Mail Transfer Agent (MTA)

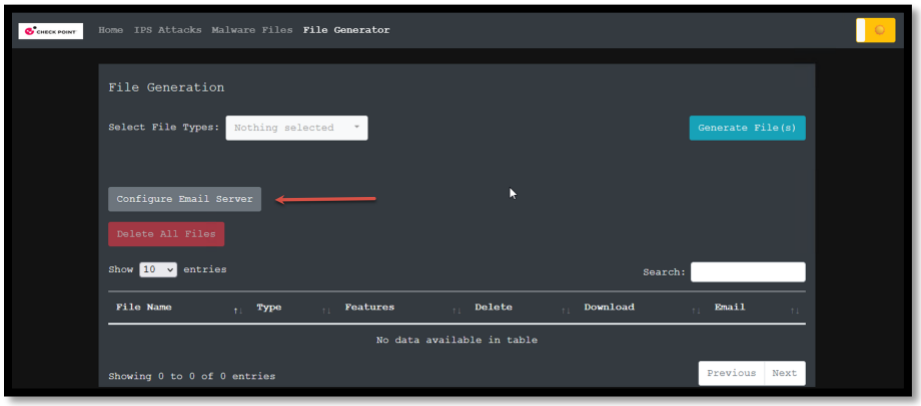
Introduction

In this lab, you will learn how to enable **MTA** mode on the **GW** with **Threat Emulation** activated. This allows the GW to participate in the email flow and, therefore, hold mail and strip malicious attachments if found. Without using **MTA** mode, the gateway is passive in the email chain and cannot guarantee successful email interception.

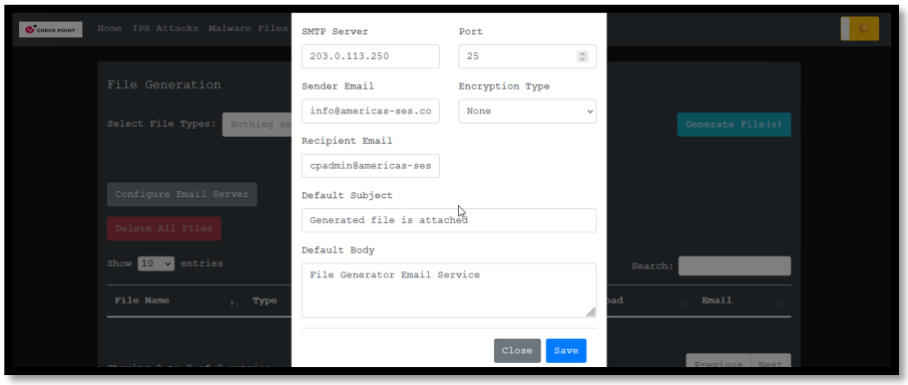
Exercise 1: Mail Inspection without using MTA mode

In this exercise, we will review the inspection of email traffic by the Threat Prevention blades when the **GW** is not acting as a Mail Transfer Agent and the limitations of this mode.

1. Connect to the **win_client** using the **RDP** session in **MobaXterm** and click **Configure Email Server**.

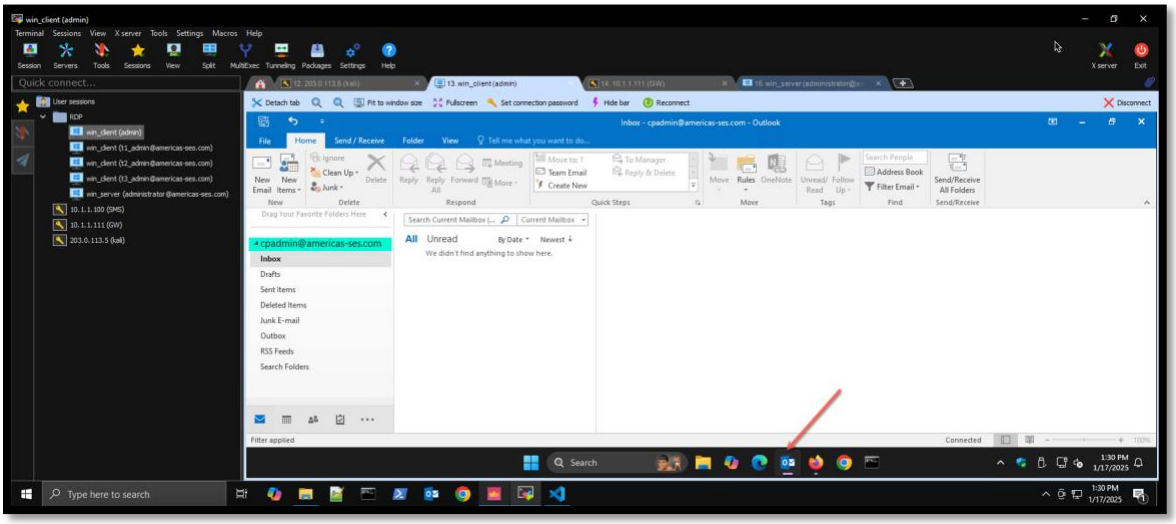


2. Review the default Email configuration and close the configuration window.

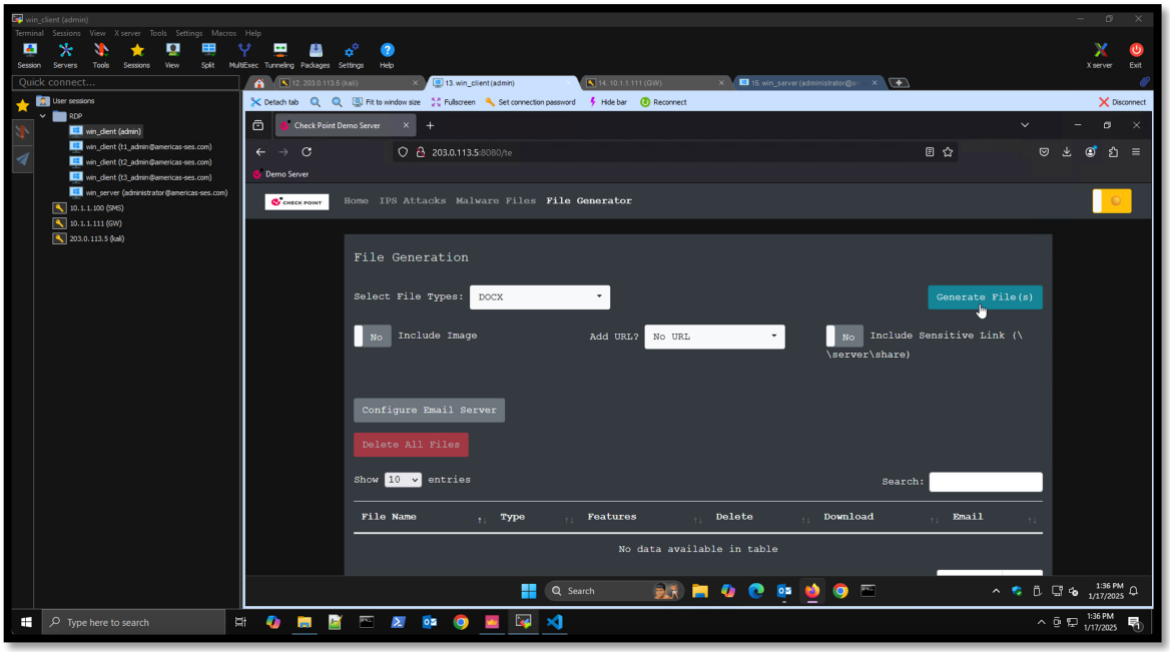


- The default settings show the following:
  - The Email Server is the **win_server.**
  - Emails are sent non-encrypted traffic on port 25/TCP.
  - The Recipient cpadmin@americas-ses.com. The Outlook application on **win_client** local account is preconfigured with this account.
  - The sender info@americas-ses.com is the mailbox for the Outlook account configured on the Jump Server. You can use any other account.

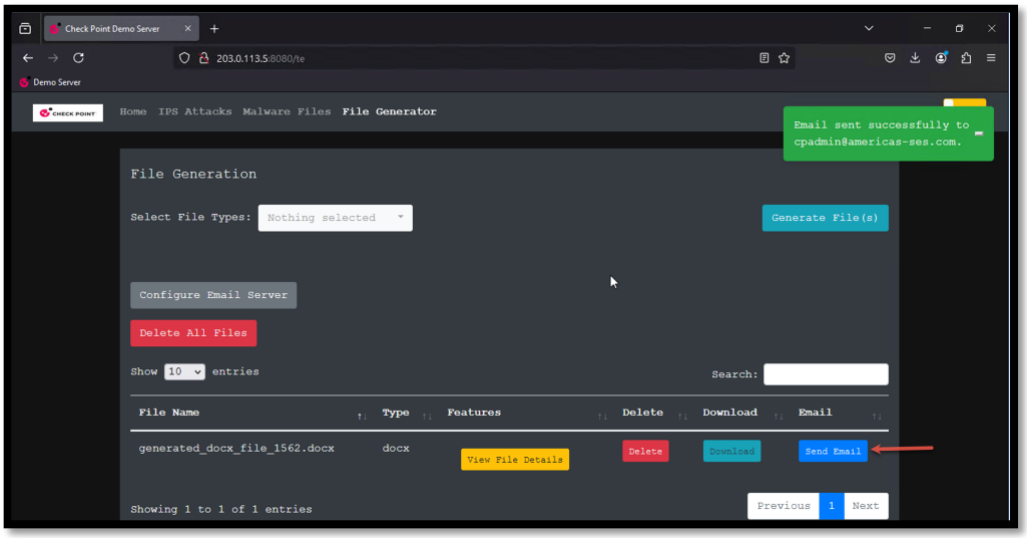
3. Open Outlook from **win_client** and review the default Email account.



4. From the same client, return to the Demo Server website and generate a new file. For example, a **docx** file.



5. Once the file is generated, click **Send Email**. This will send the file as an attachment to an email using the server settings we reviewed earlier.

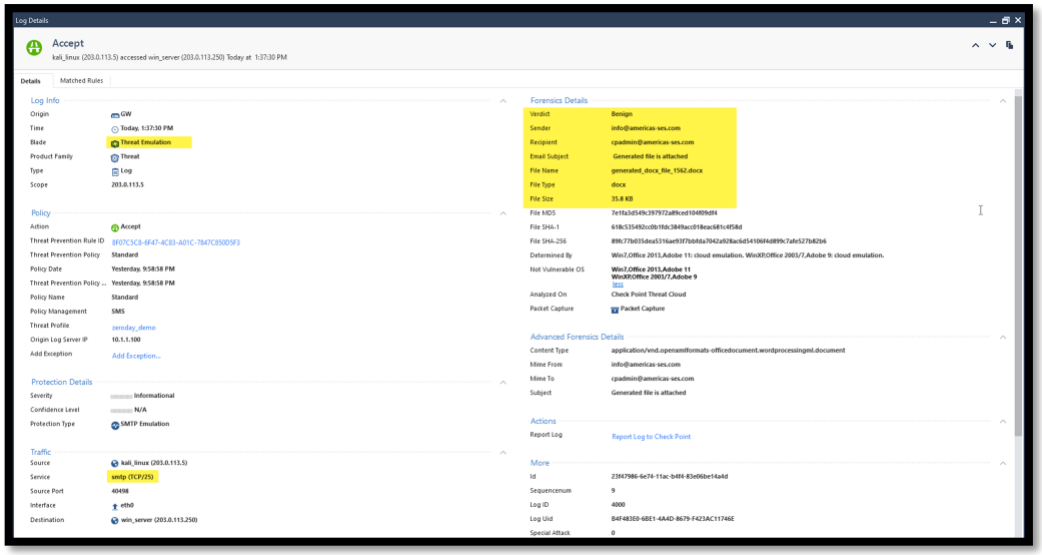


6. You can review the Threat Emulation queue using the command tecli show cloud queue or the command tecli show emulator queue to confirm the file was sent to the Check Point Threat Cloud for emulation.

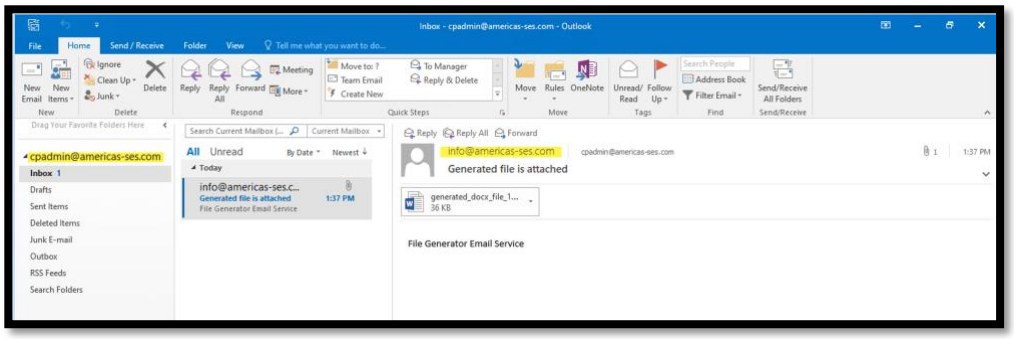
```
[Expert@GW:0]# tecli sh clo que
|file's sha1                              |file's event_id                          |file type |insert time      |status
|-----------------------------------------|-----------------------------------------|----------|-----------------|-------------------------------------------------------------------------
--------
|618c535492cc0b1fdc3849acc018eac681c4f58d|{B4F483E0-6BE1-4A4D-8679-F423AC11746E}  |docx      |34 Seconds       |Uploaded to Cloud, waiting for response.

[Expert@GW:0]# tecli sh em que
File ID (SHA1)                            File Name      Emulation Required           Status        External Key / Internal Key
----------------------------------------  -------------  ---------------------------  ------------  ------------------------------------------------------------------------------------------------
----------
618c535492cc0b1fdc3849acc018eac681c4f58d   generated_...  WinXP,Office 2003/7,Adobe 9  In Progress   436ddc864f93bf85efffba3ffcdcd097f14a4118/5ae3e0ce4e10d1c9dcc386c4c3cd70e
48d9c4a9d
618c535492cc0b1fdc3849acc018eac681c4f58d   generated_...  Win7,Office 2013,Adobe 11    In Progress   c506d64d843f8b1d009b667f3b6d841f5df54406/bc879488ab4a34ec6ad4e4c719a15bd
d656b219e
```

- Remember that we configured Threat Emulation in the Threat Prevention profile to work in Maximum Prevention mode.
  - The **GW** will try to scan the file and wait for a verdict **before** allowing the file to be delivered to the end user.
  - A long scanning time can result in a connection timeout and a connection reset from the Email server.
  - Cloud Emulation can take a few minutes to complete.
- The **GW** intercepted the traffic and extracted the file for scanning because the traffic was not encrypted.
- From the above, the two main drivers for activating the Mail Transfer Agent are:
  - Avoid timeout and scan failures, especially when the server has a short timeout.
  - The ability to scan encrypted emails.

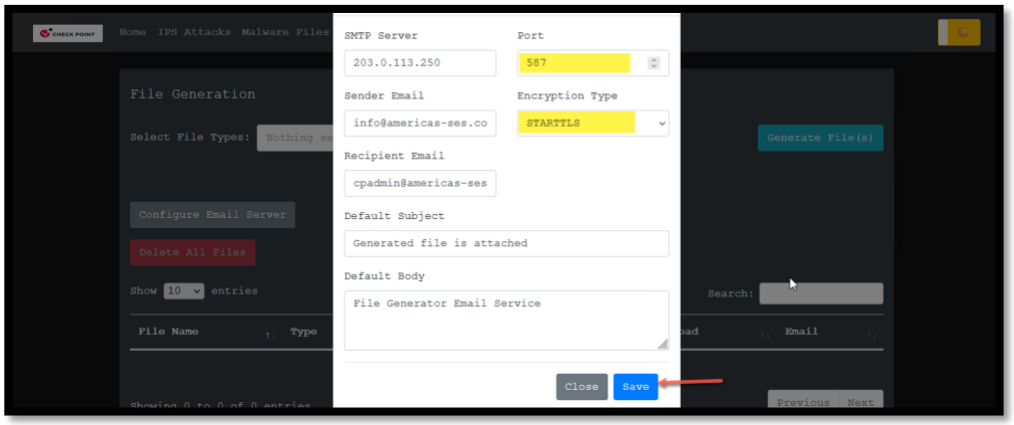
5. Review the logs for **port 25** TCP and notice that the GW successfully inspected the file and decided it was clean before allowing it. *Port 25/TCP represents clear, non-encrypted SMTP traffic*.



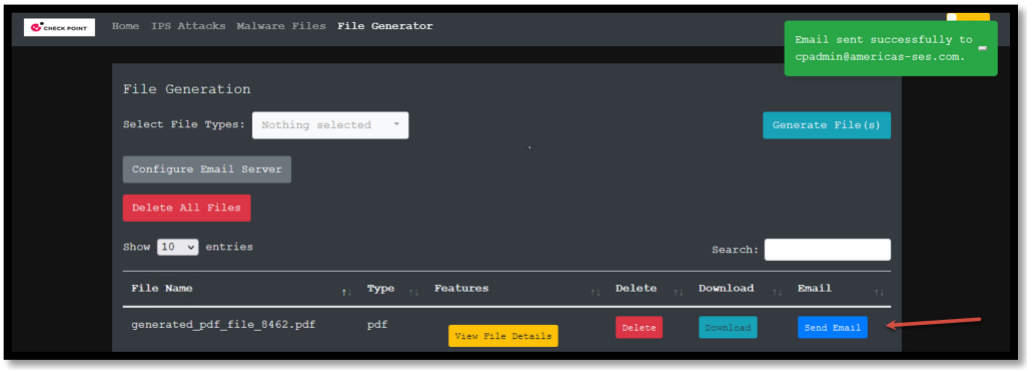
7. Check outlook on **win_client** and confirm the email was delivered as expected.



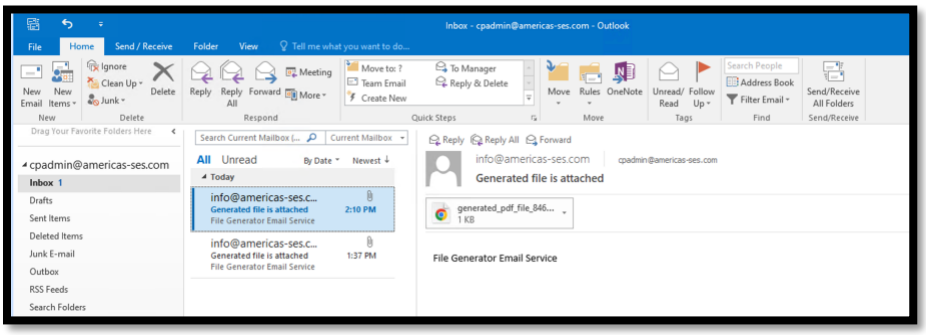
8. On the Demo Server website, change the email server configurations. Set the Port to **587,** and Encryption Type to **STARTTLS**. This will force the Demo server to send emails over an encrypted session.



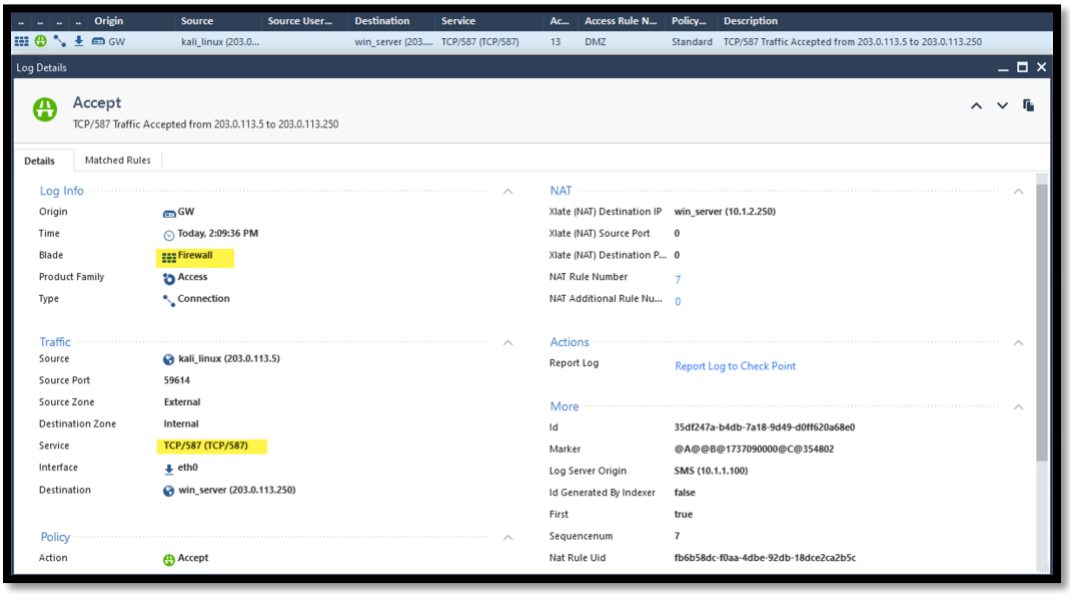
9. Make sure the new changes are saved. Generate a new file and click **Send Email**.



10. Notice that the Email was delivered almost instantly to the recipient's mailbox. It is because the GW did not hold the email for scanning.



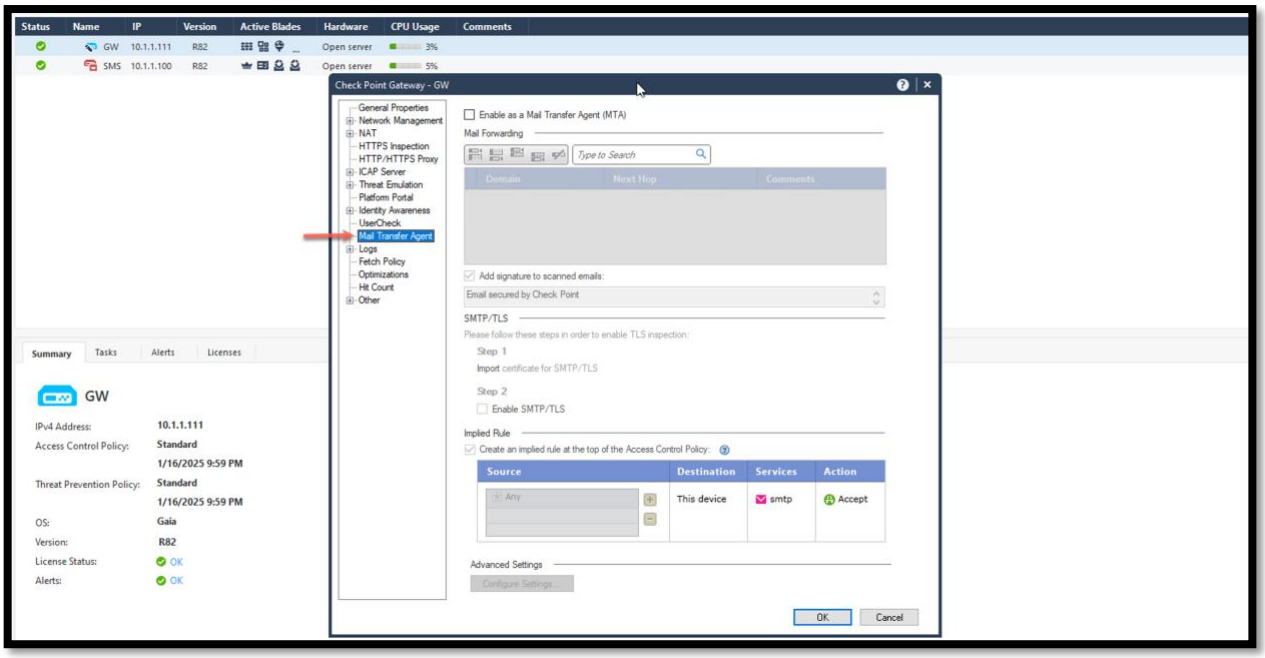
11. Review the logs to see traffic over port 587. Notice that we are only getting the Firewall blade logs indicating that the email traffic over **port 587** was accepted. The Threat Emulation blade will not intercept the traffic because it was encrypted.



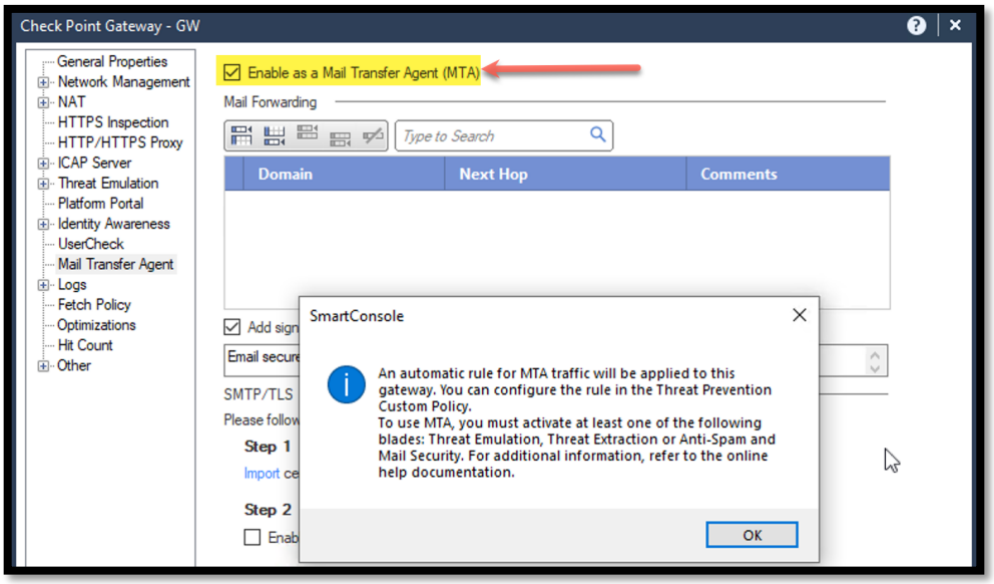
Exercise 2: MTA Onboarding

In this exercise, we will enable the Check Point MTA (Mail Transfer Agent) mode. With MTA enabled, the **GW** will be able to receive and scan emails. MTA also provides the capability to scan encrypted email traffic.

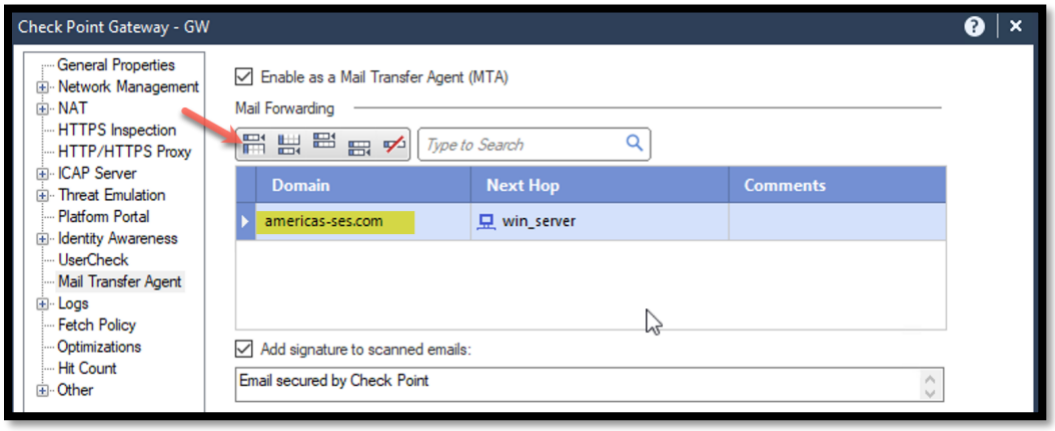
1. From the Jump Server host, connect to SmartConsole, edit the **GW** object, and open the **Mail Transfer Agent** settings.



2. Check the option Enable as a Mail Transfer Agent (MTA) and read the warning message.

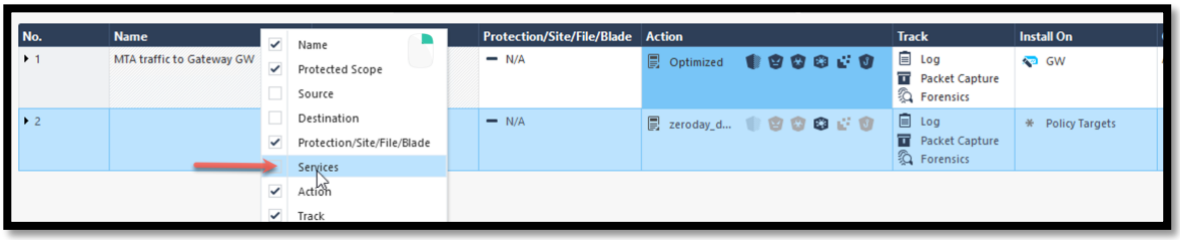


3. Under the Mail Forwarding section, add a new rule to inspect Email traffic related to our domain **americas-ses.com** and select **win_server** as the next hope.
    - It is possible to scan all domain email traffic by replacing the domain name with *
    - The Next Hop indicates the next hop email server.
    - The default signature **Email secured by Check Point** will be added to all scanned emails.



4. Save the changes and review the Threat Prevention **Custom Policy**. A new rule was created automatically to accept MTA traffic. Pay attention to the assigned profile.

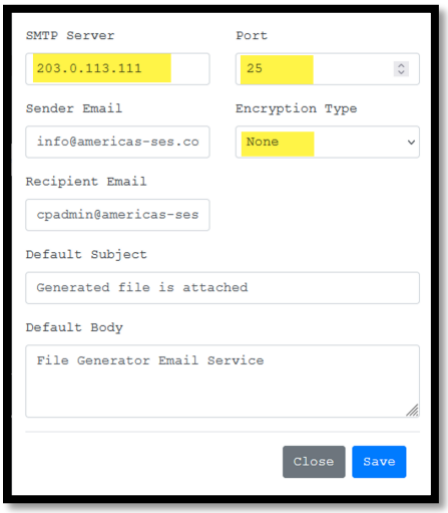
5. Right-click on the menu bar and enable the **Services** column.



6. Notice that the automatically added rule will only match email traffic. Assign the **zeroday_demo** profile to the MTA (first) rule.

7. Install the **Access Control** and the **Threat Prevention** policy.

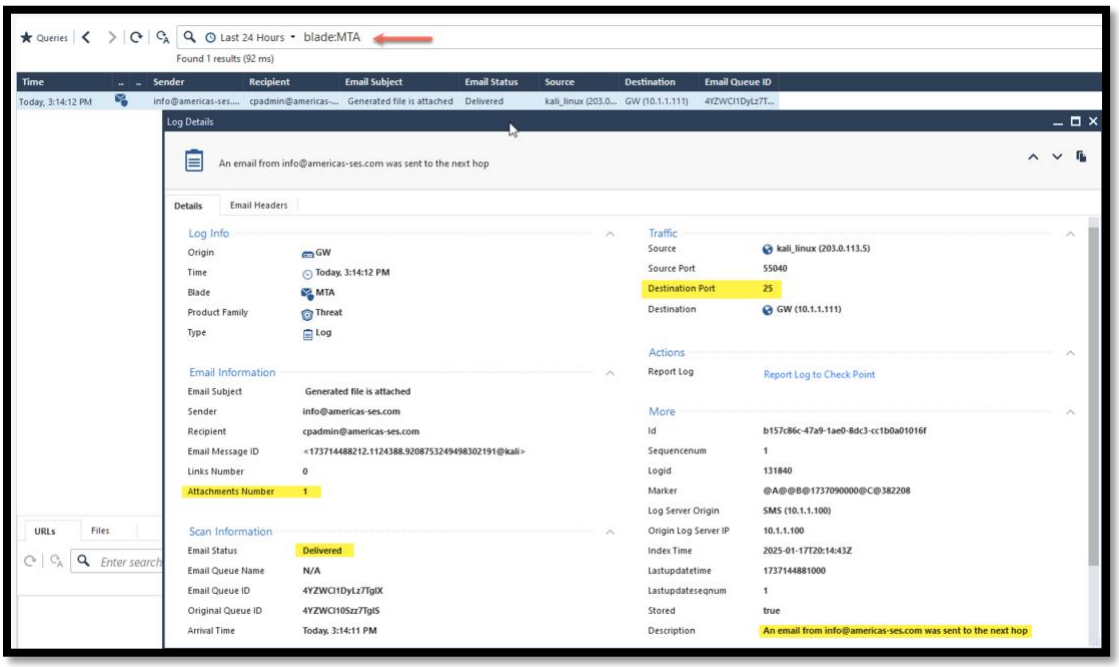
8. From **win_client** connect to the Demo Server and edit to the email server configuration. The SMTP Server will be the external IP address of the GW at **203.0.113.111** with no encryption and clear traffic on port 25. Save the changes!



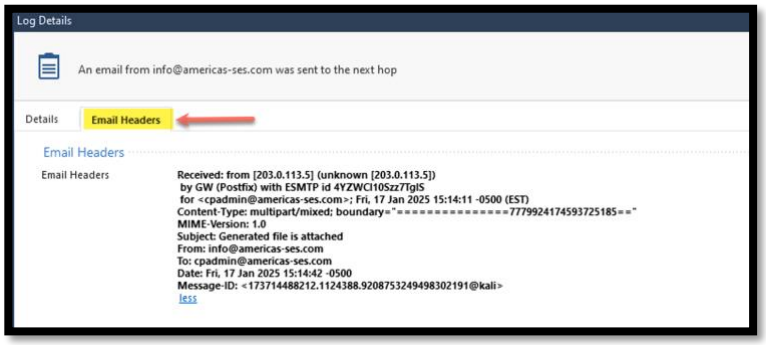
- In production, we typically change the DNS MX record to point to the public IP address of the GW with MTA enabled.

9. From the demo server, generate a new file and send it as an email attachment. For example, a PPTX file.

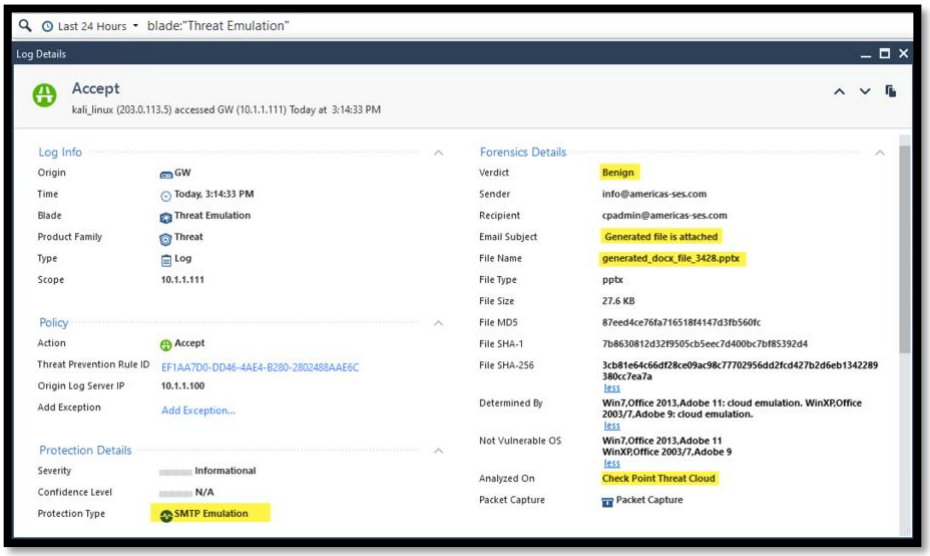
10. Review the logs in SmartConsole. You can use the filter **blade: MTA** to view only MTA-related traffic.



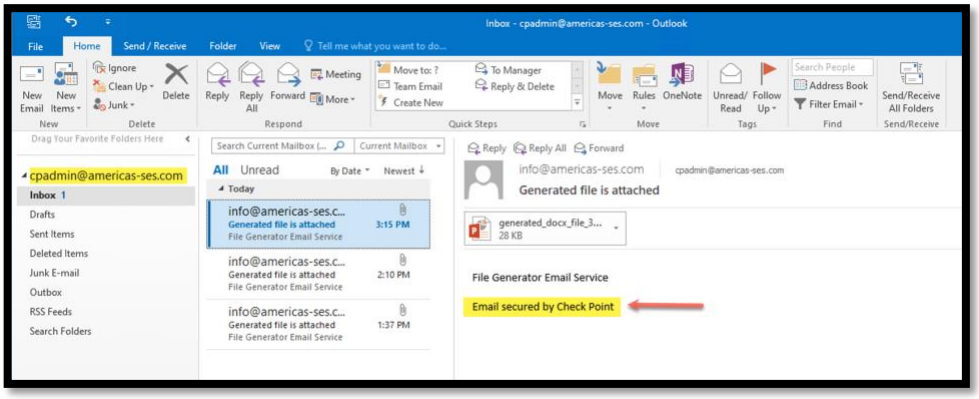
11. Review the details under the Email Headers tab in the same log record.



12. Review the Threat Emulation logs. The email details are added to the log.



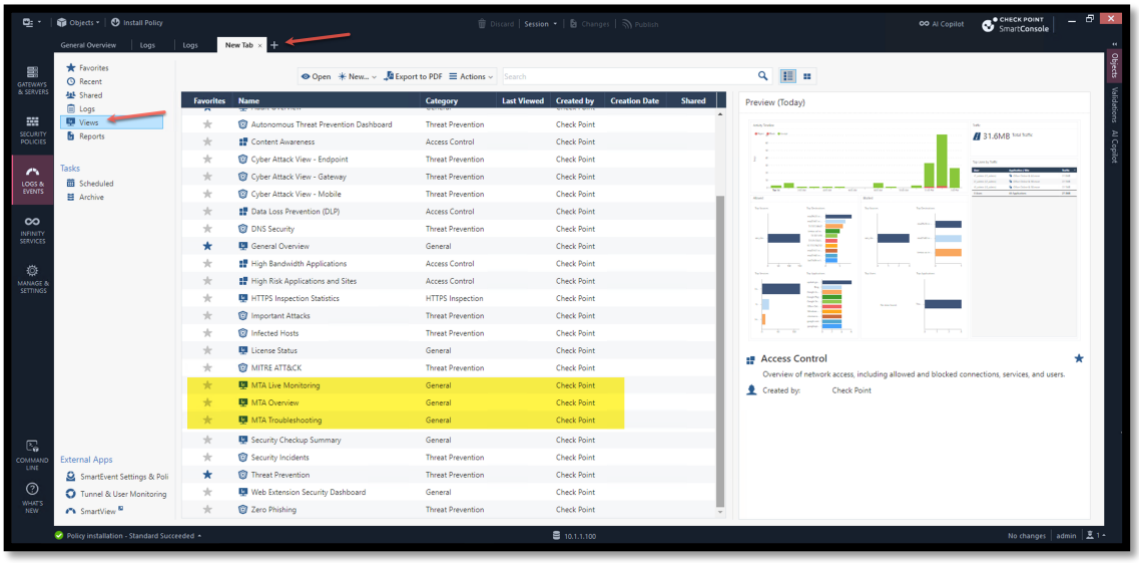
13. From **win_client**, open Outlook and review the latest email. The signature added by the MTA blade is visible in the email body.



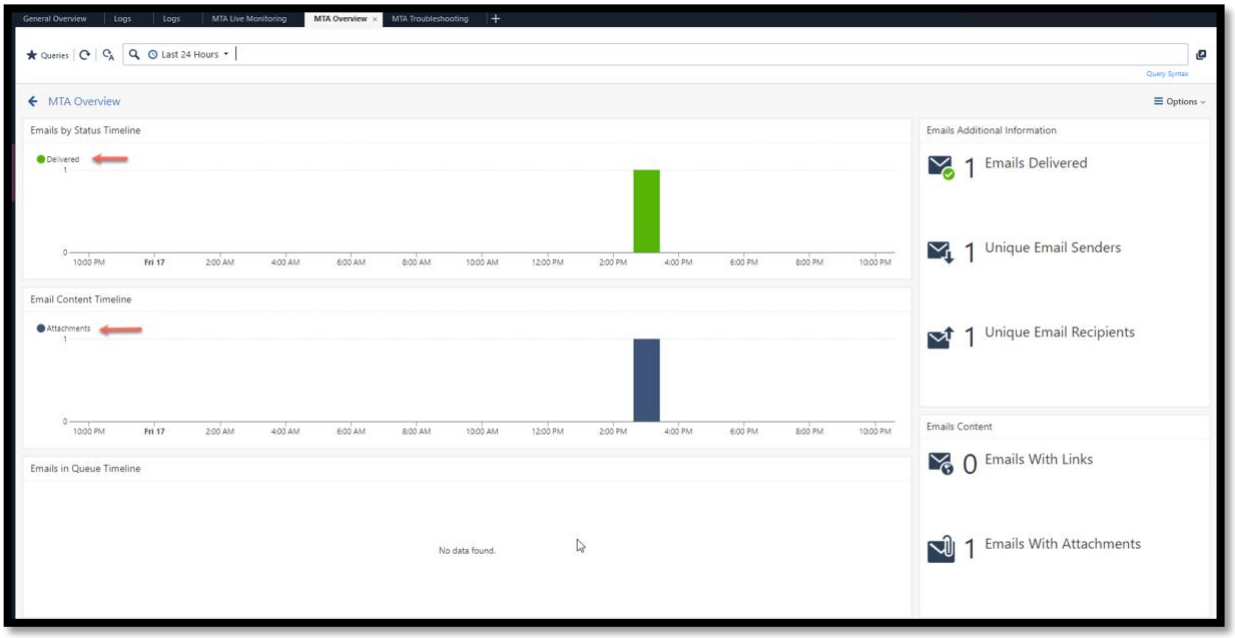
Exercise 3: MTA Monitoring

In this exercise, we will review a set of ways to track and monitor the queue and the performance of the MTA-enabled GW.

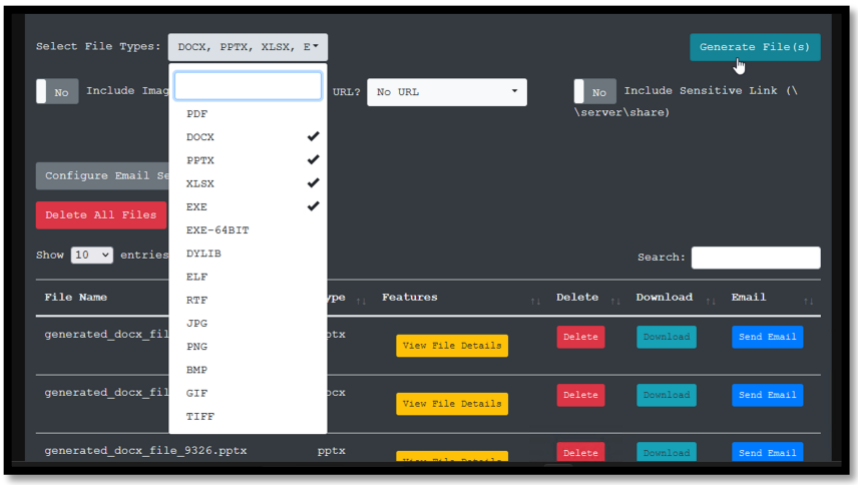
1. From the **SmartConsole** Logs & Events view, open a new tab under **Views** to find all MTA-related views.



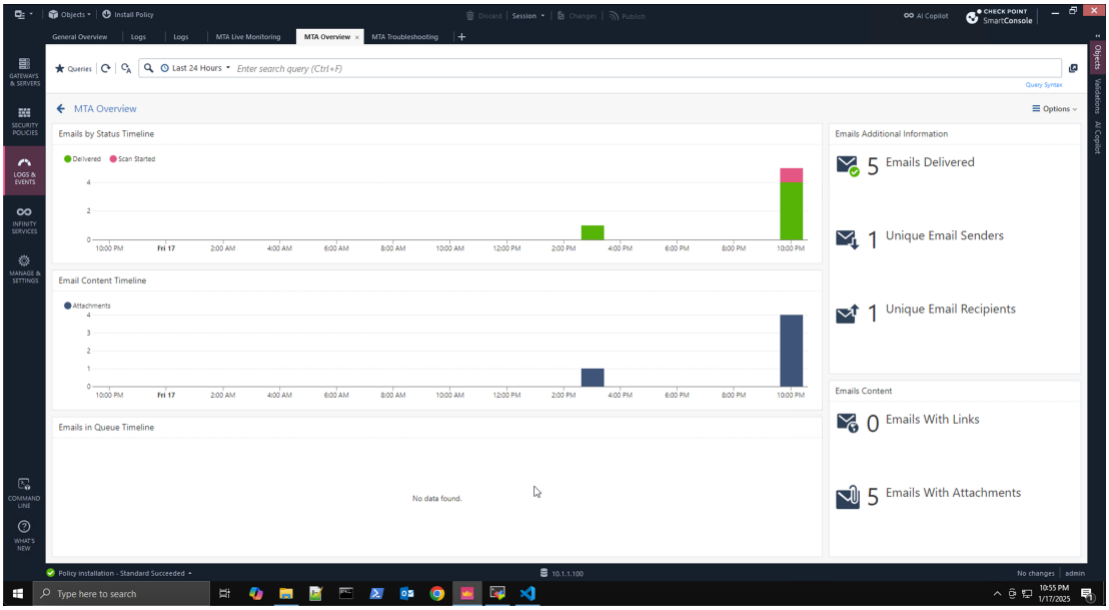
2. Open **MTA Overview** and notice that the MTA processed one email in the past 24 hours, and it is an email with attachment(s).



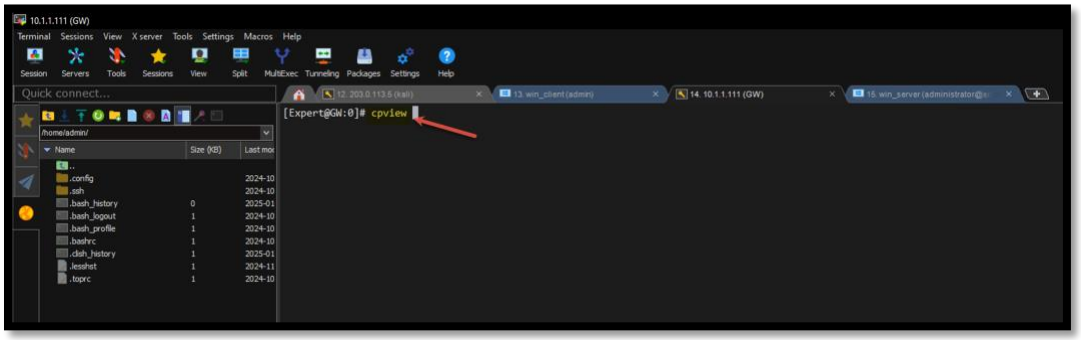
3. Use the demo server to generate and email multiple files.



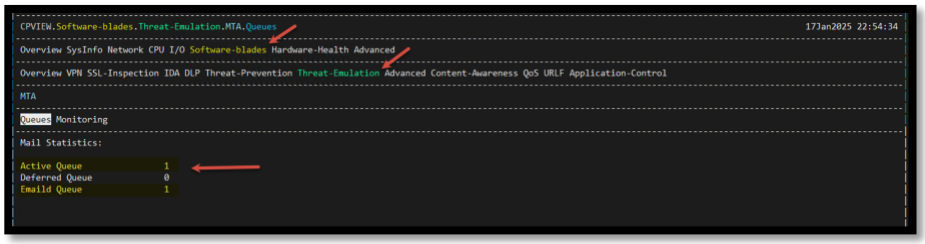
4. Check the **MTA Overview** view in the **SmartConsole** and review the updates.



5. Use the SSH client to connect to the GW and run the CPView tool using the command **cpview**.



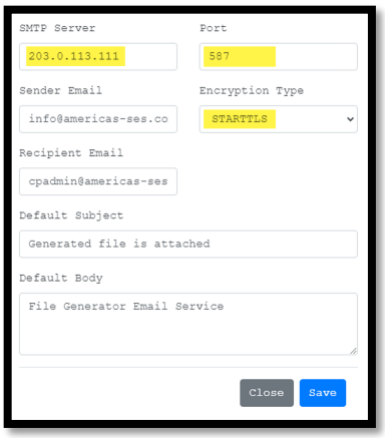
6. Review the MTA queues. You can run native postfix MTA commands.
   Read https://support.checkpoint.com/results/sk/sk109699 for more details.



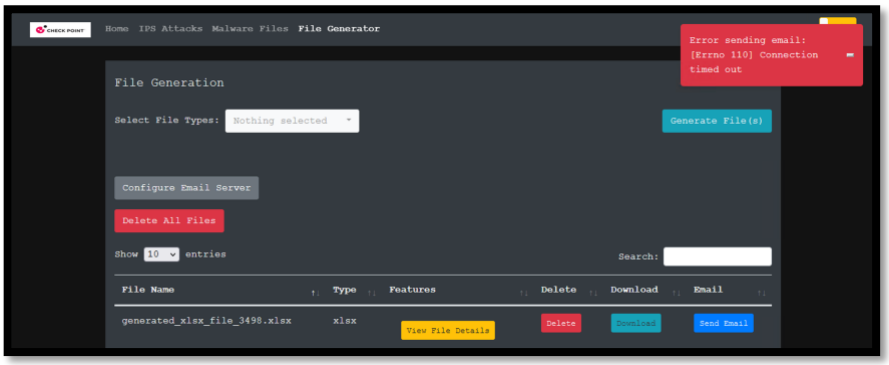
Exercise 3: MTA Over TLS and Port Customization

In this exercise, we will configure the GW MTA mode to communicate using other ports than 25/TCP. By default, the MTA allows SMTP communications over port 25/TCP. Refer to sk142932 for more details.

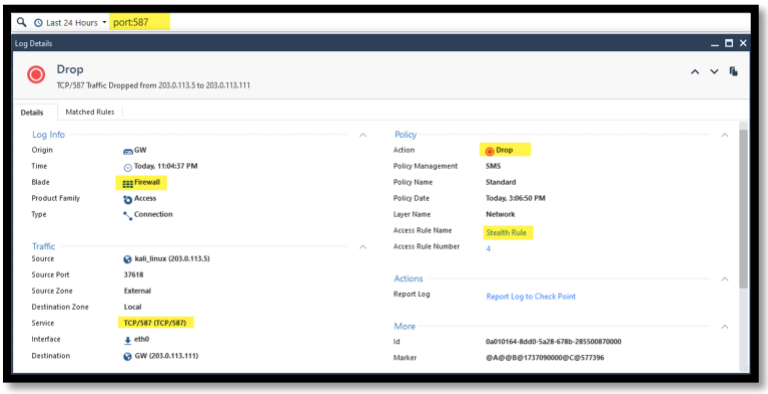
1. From **win_client**, open the Demo Server website and under the File Generator page, set the **Port 587** and the Encryption Type to **STARTTLS**.



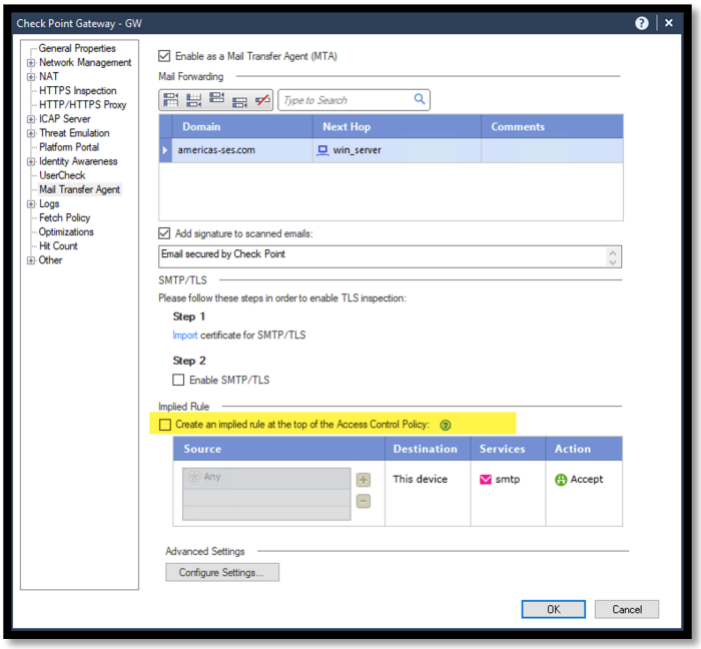
2. Generate a new file and try to email it. *The connection will **time out** after some time*.



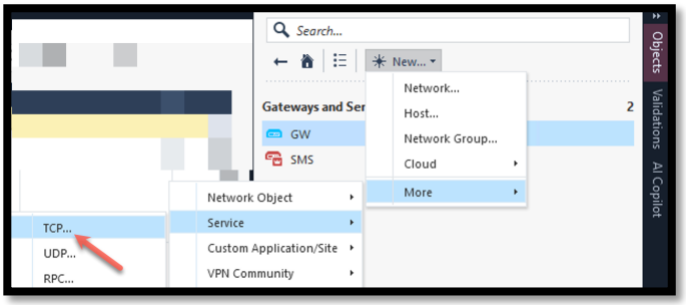
3. From SmartConsole, review the logs on **port 587**. Notice that the Stealth Rule is dropping it. The implied rule accepts traffic on **port 25 by default**.



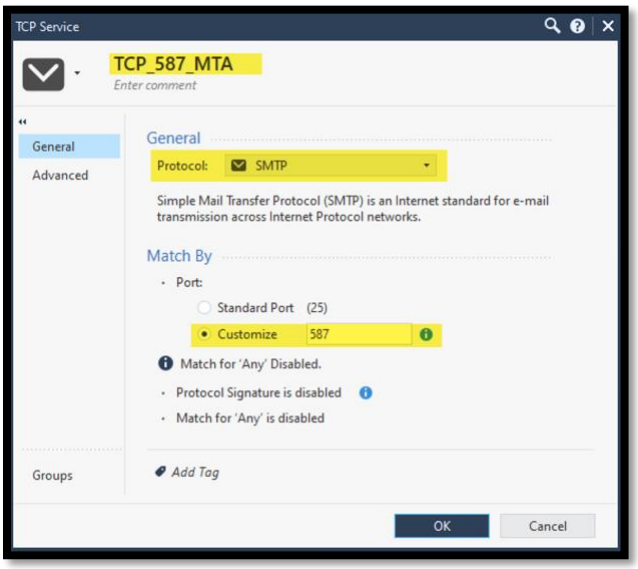
4. Edit the GW object and uncheck the option to create the Access Control implied rule.



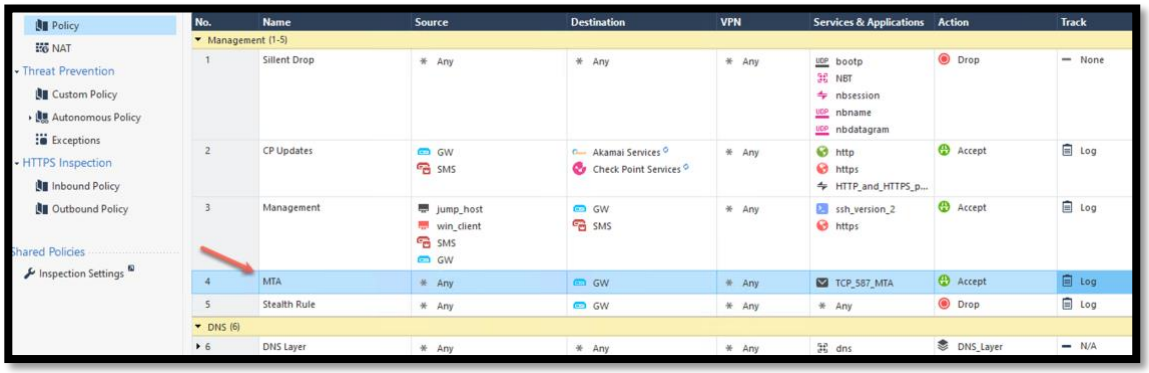
5. Create a new TCP service, we will use this service to accept traffic on the required port 587.



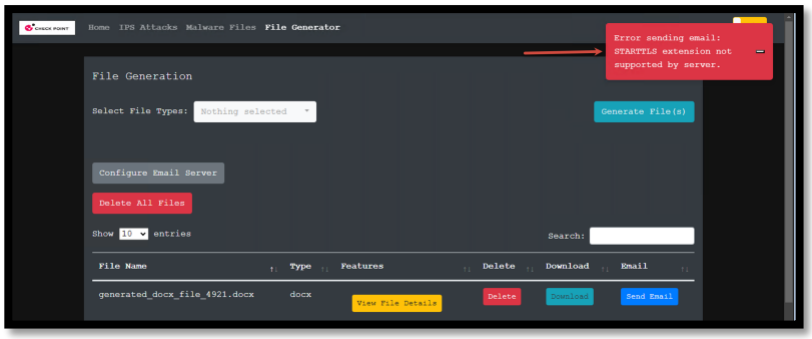
6. We will use the **SMTP** protocol with a customized port set to 587 and save the changes.



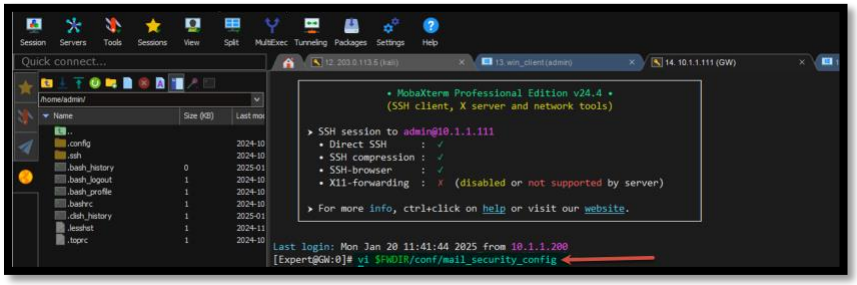
7. Add an access rule for accepting **SMTP** traffic to the Security Gateway on the required Service.



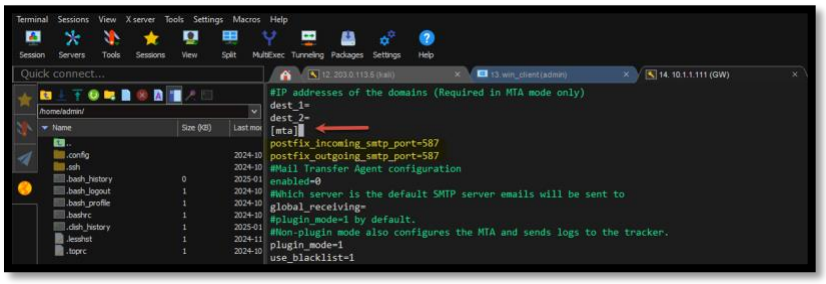
8. Generate a new file and try to send it via email. The error message indicates that the GW MTA mode does not yet support encrypted emails.



9. Use the SSH client MobaXterm to connect to the GW and add the relevant Security Gateway configuration:
    1) Edit the current *$FWDIR/conf/mail_security_config* file using the command below:
        - vi $FWDIR/conf/mail_security_config

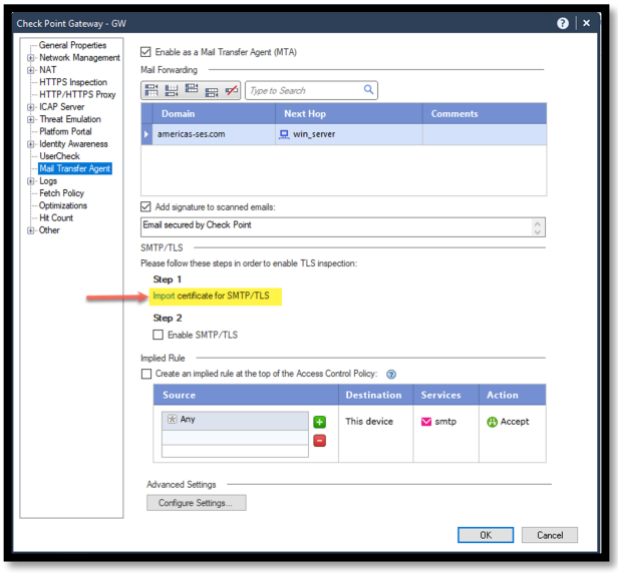


    2) Add the parameters for the new ports under **[mta]** section:
        - postfix_incoming_smtp_port=587
        - postfix_outgoing_smtp_port=587

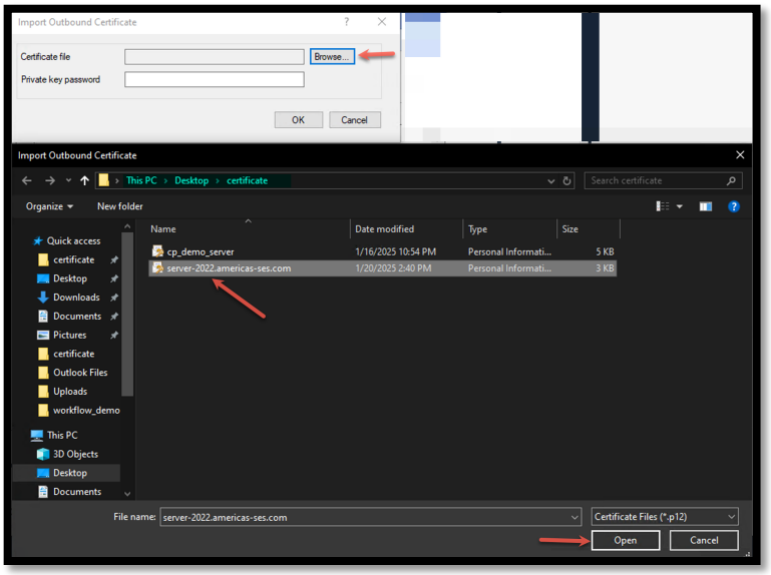


    1. The steps above change the MTA inbound and outbound ports from the default configuration port 25 to the new required port 587. The traffic is expected to be clear and non-encrypted at this stage.

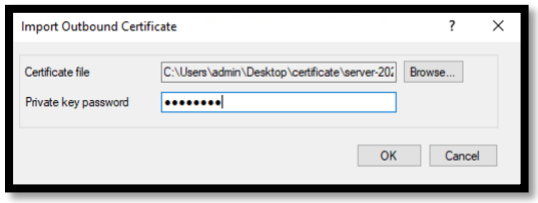
10. Edit the GW object and click **Import certificate for SMTP/TLS.**



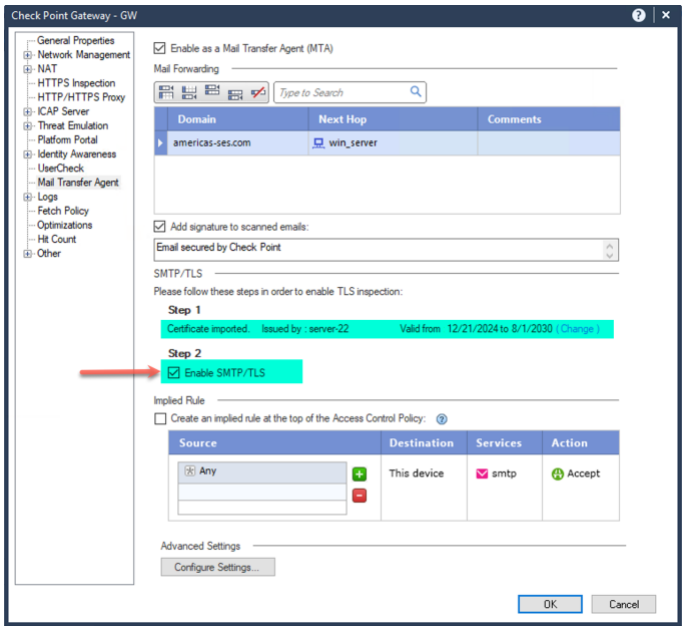
11. From the Import Wizard, navigate to the folder containing the email server certificate on the Jump Server's desktop, where SmartConsole is running.



12. Use the private key password **Cpwins!1**



13. Check the option Enable SMTP/TLS.



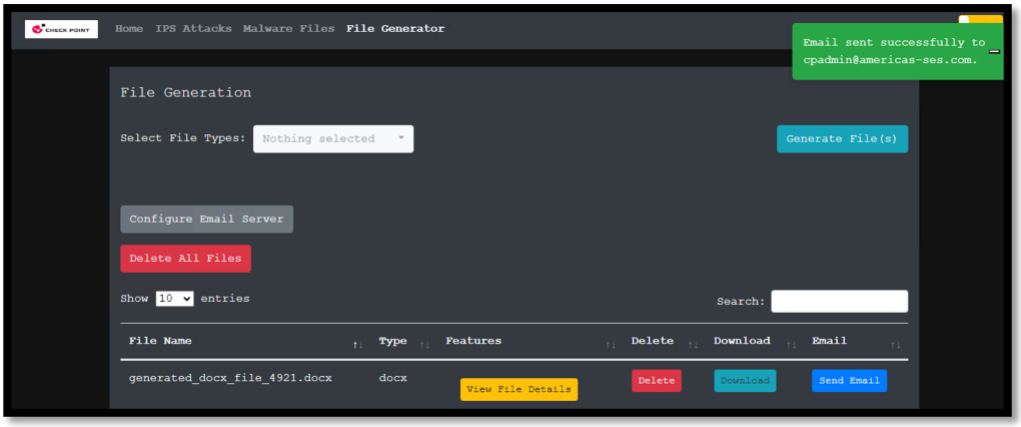
14. Back from the SSH client, create a new file to enable the encrypted mode in MTA
    `vi $FWDIR/conf/mta_postfix_options.cf`

15. Add the following line to enable:
    ***smtp_tls_security_level*=encrypt**

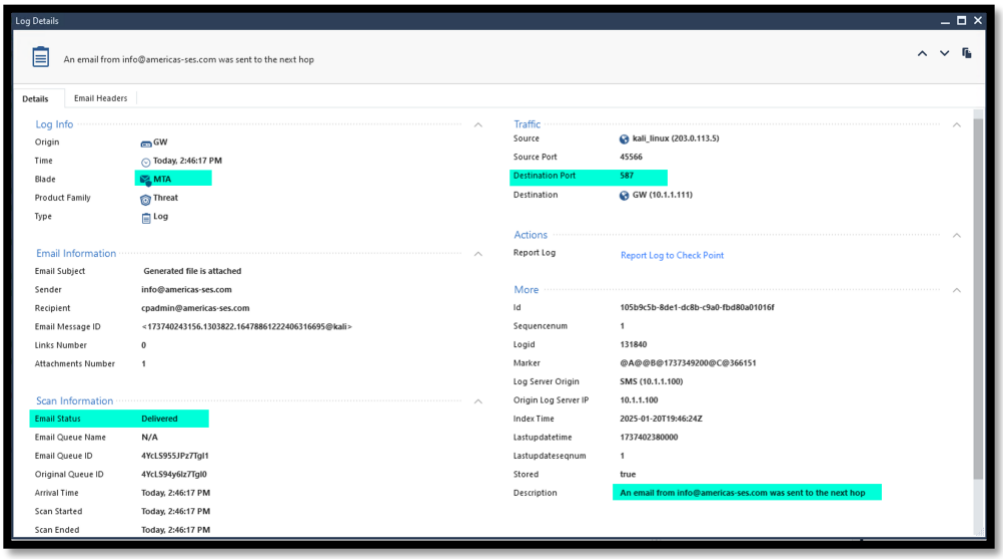
```
[Expert@GW:0]# cat $FWDIR/conf/mta_postfix_options.cf
smtp_tls_security_level=encrypt
```

16. Install the Access Control and Threat Prevention policies.

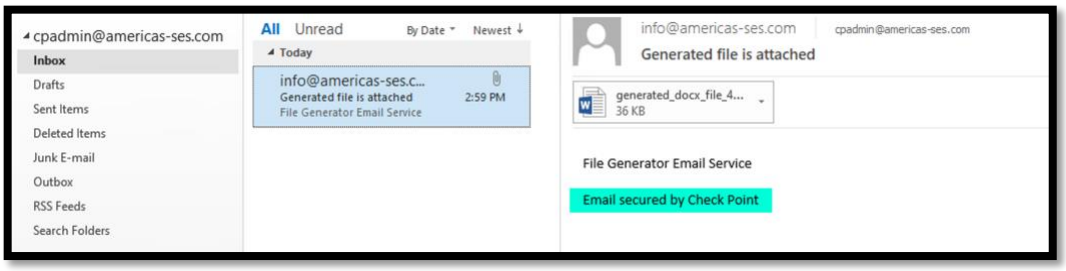
17. Utilize the Demo server website to create a file and send it via email. Ensure that the status pane indicates a successfully sent email.



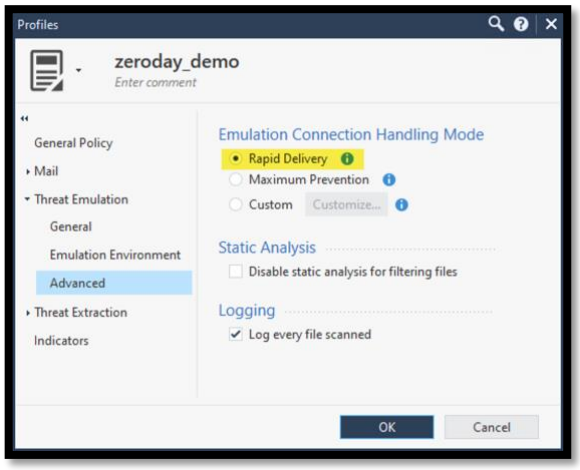
18. Check the logs in SmartConsole and verify that the MTA can manage encrypted emails on port 587.



19. Open Outlook from the **win_client** host and confirm that the email was delivered successfully.



20. Edit the Threat Profile and set the Emulation Connection Handling Mode to Rapid Delivery.



21. Install the Threat Prevention Policy.

End of Lab 9

