SEC105 - Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications

PEI Millau – Concepteur Architecte Informatique (toutes spécialités)

Objectif : comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité de base sur les messages (stockage et transport) et architectures de messageries (Windows Exchange, Web, IMAP, configuration port SSL), des interactions avec les services de résolution de nom, d'adresse, d'authentification et d'annuaire.

Thème : Architectures et protocoles de sécurité pour la messagerie

Préambule

L'usage de la messagerie électronique pour les besoins professionnels est très répandu, quels que soient la taille et le secteur d'activité de l'entité.

Les boîtes aux lettres électroniques regorgent d'informations métier ou techniques qui, agrégées, en font des cibles de choix pour les attaquants.

Dans le même temps, ce service est devenu un des principaux vecteurs d'attaque informatique :

- tentative d'hameçonnage pour récupérer des données personnelles,
- envoi de pièces jointes malveillantes pour exploiter les vulnérabilités d'un poste de travail à des fins de rançonnage ou d'espionnage, etc.

Nous allons donc essayer de faire un tour d'horizon des principaux moyens à notre disposition pour faire face à la menace.

Identifier le besoin pour maîtriser les risques

Phase 1 - état des lieux :

- la messagerie électronique est généralement identifiée comme un service nécessitant une interconnexion à Internet avec des flux entrants et sortants.
- Mais nous pouvons détailler ce besoin afin de distinguer des usages types et leur spécificités :
  - la messagerie pour les échanges des collaborateurs, entre eux ou avec l'extérieur, dite ***messagerie bureautique*** ;
  - la messagerie pour les activités métier, par exemple pour les échanges avec les clients dans le cadre d'un service après-vente ; celle-ci, dite ***messagerie métier***, est potentiellement interconnectée à un progiciel de gestion de la relation client ;
  - la messagerie pour les besoins techniques, de supervision ou d'alerte ; celle-ci, dite ***messagerie technique***, est généralement interconnectée à des outils de supervision ou de suivi de tickets, et permet parfois des échanges machine à machine.

Identifier le besoin pour maîtriser les risques

Il est important d'identifier les messageries qui nécessitent la réception ou l'envoi de courriels, lesquelles doivent être interconnectées entre elles, et lesquelles nécessitent une interconnexion à Internet.

Par exemple, une messagerie technique peut être cloisonnée au sein du SI de l'entité sans interconnexion à Internet, alors qu'une messagerie métier peut nécessiter l'envoi et la réception de courriels sur Internet.

Identifier le besoin pour maîtriser les risques

Phase 2 – analyse de risques :

Une fois ces besoins identifiés, il convient de mener une analyse de risque spécifique au service de messagerie électronique, selon une méthodologie telle EBIOS Risk manager ou, pour les entités moins matures, sur la base de questions simples, pour identifier les besoins de sécurité :

- quelle est l'indisponibilité acceptable de ce service ?
- quelles seraient les conséquences de la destruction de l'ensemble des courriels ?
- quelles seraient les conséquences de la récupération de l'ensemble des courriels par un tiers, éventuellement le fournisseur du service de messagerie ou un concurrent ?
- quelles seraient les conséquences d'une usurpation d'identité de l'expéditeur ?

L'administration fonctionnelle du service, qu'elle soit internalisée ou externalisée, doit également être traitée avec attention dans l'analyse de risque.

En effet, les administrateurs de messagerie ont des droits privilégiés leur donnant accès aux paramètres et aux contenus des boîtes aux lettres.

Connaitre l'architecture pour maîtriser les risques

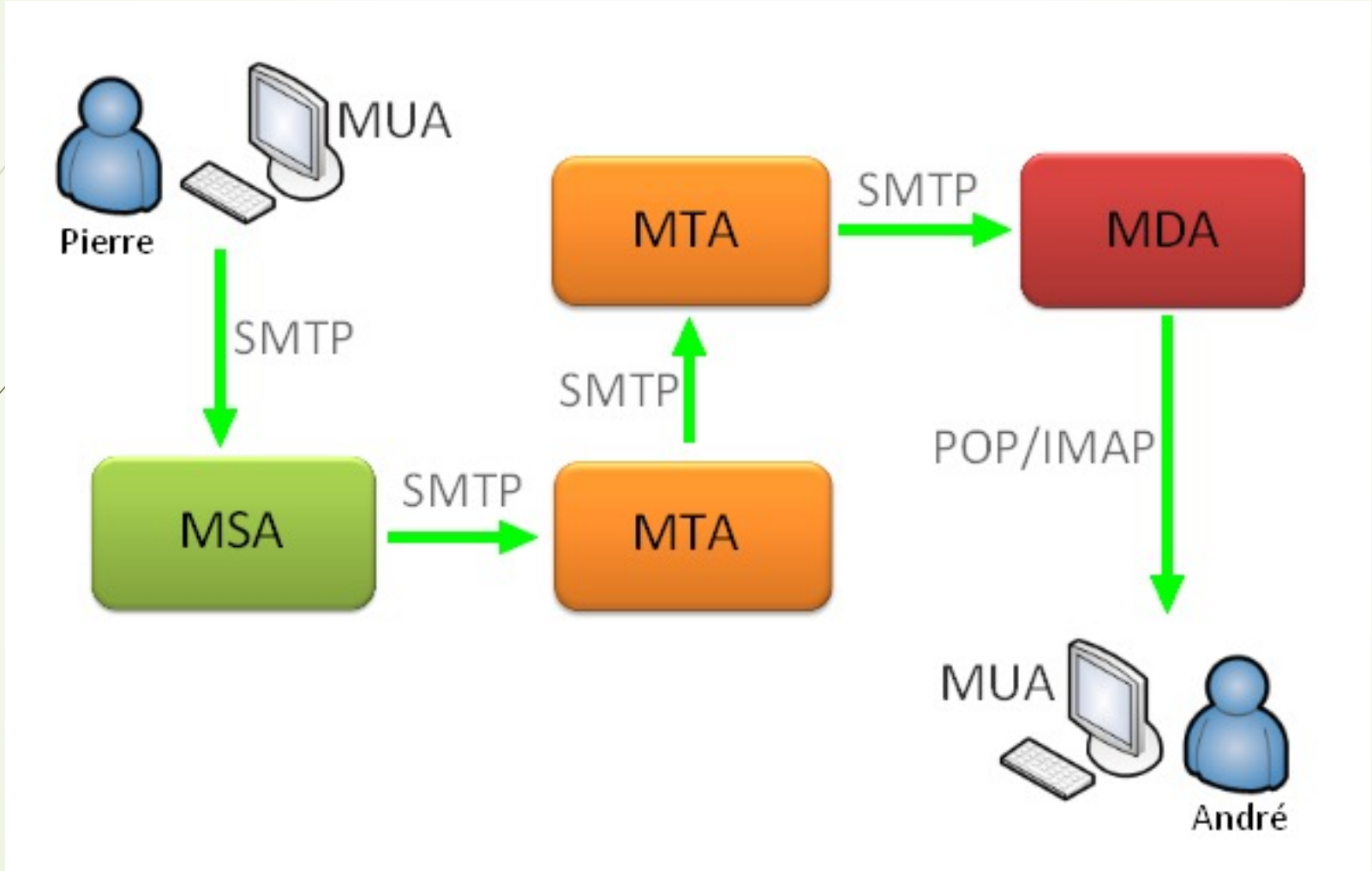
Identifier les composantes de notre service de messagerie :

Afin de produire, stocker et transmettre des courriels, il existe un nombre important de composants logiciels intervenant dans un système de messagerie électronique. Il ne s'agit pas ici d'expliquer en détail ces différents composants du point de vue fonctionnel, mais d'avoir un vocabulaire commun pour expliquer les concepts de sécurité à appliquer.

De façon simplifiée, on distingue dans les systèmes de messagerie électronique :

- les clients de messagerie (Mail User Agent) qui permettent de produire et consulter des courriels ;
- les serveurs de boîtes aux lettres (mailboxes) qui stockent des courriels ;
- les serveurs de transfert de courriels (Mail Transfer Agent) dits aussi serveurs relais, ou serveurs SMTP (Server Mail Transfer Protocol) – du nom du protocole qu'ils utilisent majoritairement pour la transmission des courriels à travers les réseaux. Le premier serveur relais, qui accepte les courriels des clients de messagerie, est appelé (Mail Submission Agent) et le dernier serveur relais, qui délivre les courriels dans les boîtes aux lettres, est appelé (Mail Delivery Agent).

Connaitre l'architecture pour maîtriser les risques



Cloisonner et filtrer

Sauf cas particulier, les serveurs de boîtes aux lettres, accessibles par les clients de messagerie, doivent être hébergés au sein du SI de l'entité. Ils peuvent communiquer avec des serveurs relais internes au SI de l'entité, ou des serveurs SMTP, au sein de la passer elle Internet sécurisée, pour les échanges sur Internet.

Voici les recommandations de l'ANSSI à ce sujet :

Déployer les serveurs de boîtes aux lettres au sein du SI

Les serveurs de boîtes aux lettres et le stockage associé doivent être déployés au sein du SI de l'entité (et non au sein de la passerelle Internet sécurisée).

Déployer les serveurs relais en fonction des stricts besoins

Pour les besoins de messagerie strictement internes à l'entité, au moins un serveur relais doit être positionné au sein du SI de l'entité, et dédié à cette fonction. Ce serveur ne doit pas être chaîné avec un serveur SMTP exposé sur Internet.
Pour les besoins de messagerie externes à l'entité (*i.e.* avec une interconnexion à Internet), au moins un serveur SMTP doit être positionné au sein de la passerelle Internet sécurisée.

Cloisonner et filtrer

Cloisonner les serveurs SMTP d'envoi et de réception

Il est recommandé de cloisonner les serveurs SMTP d'envoi et de réception (ex. : deux machines virtuelles distinctes) au sein de la passerelle Internet sécurisée. Ils doivent être configurés en conséquence ; par exemple :

- un serveur SMTP d'envoi n'accepte les courriels que depuis une liste de serveurs autorisés (serveurs relais internes ou serveurs de boîtes aux lettres) et assure des fonctions de nettoyage des en-têtes (cf. recommandation R21) ;
- un serveur SMTP de réception applique les premières politiques de sécurité, assure des fonctions d'analyse protocolaire et de contenu, qualifie les courriels nécessitant une mise en quarantaine, transmet *in fine* les courriers à un autre serveur relais de l'entité ou à un serveur de boîtes aux lettres.

Cloisonner et filtrer

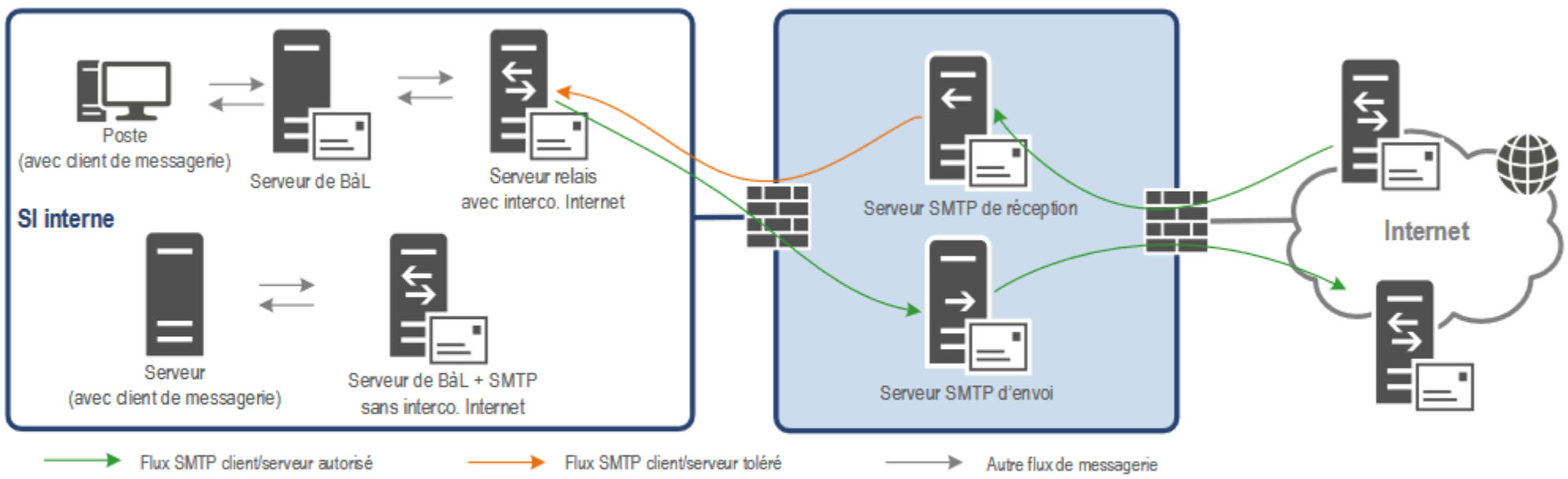


FIGURE 5.1 – Exemple d'architecture de messageries (interconnectées ou non à Internet)

Cloisonner et filtrer

Dès lors que les serveurs de boîtes aux lettres et les serveurs relais sont positionnés dans l'architecture, ils doivent être les seuls à pouvoir échanger grâce aux protocoles de messagerie (ex. : SMTP,MAPI).

De plus, les clients de messagerie doivent se connecter exclusivement aux serveurs de boîtes aux lettres, avec les protocoles **ad hoc**(ex. : IMAPS, MAPI).

Cela doit se traduire dans les matrices de flux internes, et propres à la passerelle Internet sécurisée, afin d'éviter l'envoi, ou la réception, de courriels par d'autres machines.

Source \ Destination	Postes clients utilisateurs	Postes clients scanner de bureau	Proxy frontal	Serveur HTTPD / Maarch Apps	Cluster SGBDR PostgreSQL	Serveur messagerie	Serveur Annuaire
Postes clients utilisateurs			Https (443)				
Postes clients scanner de bureau			Https (443)				
Proxy frontal	Https (443)	Https (443)					
Serveur HTTPD / Maarch Apps			Http (80)	Http (80)	tcp/ip (5432)	IMAP (143) ou IMAPS (993)	389
Cluster SGBDR PostgreSQL				tcp/ip (5432)			
Serveur messagerie				IMAP (143) ou IMAPS (993)			
Serveur Annuaire				389			

Cloisonner et filtrer

N'autoriser les protocoles de messagerie qu'entre infrastructures légitimes

Afin d'éviter des usages détournés du service de messagerie électronique, les protocoles de messagerie doivent être autorisés selon le strict besoin opérationnel des infrastructures légitimes.
En particulier, l'utilisation illégitime des ports SMTP (TCP/25 sans chiffrement et TCP/465 avec chiffrement implicite) par un serveur autre qu'un serveur SMTP doit générer des journaux au niveau des pare-feux et une alerte de sécurité.

Mettre en place des mécanismes antispam et de recherche de contenu malveillant

La messagerie électronique étant un vecteur de compromission, des mécanismes doivent être mis en œuvre pour tenter de détecter (et stopper dans la mesure du possible) au plus tôt les courriels indésirables (spam).

Ces mécanismes doivent en particulier couvrir la recherche de contenu malveillant. Le blocage des courriels indésirables, dont font partie les courriels d'hameçonnage (phishing), est généralement complexe à mettre en œuvre, d'un point de vue technique, pour être efficient.

Il nécessite une attention particulière pour éviter les faux-positifs (un courriel bloqué qui ne serait en fait pas indésirable) ayant un impact direct pour les utilisateurs.

Différents mécanismes d'analyse des en-têtes d'une part, et des corps de courriels d'autre part existent, par exemple :

- les listes d'autorisations, d'interdictions ou d'interdictions provisoires (aussi appelées listes blanche, noire et grise) d'adresses IP ou de noms de domaine permettant respectivement d'autoriser, de bloquer ou de bloquer temporairement les courriels en provenance de ces sources ;
- l'analyse heuristique du corps des courriels ;

Mettre en place des mécanismes antispam et de recherche de contenu malveillant

- le test de Turing permettant d'identifier l'expéditeur comme un humain (ex. : reproduction d'un code affiché dans une image, ou calcul d'une opération lors de la réception du premier courriel d'un nouvel expéditeur).

L'activation de ces mécanismes complémentaires n'est pas nécessairement systématique pour chaque courriel reçu. Par exemple, un courriel reçu depuis un domaine présent dans une liste d'autorisations peut dispenser d'un test de Turing pour l'expéditeur. Ce test peut être activé en dernier recours pour un courriel dont le caractère indésirable n'a pas pu être déterminé par d'autres mécanismes.

Mettre en place des mécanismes antispam et de recherche de contenu malveillant

Ces mécanismes antispam permettent d'éliminer une part importante de courriels indésirables mais ne sont pas des remparts infaillibles contre des courriels indésirables ciblés.

En effet, un attaquant peut respecter les standards de rédaction d'un courriel, utiliser un serveur d'envoi légitime et valider un test de Turing.

De manière complémentaire, les pièces jointes d'un courriel doivent être analysées par un antivirus ; cette analyse préalable à la délivrance du courriel sur le client de messagerie ne se substitue pas à une analyse antivirus au niveau du poste de travail, préférentiellement avec une technologie distincte.

De plus, une analyse des liens contenus dans le corps des courriels doit être menée afin de détecter ceux vers des pages Web malveillantes (ex. : site Web d'hameçonnage imitant un site légitime en vue de récupérer des données personnelles).

Maitriser l'exposition des utilisateurs à la messagerie sur Internet

Afin de garder la maîtrise des courriels échangés et stockés, mais également de limiter la surface d'attaque du SI de l'entité, il est recommandé de ne pas exposer sur Internet les accès utilisateurs à la messagerie.

Dans ce cas, conformément au guide ANSSI sur le nomadisme numérique, les utilisateurs nomades doivent accéder à leurs courriels exclusivement depuis un équipement(ordinateur, tablette, mobile multifonction) maîtrisé par l'entité, à travers un tunnel VPN établi jusqu'au SI de l'entité.

Utiliser des canaux de transport sécurisés

Sécuriser le canal de transport entre clients de messagerie et serveurs de boîtes aux lettres

Quel que soit le protocole utilisé, les flux de messagerie entre les clients de messagerie et les serveurs de boîtes aux lettres doivent être chiffrés et authentifiés. Cette authentification des flux est complémentaire à l'authentification applicative des utilisateurs.
Ainsi, l'utilisation des protocoles sécurisés de messagerie, désormais standards (ex. : SMTPS, POPS, IMAPS ou HTTPS) est recommandée.

Activer l'option STARTTLS sur les serveurs SMTP

Sur les serveurs SMTP, l'option STARTTLS doit être activée avec une configuration TLS supportant l'état de l'art et tolérant des paramètres d'un niveau de sécurité moindre.
Le cycle de vie des certificats doit être traité avec attention.
De plus, il est recommandé dans ce cas de désactiver sur les serveurs SMTP, et de bloquer sur les briques de filtrage, le service SMTP avec chiffrement implicite (TCP/465).

Activer l'option REQUIRETLS sur les serveurs SMTP

Pour forcer les échanges à travers un canal TLS avec une entité destinataire qui le supporte, il est recommandé d'activer l'option REQUIRETLS.

Se protéger contre les courriels illégitimes

Certaines attaques commencent par des campagnes de courriels usurpant l'identité d'expéditeurs légitimes.

Il s'agit d'un cas particulier de courriels indésirables, pour lesquels des recommandations générales vues précédemment.

Pour limiter la nuisance de ces courriels, en amont de leur réception par les utilisateurs, certains protocoles ont pour rôle de vérifier l'authenticité et l'intégrité des courriels. Ils nécessitent une configuration, non seulement par l'entité expéditrice sur les enregistrements DNS de ses noms de domaine, mais aussi par l'entité destinataire sur ses serveurs SMTP de réception. Ces protocoles sont :

- ***Sender Policy Framework (SPF)*** qui permet de spécifier les adresses IP des serveurs autorisés à émettre les courriels d'un domaine ;
- ***Domain Keys Identified Mail (DKIM)*** qui permet l'authentification du domaine de messagerie d'un courriel à l'aide d'une signature cryptographique ;
- ***Domain-based Message Authentication, Reporting and Conformance (DMARC)*** qui permet notamment à une entité de définir une politique de traitement de ses courriels envoyés en fonction des résultats de conformité SPF et DKIM.

Se protéger contre les courriels illégitimes

Ces protocoles ont un intérêt double pour l'entité :

- en tant que destinataire, ils renforcent la vérification de la légitimité des courriels reçus ;
- en tant qu'expéditrice :
  - ils fournissent, aux destinataires des courriels qu'elle envoie, des informations techniques pour s'assurer de la légitimité des courriels envoyés,
  - ils lui permettent de recevoir des statistiques sur l'utilisation de son ou ses domaines de messagerie

Se protéger contre les courriels illégitimes

Cas d'utilisation type :

- l'envoi d'un courriel comportant une signature DKIM (dit courriel signé) depuis le domaine *monpartenaire.fr* et sa réception par le serveur SMTP de l'entité ;
- la vérification des paramètres SPF, DKIM et DMARC du courriel...
- .... nécessitant le recours aux enregistrements DNS publics de l'expéditeur ;
- enfin, l'envoi d'un rapport DMARC à l'expéditeur selon la politique qu'il a définie,

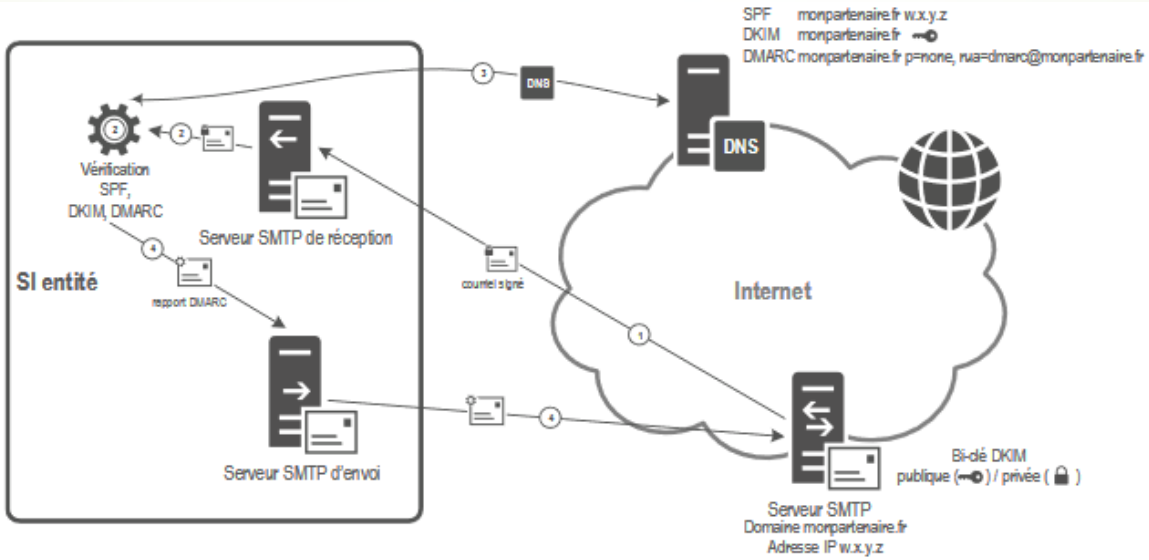


FIGURE 5.2 – Cinématique simplifiée du fonctionnement de SPF, DKIM et DMARC pour une entité destinataire de courriels

Se protéger contre les courriels illégitimes

SPF : « *Sender Policy Framework* »

- Sender Policy Framework (SPF) est une norme de vérification du nom de domaine de l'expéditeur d'un courrier électronique, normalisée dans la RFC 7208.
- L'adoption de cette norme est de nature à réduire le spam.
- Le protocole Simple Mail Transfer Protocol (SMTP) utilisé pour le transfert du courrier électronique sur Internet ne prévoit pas de mécanisme de vérification de l'expéditeur, c'est-à-dire qu'il est facile d'envoyer un courrier avec une adresse d'expéditeur factice, voire usurpée.
- SPF vise à réduire les possibilités d'usurpation en publiant, dans le DNS, un enregistrement (de type TXT) indiquant quelles adresses IP sont autorisées ou interdites à envoyer du courrier pour le domaine considéré.
- L'identité testée par SPF est celle indiquée par la commande MAIL FROM dans la session SMTP. C'est donc une information qui appartient à l'enveloppe du courrier, pas à ses en-têtes. (Dans certaines conditions, SPF peut aussi utiliser le nom de la machine expéditrice, tel que spécifié dans la commande HELO.)

Se protéger contre les courriels illégitimes

DKIM : « DomainKeys Identified Mail »

- DKIM (DomainKeys Identified Mail) est une norme d'authentification fiable du nom de domaine de l'expéditeur d'un courrier électronique. Elle constitue une protection efficace contre le spam et l'hameçonnage.
- DKIM fonctionne par signature cryptographique du corps du message ou d'une partie de celui-ci et d'une partie de ses en-têtes.
- Il s'agit d'ajouter dans tous les emails sortant, une signature DKIM contenant une liste de "clé=valeur". Les clés sont courtes, généralement une ou deux lettres.
- Les paramètres par défaut du mécanisme de facteur d'authentification sont d'utiliser SHA-256 comme fonction de hachage cryptographique, le chiffrement RSA pour la cryptographie asymétrique, et de coder le hachage avec Base64.
- Un serveur SMTP réceptionnant un email signé utilise ensuite l'identifiant de domaine responsable de la signature (SDID) et le sélecteur associé annoncés dans les en-têtes afin de récupérer la clé publique publiée dans le serveur DNS du SDID. Cette clé est utilisée pour vérifier la validité des signatures.

Se protéger contre les courriels illégitimes

DMARC : « Domain-based Message Authentication, Reporting and Conformance »

- C'est une spécification technique créée par un groupe d'organisations qui souhaite aider à réduire l'usage abusif des e-mails, tels que le spam, le phishing, en proposant une solution de déploiement et de surveillance des problèmes liés à l'authentification des e-mails.
- DMARC standardise la façon dont les destinataires (au sens des MTA destinataires) réalisent l'authentification des e-mails en utilisant les mécanismes de Sender Policy Framework et de DomainKeys Identified Mail. Cela signifie que l'expéditeur (au sens d'un MTA expéditeur) recevra les résultats de l'authentification de ses messages par tout destinataire qui implémente DMARC
- Les politiques DMARC sont publiées dans le DNS public du domaine comme enregistrement TXT et annoncent ce que le destinataire d'un email doit faire si ce dernier ne satisfait pas les mécaniques d'authentification SPF et/ou DKIM.
- DMARC va vérifier la cohérence (en mode strict et/ou relax) des trois noms de domaines suivants :
- Le nom de domaine pour DMARC est celui du champ From : de l'e-mail (après @).
- Le nom de domaine pour DKIM est celui déclaré dans la signature (champ d=).
- Le nom de domaine pour SPF est celui de la commande MAIL FROM du SMTP.