**SUPPORT DE COURS SECURISATION DE LA MESSAGERIE**

**M1 Sécurité et Administration Système**

**Université Polytechnique de Bingerville**

1. **RAPPELS SUR LA MESSAGERIE ELECTRONIQUE**
2. **Les protocoles de la messagerie électronique**

Il existe 3 protocoles essentiels pour la messagerie :

* SMTP (Simple Mail Tranfer Protocol) ;
* POP3 (Post Office Protocol) ;
* IMAP (Internet Message Access Protocol).

1. **Les services de la messagerie électronique**

Nous avons 3 services essentiels de la messagerie :

* MUA (Mail User Agent ou Agent de Gestion du Courrier)
* MTA (Mail Transfer Agent ou Agent de Transfert de Courriers)
* MDA (Mail Delivery Agent ou Agent de Distribution de Courriers)

Expéditeur

gouho@upb.ci

Destinataire

bali@setistech.ci

SMTP

SMTP

POP3

OU

IMAP

POP3

OU

IMAP

1. **Généralités sur le protocole SMTP**

La RFC (Request For Comments) du protocole SMTP est la RFC 821. Cette RFC définie les messages de base échangés lors d’une session SMTP. Cela se fait par les mots clés suivant :

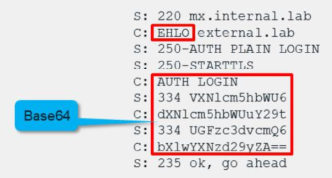
* **HELO** : initie une session SMTP ;
* **MAIL FROM** : indique l’adresse mail de l’émetteur ;
* **RCPT TO** : indique l’adresse mail du récepteur ;
* **DATA**: montre le contenu du mail ;
* **RSET**: termine une session active ;
* **NOOP**: maintient une session active ;
* **QUIT**: termine une session correctement ;
* **2xx, 3xx, 4xx, 5xx** : représentent les codes à trois chiffres utilisés pour les réponses

Par serveur.

Il existe une version complémentaire de la RFC 821 qui est la RFC 1869 pour « Extended SMTP (ESMTP) ». La RFC 1869 introduit des fonctionnalités comme **STARTTLS** et **AUTH** qui sont utilisés pour le cryptage du corps du mail.

Dans les débuts de SMTP en 1982 il n’y avait de processus de sécurité lors de la transmission des mails, mais dans les années 90 « AUTH » fût introduit dans le but de permettre à des utilisateurs autorisés d’envoyer des mails à des serveurs externes dont l’identité a été vérifier.

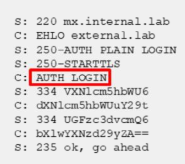
Elle ajoute de la sécurité mais ne permet pas de lutter contre les messages provenant des adresses usurpées provenant d’un serveur externe.



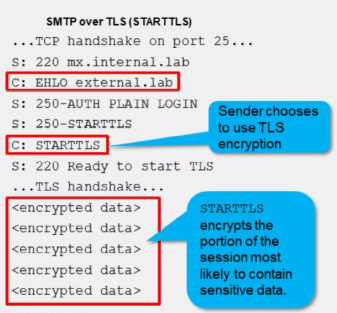
**Figure 1 : Session AUTH**

« STARTTLS » a été ajouté comme une option par ESMTP pour le cryptage des messages avec TLS (Transport Layer Security). Ce qui fera que le MTA acceptera seulement les enveloppes d’adresses (MAIL FROM, RCPT TO) des serveurs où TLS est activé.

La figure 2 et 3 nous montre cela.

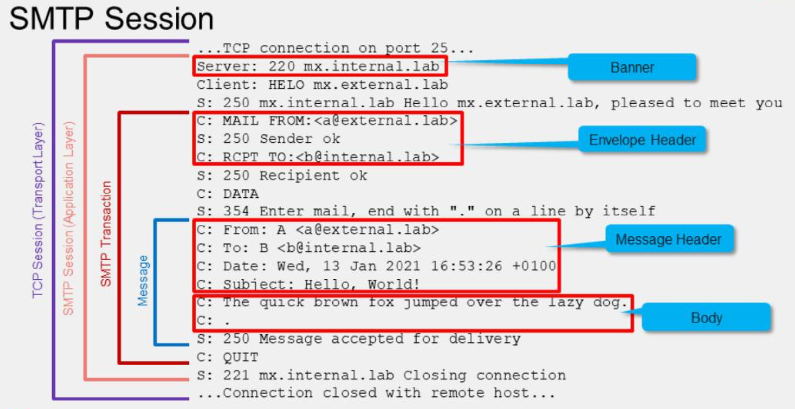


**Figure 2**



**Figure 3**

La figure 4 nous présente une session SMTP.



**Figure 4 : session SMTP**

La figure nous présente une session SMTP initier entre un client et un serveur de messagerie par le port classique du SMTP qui est le port TCP 25.

Si la session est établie, le serveur présente une bannière au client ce qui permettra au client d’envoyer un message « **HELO** » que le serveur devra accepter.

Le client utilise la commande « **DATA** » pour indiquer départ du message, cela inclus un entête et le corps du message.

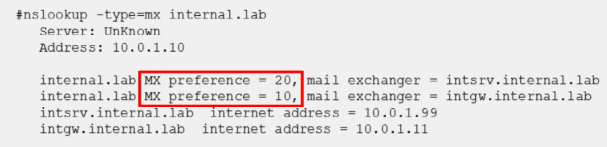
Le client envoie un «**.**» pour indiquer la fin du message et le serveur envoie un accusé de réception. Pour finir la session TCP le client envoie un « **QUIT** » que le serveur doit accepter pour terminer la session.

Ce processus est exécuté chaque fois qu’il a un échange entre un « MUA » et un « MTA » ou entre « MTA » et un « MTA ».

Cela diffère chez Microsoft qui utilise son protocole propriétaire qu’est MAPI (Messaging Application Programming Interface) pour les échanges entre Microsoft Outlook et Microsoft Exchange server.

1. **Le Mail eXchanger (MX)**

L'enregistrement MX, également appelé « Mail Exchanger Record », est la partie du système de noms de domaine (DNS) qui fournit des informations sur le serveur de messagerie utilisé par votre nom de domaine. Vous pouvez éventuellement indiquer plusieurs enregistrements MX, chacun avec une priorité différente.

Lorsque plusieurs MTA sont indiqués, la valeur de la préférence la moins élevée sera celle qui sera prioritaire.

1. **GENERALITES SUR LES SYSTEMES DE SECURISATION DE LA MESSAGERIE AVEC FORTIMAIL**

FortiMail protège les organisations contre toute la gamme des menaces basées sur le courrier électronique telles que le phishing, les ransomware, le zéro jour et les attaques de compromis par courrier électronique (BEC). Cette solution exploite les services de sécurité alimentés par l'IA FortiGuard développés par FortiGuard Labs, fournissant des technologies de sécurité de pointe pour prévenir, détecter et répondre aux menaces basées sur le courrier électronique en temps réel.

FortiMail offre une protection complète et éprouvée contre les menaces par courrier électronique. En outre, FortiMail offre une flexibilité grâce à des options de déploiement, y compris des moyens de sécurité en tant que service de courrier électronique, et des modes d'exploitation pour des environnements de courrier électronique basés sur le cloud, sur site ou hybrides.

Les avantages de FortiMail sont :

* **Protection de l'IA**

Utilisations des services de sécurité mis au point et optimisés par FortiGuard AI.

* **Protection contre les attaques de type « zéro jour »**

Étudie avec FortiSandbox pour l'analyse de fichiers afin de détecter des logiciels malveillants sophistiqués et des menaces de type « zéro jour ».

* **Protection Microsoft 365**

Fournit une sécurité avancée pour les modèles de support d'API Exchange Online via la passerelle.

* **Protection contre les ransomwares**

Détecte et empêche les charges utiles de ransomware d'atteindre les boîtes de réception avec les technologies d'analyse de fichiers URL

* **Détection d’usurpation d'identité**

Détecte l'usurpation d'identité et les attaques BEC avec vérification de l'expéditeur, la détection de domaine.

1. **Les modes de fonctionnement de Fortimail**

La passerelle de sécurisation de la messagerie Fortimail à 3 modes de fonctionnement :

* Le mode serveur ;
* Le mode gateway ;
* Le mode transparent.

1. Mode gateway

C’est mode par défaut de fonctionnement de Fortimail lors de la prise en main.

Ce mode travail un DNS MX et tous les mails provenant de l’extérieur passent d’abord par le Fortimail qui pourra ensuite router les mails vers le serveur de messagerie.