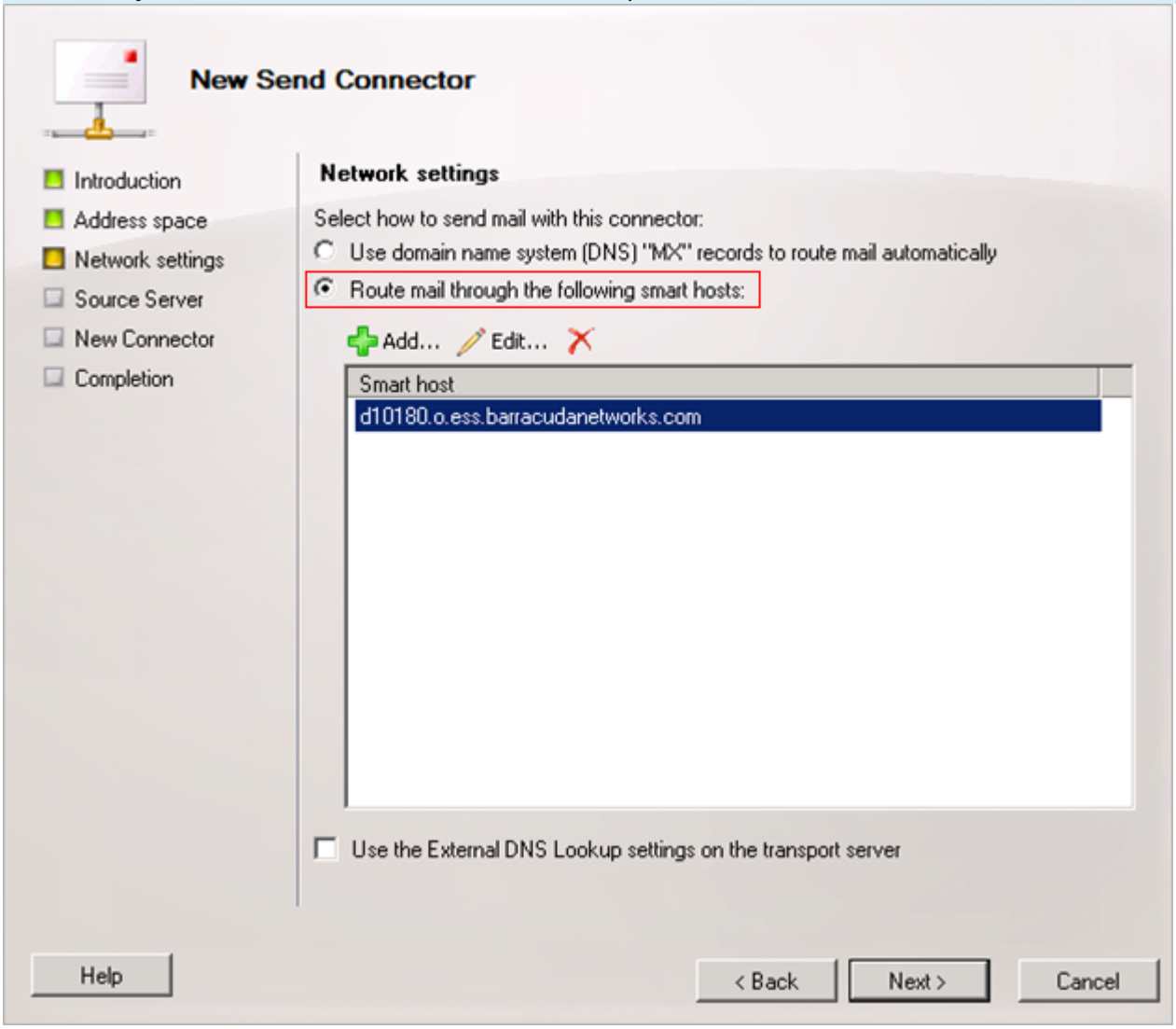
1. Log into Email Gateway Defense, click **Domains**, and click on the domain name to toggle the MX records configuration; make note of the **Outbound Hostname**.
2. Open the Exchange Management Console.
3. Under **Organization Configuration**, select **Hub Transport**, and then click the **Send Connectors** tab:
4. In the **Name** field, type: `Email Gateway Defense Outbound Connector`



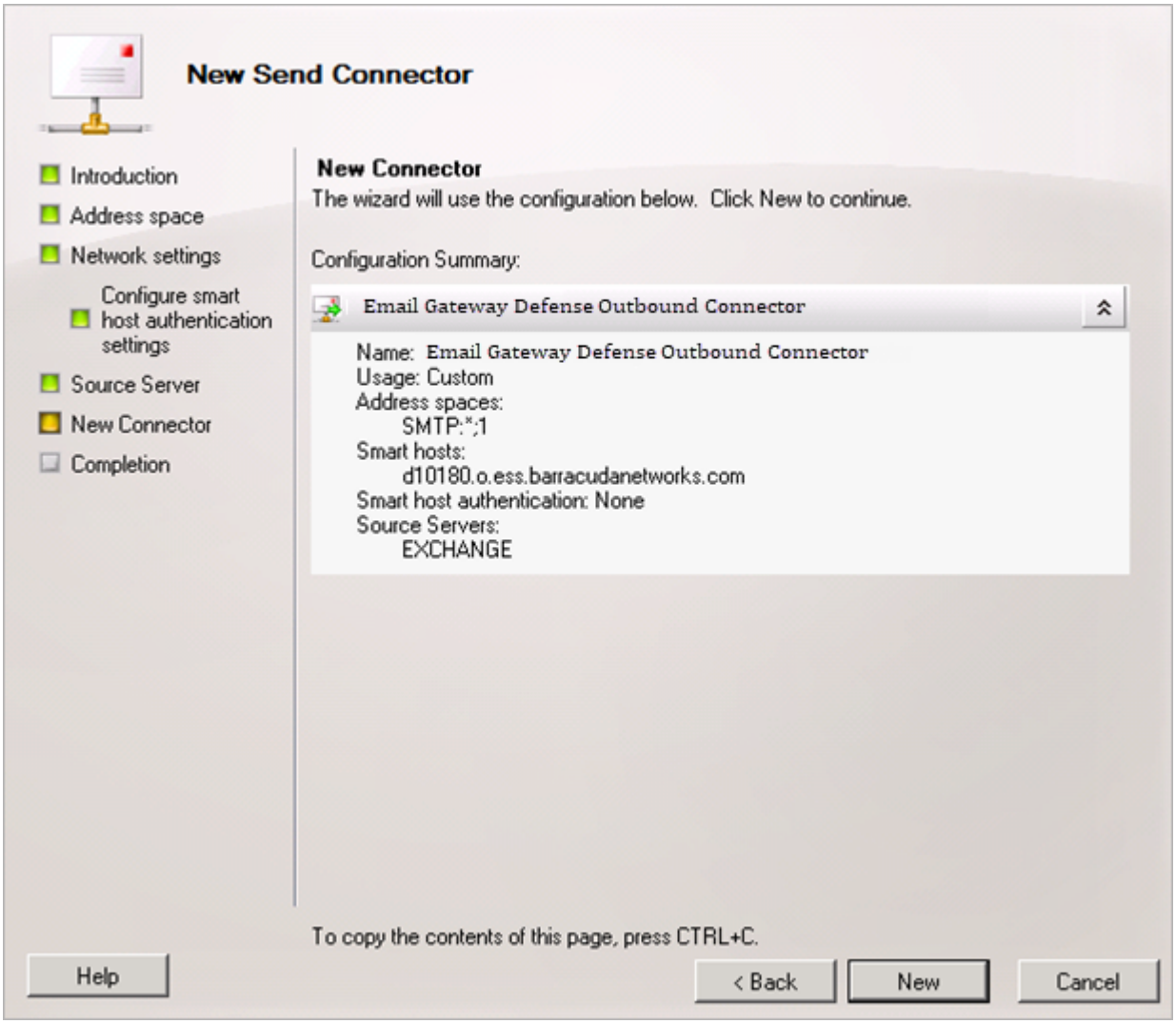
5. Click **Next**. The **Address Space** page displays:

6. Click **Add**. The **SMTP Address space** dialog box displays. In the **Address** field, type an asterisk: *****
7. Click **OK**, and click **Next** in the **Address space** page.
8. The **Network settings** page displays. Select **Route mail through the following smart hosts**:

   If you have an existing outbound connector, you must disable it or update it with Email Gateway Defense outbound hostname from *Step 1* above.



9. Click **Add**. Enter the **Outbound Hostname** from *Step 1* above, and click **OK**.
10. Click **Next** in the **Network settings** page. The **Source Server** page displays. If your Exchange servers are not listed, click **Add**.
11. In the **Select Hub Transport** dialog box, select all servers that have *Hub Transport* roles installed, and click **OK**.
12. Click **Next** in the **Source Server** page. The **New Connector** displays. Review your settings:



13. Click **New**, and then click **OK** to save your connector and route outbound mail through Email Gateway Defense.

Step 6. Verify Mail is Flowing

1. Log into Email Gateway Defense.
2. In the **Dashboard** page verify inbound and outbound messages are being logged for the selected domain.

   You can also click **Message Log** to view inbound and outbound email traffic. Use the filters to refine your search.

Step 7. Configure Sender Policy Framework for Outbound Mail

To assure Barracuda Networks is the authorized sending mail service of outbound mail from Email

Gateway Defense, add the following to the Sender Policy Framework (SPF) record INCLUDE line of the SPF record for your sending mail server for each domain sending outbound mail. Select the relevant SPF INCLUDE based on the region you selected for your Barracuda Networks instance:

AU (Australia)

```
include:spf.ess.au.barracudanetworks.com -all
```

CA (Canada)

```
include:spf.ess.ca.barracudanetworks.com -all
```

DE (Germany)

```
include:spf.ess.de.barracudanetworks.com -all
```

UK (United Kingdom)

```
include:spf.ess.uk.barracudanetworks.com -all
```

US (United States)

```
include:spf.ess.barracudanetworks.com -all
```

See Sender Authentication for more information.

- If you have an SPF record set up for your domain, edit the existing record, and add the following to the INCLUDE line for each domain sending outbound mail based on your Barracuda Networks instance. For example: `include:spf.ess.barracudanetworks.com -all`
- If you do not have an SPF record set up for your domain, use the following value to create a TXT record that creates a HARD Fail SPF for your domain based on your Barracuda Networks instance. For example: `v=spf1 include:spf.ess.barracudanetworks.com -all`

Step 8. Enable Advanced Threat Protection

Files blocked by ATP display on the **Dashboard**.

1. Go to **ATP Settings**, and select the desired option:
    - **Deliver First, then Scan** – Attachments are delivered with the message to the recipient and then scanned by the ATP service; if a virus is detected, an email notification is sent to the email recipient. Additionally, if **Notify Admin** is set to **Yes**, and a virus is detected in the scanned attachment, an email is sent to the administrator.
    - **Scan First, then Deliver** – Attachments are scanned by the ATP service before delivery. If a virus is detected in the attachment the message is blocked, otherwise it is delivered

to the recipient.

2. Select whether to **Notify Admin** if a virus is detected in a scanned attachment. When set to **Yes**, enter the **ATP Notification Email** address in the associated field.

   When ATP is set to either **Deliver First, then Scan** or **Scan First, then Deliver**, you can exempt sender email addresses, sender domains, recipient email addresses, recipient domains, or sender IP addresses from ATP scanning in the **ATP Exemptions** section on the **ATP Settings** page.

Figures

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.