

MET PROCESSORS – Vanishing emails

Background Information

You are the Operations Manager of MET and you've been presented with the following incident:

The Problem

We received the first complaints from employees that their Outlook had stopped working and they were not receiving emails that they were supposed to during the afternoon of Tuesday 28th January. An employee said that they had been in contact with a vendor and was promised that an email had been sent to the correct address, she waited for over 20 minutes without receiving it. In fact she has not received any emails during this time but could still navigate to various web sites. Another user said that he always receives bills on the 28th of each month, but he has not received anything yet. Your team asks users more questions and does some initial testing while more complaints are received. It seems as though this problem is affecting the entire company.

After all information from the questions is gathered you can confirm the following:

1. The last confirmed email was received at 14:27 on Tuesday 28th.
2. This outage is affecting all employees, both on site and externally.
3. The outage is affecting both Outlook clients and mobile phone clients (iPhone and Android).

Initial tests were done with company email addresses (corporate) as well as some private email addresses (personal) to create a comparison:

1. Emails sent from corporate email accounts are not received by other employees.
2. Emails sent from personal accounts to corporate employee accounts are not received.
3. Emails sent from corporate accounts to personal accounts are being received.
4. All servers involved with the mail flow are on and responsive. (Firewall was not checked)

Recently the spam server and firewall resource utilization has been high (well above the recommended limits) with several crashes reported. A modification to the "rules" on the spam server was made on Sunday to try and alleviate some of the work; this rule could affect incoming and outgoing emails. At the same time an external DNS change was made to point to a backup server if an interruption occurs, DNS changes take some time to propagate. There have also been alerts of low disk space on the mailbox and Print servers, but have not been followed up on.

You are tasked to solve this problem immediately as it is critical to all work functions. There are a number of elements that could be causing this problem: the connection between the outlook client and the exchange server, the spam server or the DNS server to name a few. The email system is a complex system, and the problem could lie anywhere. The following diagram explains the basic elements of our email flow.

More Information

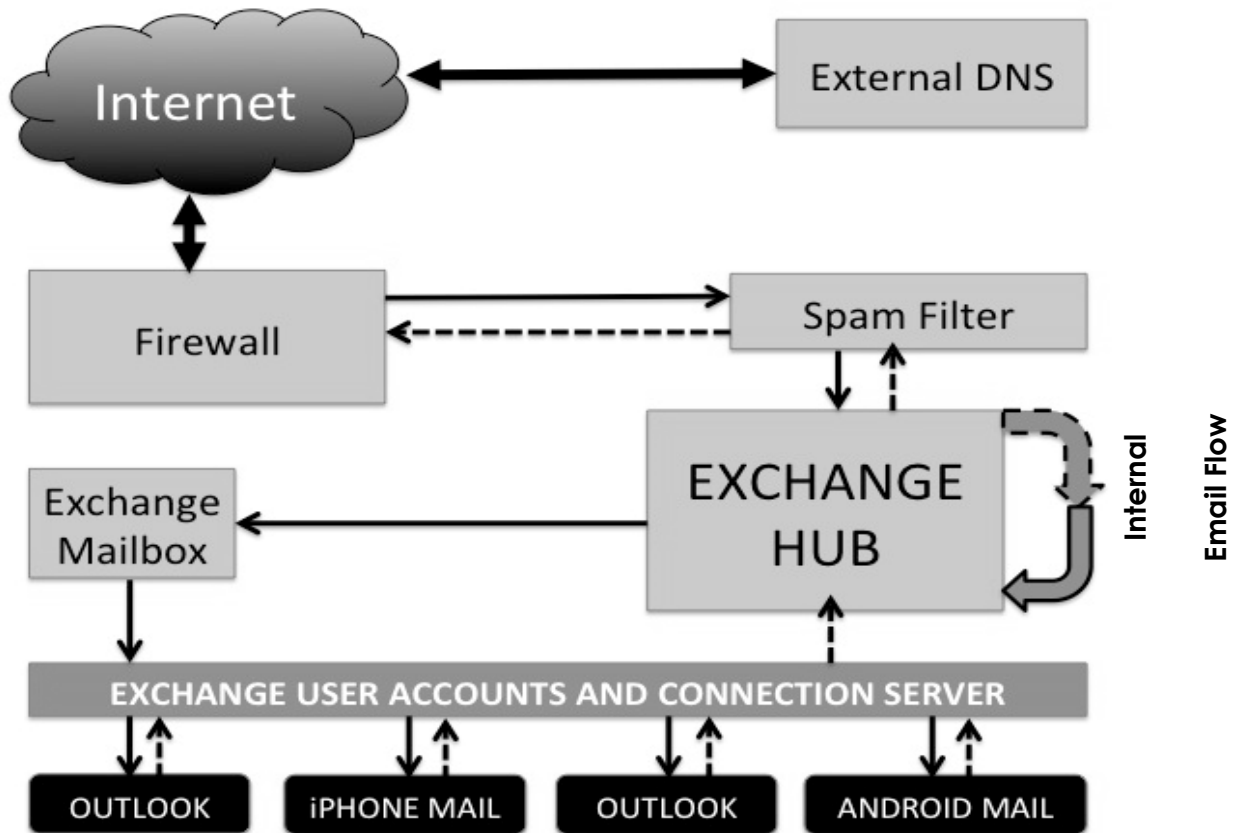


Figure 1: Solid arrows indicate Incoming emails. Dotted arrows indicate outgoing emails.

Device	Description
Spam Filter Server	All Emails pass through the spam filter and emails that don't meet the requirements are removed.
Firewall	This firewall is a standard stable firewall; it allows all mail to pass through without affecting it. However if the firewall is down it should stop all traffic.
Exchange user accounts and connection server	All email accounts are created and stored here. When a user tries to access their email, their client (outlook or mobile) connects to this server, verifies their account details and then syncs with their mailbox.
Exchange Mailbox Server	The mailbox is where all incoming emails are permanently stored for each user. When the emails are synced, the emails are pulled from here onto the user's device.
Exchange Hub Server	The Exchange hub holds all email queues and directs the email. All email pass though this HUB and then either get sent or placed into the appropriate mailbox. Even internal emails pass through the HUB.
External DNS Server	The location of the receiving exchange server is stored here. Only emails from external users will check the DNS server to see where they have to send the emails.