CHOUTEAU Lydéric et MAROUSE Grégoire

Compte-rendu R3.06

TD5 : Mini-projet

BUT 2 - Gr B

Décembre 2025

1. La communication est importante

1.1. Jeu de passe-passe

Question 1:

Nous avons configuré les tables de routage de chaque routeur (A à E) pour implémenter le routage en anneau. Chaque routeur transmet les paquets destinés aux réseaux qu'il ne gère pas directement vers le routeur suivant dans l'anneau (A→B→C→D→E→A). Les tables montrent les routes avec les masques de sous-réseau et les passerelles correspondantes.

ROUTEUR A :

8.8.8.0	255.255.255.0	10.0.0.2	10.0.0.1
192.168.1.0	255.255.255.0	10.0.0.2	10.0.0.1
1.1.1.0	255.255.255.0	10.0.0.2	10.0.0.1
9.9.9.0	255.255.255.0	10.0.0.2	10.0.0.1

ROUTEUR B :

8.8.8.0	255.255.255.0	10.0.1.2	10.0.1.1
1.1.1.0	255.255.255.0	10.0.1.2	10.0.1.1
9.9.9.0	255.255.255.0	10.0.1.2	10.0.1.1
192.168.0.0	255.255.255.0	10.0.1.2	10.0.1.1

ROUTEUR C :

1.1.1.0	255.255.255.0	10.0.2.2	10.0.2.1
9.9.9.0	255.255.255.0	10.0.2.2	10.0.2.1
192.168.0.0	255.255.255.0	10.0.2.2	10.0.2.1
192.168.1.0	255.255.255.0	10.0.2.2	10.0.2.1

ROUTEUR D :

IP de destination	Masque	Passerelle suivante	Via l'interface
9.9.9.0	255.255.255.0	10.0.3.2	10.0.3.1
192.168.0.0	255.255.255.0	10.0.3.2	10.0.3.1
192.168.1.0	255.255.255.0	10.0.3.2	10.0.3.1
8.8.8.0	255.255.255.0	10.0.3.2	10.0.3.1

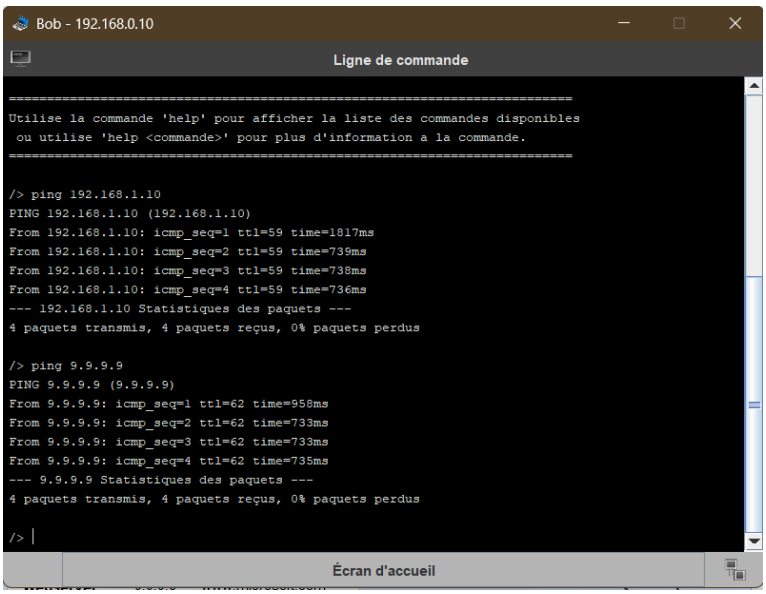
ROUTEUR E :

192.168.0.0	255.255.255.0	10.0.4.2	10.0.4.1
192.168.1.0	255.255.255.0	10.0.4.2	10.0.4.1
8.8.8.0	255.255.255.0	10.0.4.2	10.0.4.1
1.1.1.0	255.255.255.0	10.0.4.2	10.0.4.1

Question 2 :

Les tests ping depuis Bob (192.168.0.10) vers Alice (192.168.1.10) et vers le serveur Microsoft (9.9.9.9) confirment que le routage fonctionne correctement. Les paquets sont acheminés avec succès à travers le réseau Internet, validant la configuration des tables de routage.

Tests de ping :



1.2. La sécurité avant tout !

Question 3 :

L'accès aux sites web de Microsoft et Google est bloqué. Le problème provient des pare-feux des routeurs C et E qui rejettent tout le trafic entrant vers leurs réseaux respectifs, à l'exception des requêtes ICMP. L'accès par IP ou URL produit le même résultat négatif.

Question 4 :

La ligne existante dans le pare-feu bloque tout le trafic à destination du réseau (8.8.8.0 pour le routeur C et 9.9.9.0 pour le routeur E) en le rejetant. Cette règle par défaut empêche toute communication avec les serveurs du réseau protégé.

Routeur C

7			8.8.8.0	255.255.255.0	*		rejeter

Routeur E

7			9.9.9.0	255.255.255.0	*		rejeter

Question 5 :

Nous avons ajouté deux règles dans les pare-feux des routeurs C et E :

- Une règle autorisant le trafic TCP sur le port 80 (HTTP) vers les serveurs web
- Une règle autorisant le trafic UDP sur le port 53 (DNS) vers les serveurs DNS Ces règles permettent désormais la résolution de noms de domaine et l'accès aux sites web.

ROUTEUR C :

ID	IP source	Masque	IP destination	Masque	Protocole	Port	Action
1			8.8.8.8	255.255.255.0	UDP	53	accepter
2			8.8.8.7	255.255.255.0	TCP	80	accepter

ROUTEUR E :

ID	IP source	Masque	IP destination	Masque	Protocole	Port	Action
1			9.9.9.8	255.255.255.255	TCP	80	accepter
2			9.9.9.9	255.255.255.255	UDP	53	accepter

2. La poste n'est plus à jour

Question 6 :

Nous avons créé les comptes utilisateurs sur les serveurs mail :

- Sur Outlook (Microsoft) : Bob et Jessica
- Sur Gmail (Google) : Alice et Fred Chaque compte utilise le prénom comme identifiant et un mot de passe défini.

Google :

Adresse électronique	Nombre de messages
Alice@google.com	0
Fred@google.com	0

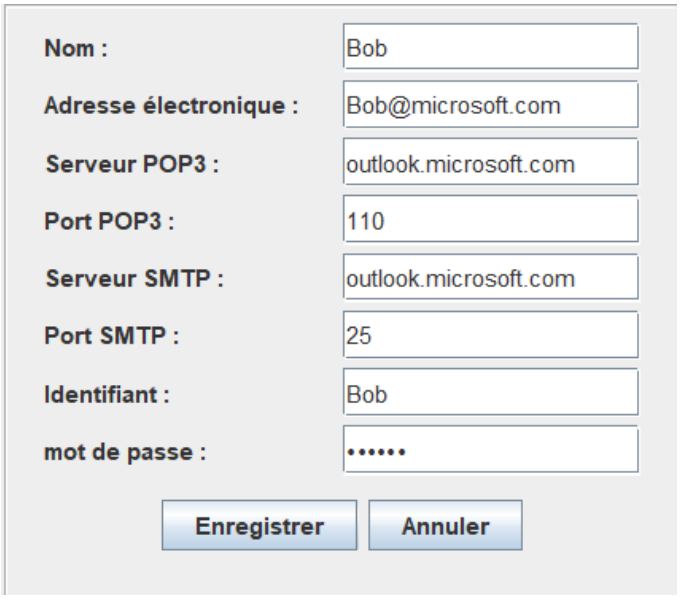
Microsoft :

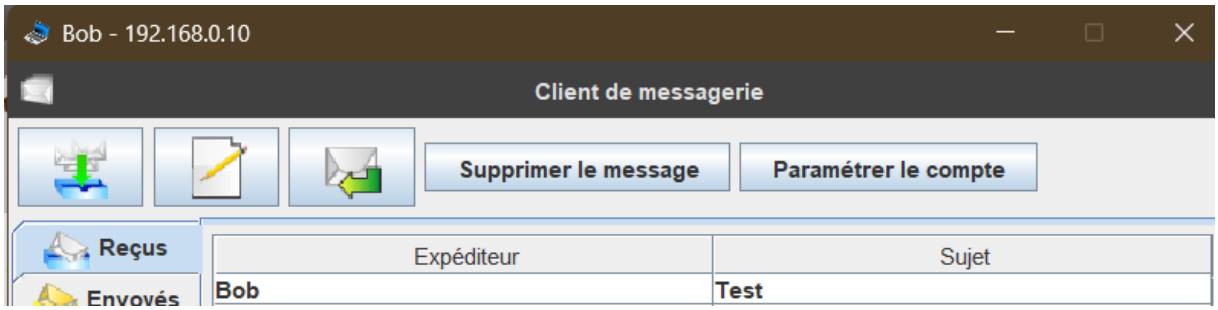
Adresse électronique	Nombre de messages
Bob@microsoft.com	0
Jessica@microsoft.com	0

Question 7 :

La configuration du client mail de Bob comprend :

- Serveur POP3 : outlook.microsoft.com (port 110)
- Serveur SMTP : outlook.microsoft.com (port 25)
- Identifiants et mot de passe correspondants Cette configuration permet de récupérer et envoyer des mails.





Question 8 :

L'erreur de connexion provenait du blocage des protocoles POP3 (port 110) et SMTP (port 25) par les pare-feux des routeurs C et E. Nous avons ajouté :

- Une règle TCP port 110 pour POP3
- Une règle TCP port 25 pour SMTP Ces modifications permettent désormais la communication entre les clients mail et les serveurs.

Routeur E

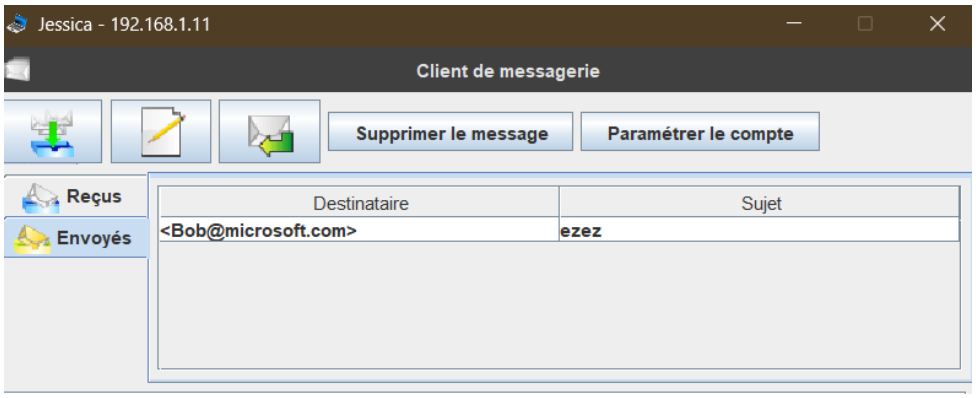
3			8.8.8.9	255.255.255.0	TCP	110	accepter
4			8.8.8.9	255.255.255.0	TCP	25	accepter

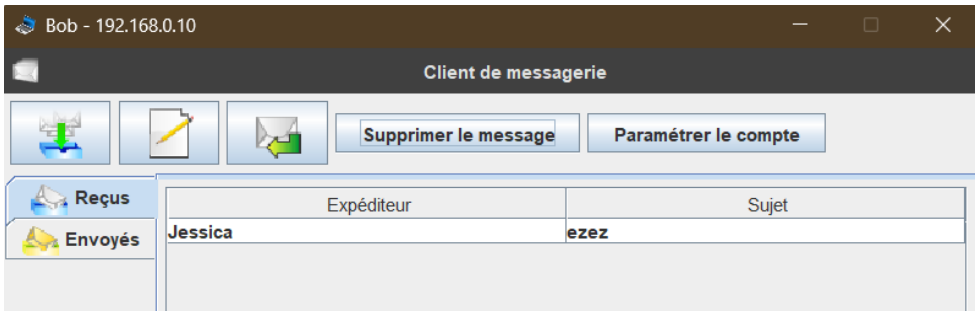
Routeur C

3			9.9.9.10	255.255.255.255	TCP	110	accepter
4			9.9.9.10	255.255.255.255	TCP	25	accepter

Question 9 :

L'observation des échanges SMTP et POP3 révèle que ces protocoles transmettent les données en clair, sans chiffrement. Les identifiants, mots de passe et contenus des messages sont visibles en texte brut, ce qui pose un risque de sécurité important en cas d'interception.





Question 10 :

L'envoi de mails entre domaines est bloqué car le serveur DNS racine (nécessaire pour résoudre les domaines externes) n'est pas autorisé à traverser les pare-feux. Nous avons ajouté :

- Une règle UDP port 53 autorisant le trafic depuis/vers le réseau externe (1.1.1.0)
- Une règle TCP port 25 pour permettre la communication SMTP entre les serveurs mail des deux domaines

Routeur C

5	8.8.8.8	255.255.255.255			UDP	53	accepter
6	8.8.8.9	255.255.255.255			TCP	25	accepter

Routeur E

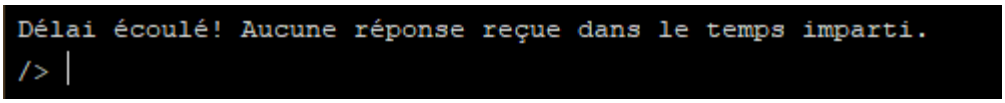
5	9.9.9.9	255.255.255.255			UDP	53	accepter
6	9.9.9.10	255.255.255.255			TCP	25	accepter

Question 11:

Le récepteur ne reçoit pas le message car le serveur émetteur ne peut pas résoudre le domaine du destinataire. La commande host gmail.google.com depuis outlook.microsoft.com échoue ("Aucune réponse reçue"), confirmant que les enregistrements DNS nécessaires sont manquants.

Depuis outlook.microsoft.com

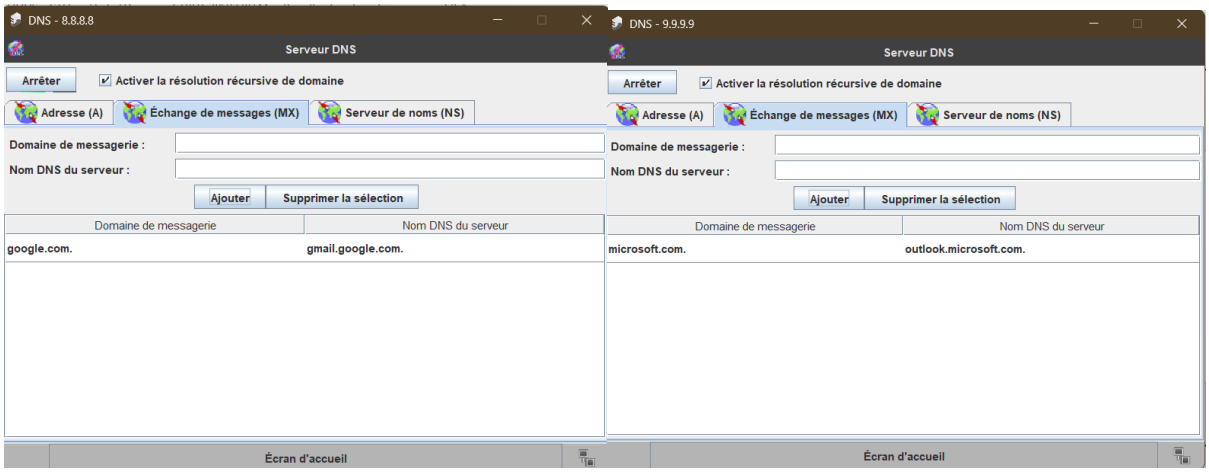
- host gmail.google.com



Question 12 :

Nous avons ajouté des enregistrements MX (Mail eXchanger) dans les serveurs DNS :

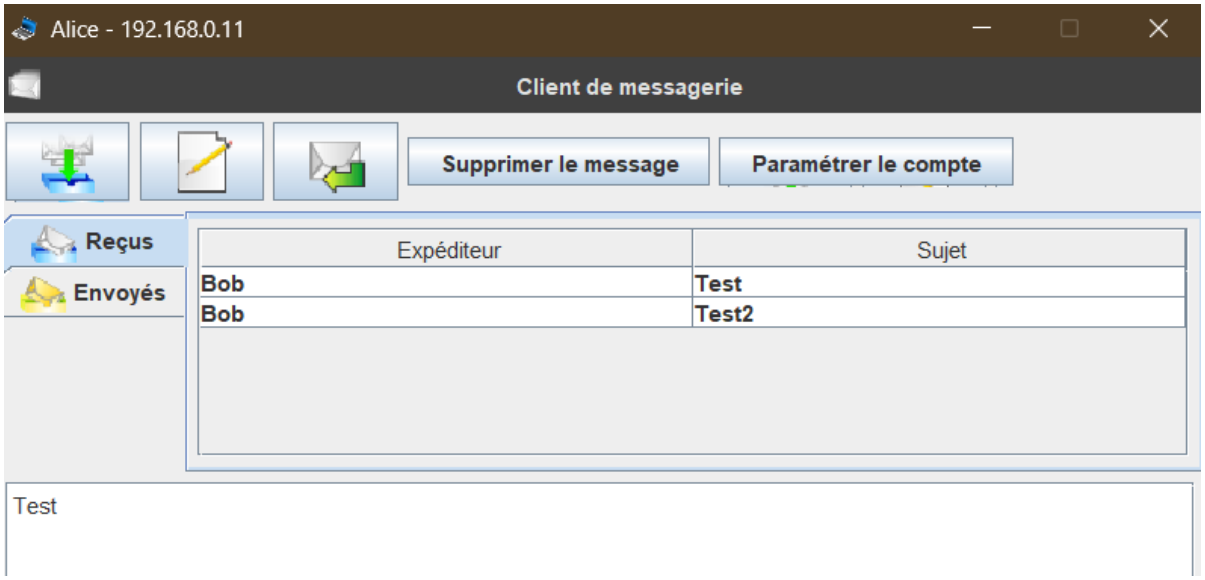
- DNS Google : MX pointant vers gmail.google.com
- DNS Microsoft : MX pointant vers outlook.microsoft.com Ces enregistrements indiquent quel serveur gère les emails pour chaque domaine. La commande host confirme maintenant la présence de ces enregistrements.



Question 13 :

Les logs montrent que SMTP fonctionne en mode relais : le serveur émetteur contacte d'abord le DNS pour obtenir l'enregistrement MX du domaine destinataire, puis établit une connexion directe avec le serveur mail correspondant pour transmettre le message.

Le protocole utilise une série de commandes (HELO, MAIL FROM, RCPT TO, DATA) pour négocier et transférer les emails.



3. Patch moi ça !

3.1. On relaie… On relaie

Question 14 :

Nous avons modifié les pare-feux des routeurs C et E pour :

- Autoriser uniquement le proxy SMTP (1.1.1.3) comme source pour le trafic SMTP entrant (port 25)
- Supprimer la règle SMTP sortante car c'est désormais le proxy qui gère la distribution La réception POP3 reste fonctionnelle car elle n'est pas affectée par ces modifications.

Routeur C :

Règle par défaut (appliquée si aucune règle de la liste n'est satisfaite) : accepter

ID	IP source	Masque	IP destination	Masque	Protocole	Port	Action
1			8.8.8.8	255.255.255.0	UDP	53	accepter
2			8.8.8.7	255.255.255.0	TCP	80	accepter
3			8.8.8.9	255.255.255.0	TCP	110	accepter
4	8.8.8.8	255.255.255.255			UDP	53	accepter
5	1.1.1.3	255.255.255.255			TCP	25	accepter
6			8.8.8.0	255.255.255.0	*		rejeter

Routeur E :

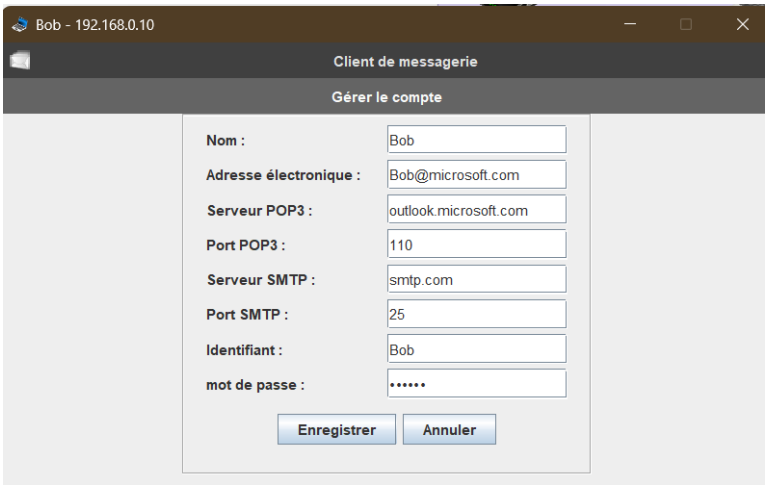
Règle par défaut (appliquée si aucune règle de la liste n'est satisfaite) : accepter

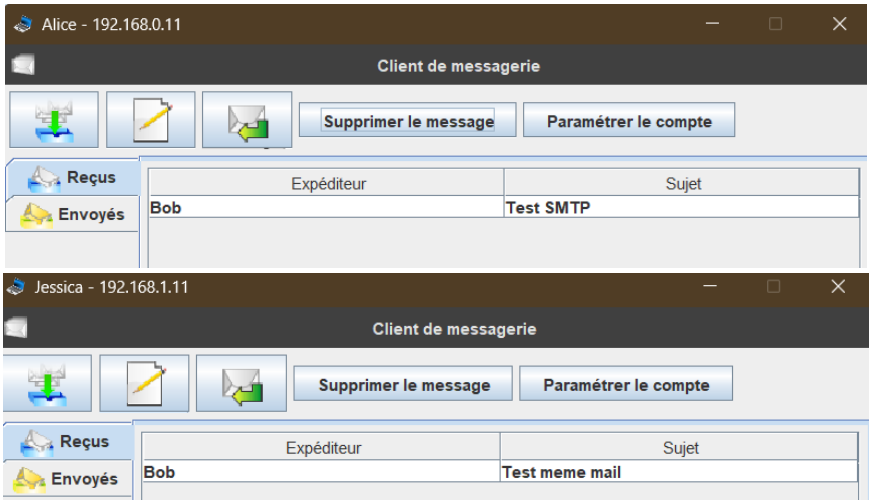
ID	IP source	Masque	IP destination	Masque	Protocole	Port	Action
1			9.9.9.8	255.255.255.255	TCP	80	accepter
2			9.9.9.9	255.255.255.255	UDP	53	accepter
3			9.9.9.10	255.255.255.255	TCP	110	accepter
4	9.9.9.9	255.255.255.255			UDP	53	accepter
5	1.1.1.3	255.255.255.255			TCP	25	accepter
6			9.9.9.0	255.255.255.0	*		rejeter

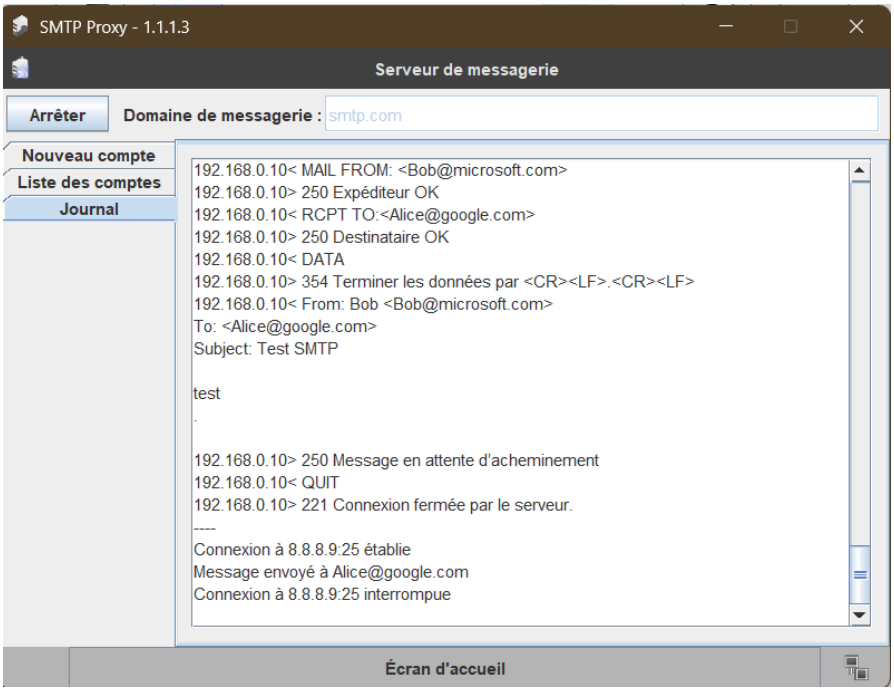
Question 15 :

Nous avons reconfiguré tous les clients mail pour utiliser smtp.com comme serveur SMTP au lieu des serveurs directs. Les logs montrent que :

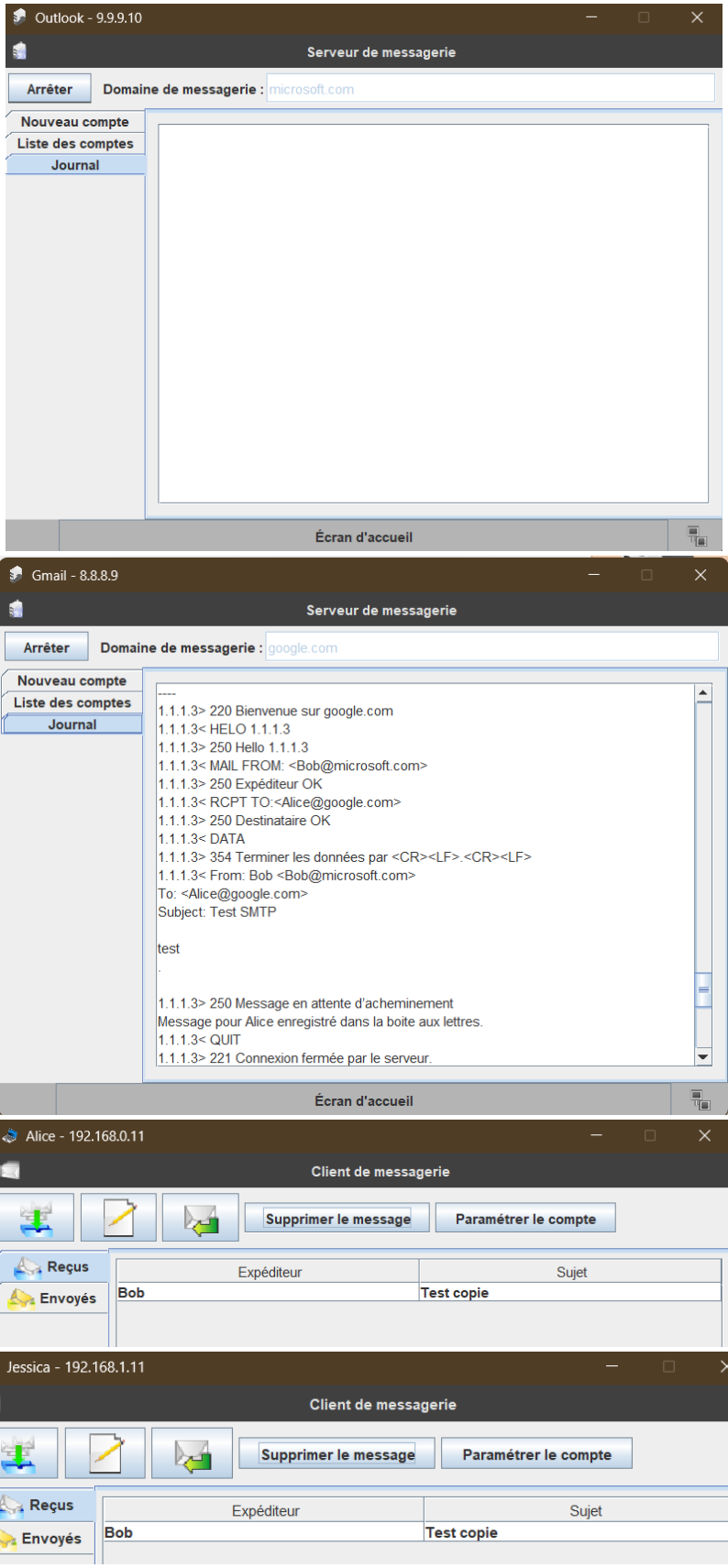
- Le client envoie au proxy (1.1.1.3)
- Le proxy achemine vers le serveur de destination approprié (Outlook ou Gmail)
- Le système gère correctement les destinataires multiples (champs cc) Cette architecture centralisée améliore la sécurité et le contrôle du trafic mail.


Bob - 192.168.0.10
Client de messagerie
Gérer le compte
Nom :
Bob
Adresse électronique :
Bob@microsoft.com
Serveur POP3 :
outlook.microsoft.com
Port POP3 :
110
Serveur SMTP :
smtp.com
Port SMTP :
25
Identifiant :
Bob
mot de passe :
Enregistrer
Annuler


Alice - 192.168.0.11
Client de messagerie
Supprimer le message
Paramétrer le compte
Reçus
Envoyés
Expéditeur
Sujet
Bob
Test SMTP
Jessica - 192.168.1.11
Client de messagerie
Supprimer le message
Paramétrer le compte
Reçus
Envoyés
Expéditeur
Sujet
Bob
Test meme mail


SMTP Proxy - 1.1.1.3
Serveur de messagerie
Arrêter
Domaine de messagerie :
smtp.com
Nouveau compte
Liste des comptes
Journal
192.168.0.10< MAIL FROM: <Bob@microsoft.com>
192.168.0.10> 250 Expéditeur OK
192.168.0.10< RCPT TO:<Alice@google.com>
192.168.0.10> 250 Destinataire OK
192.168.0.10< DATA
192.168.0.10> 354 Terminer les données par <CR><LF>.<CR><LF>
192.168.0.10< From: Bob <Bob@microsoft.com>
To: <Alice@google.com>
Subject: Test SMTP
test
.
192.168.0.10> 250 Message en attente d'acheminement
192.168.0.10< QUIT
192.168.0.10> 221 Connexion fermée par le serveur.

Connexion à 8.8.8.9:25 établie
Message envoyé à Alice@google.com
Connexion à 8.8.8.9:25 interrompue
Écran d'accueil


Outlook - 9.9.9.10
Serveur de messagerie
Arrêter
Domaine de messagerie : microsoft.com
Nouveau compte
Liste des comptes
Journal
Écran d'accueil
Gmail - 8.8.8.9
Serveur de messagerie
Arrêter
Domaine de messagerie : google.com
Nouveau compte
Liste des comptes
Journal

1.1.1.3> 220 Bienvenue sur google.com
1.1.1.3< HELO 1.1.1.3
1.1.1.3> 250 Hello 1.1.1.3
1.1.1.3< MAIL FROM: <Bob@microsoft.com>
1.1.1.3> 250 Expéditeur OK
1.1.1.3< RCPT TO:<Alice@google.com>
1.1.1.3> 250 Destinataire OK
1.1.1.3< DATA
1.1.1.3> 354 Terminer les données par <CR><LF>.<CR><LF>
1.1.1.3< From: Bob <Bob@microsoft.com>
To: <Alice@google.com>
Subject: Test SMTP
test
.
1.1.1.3> 250 Message en attente d'acheminement
Message pour Alice enregistré dans la boite aux lettres.
1.1.1.3< QUIT
1.1.1.3> 221 Connexion fermée par le serveur.
Écran d'accueil
Alice - 192.168.0.11
Client de messagerie
Supprimer le message
Paramétrer le compte
Reçus
Envoyés
Expéditeur
Sujet
Bob
Test copie
Jessica - 192.168.1.11
Client de messagerie
Supprimer le message
Paramétrer le compte
Reçus
Envoyés
Expéditeur
Sujet
Bob
Test copie

3.2. Filtrons, filtrons

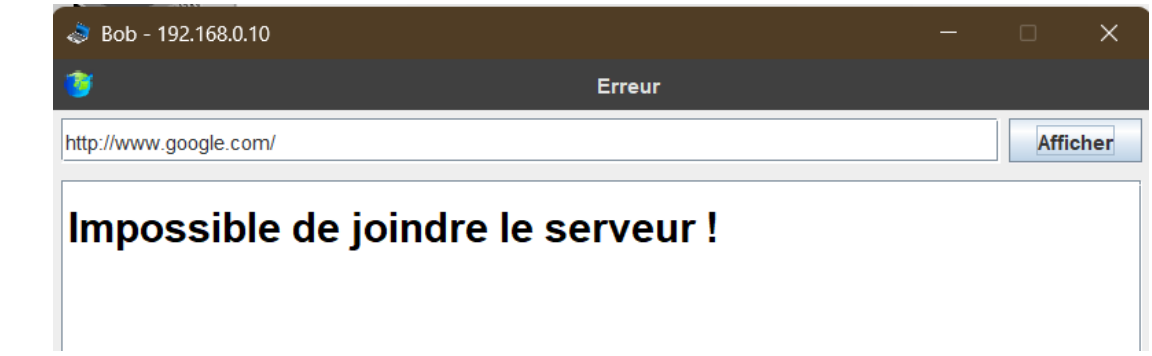
Question 16 :

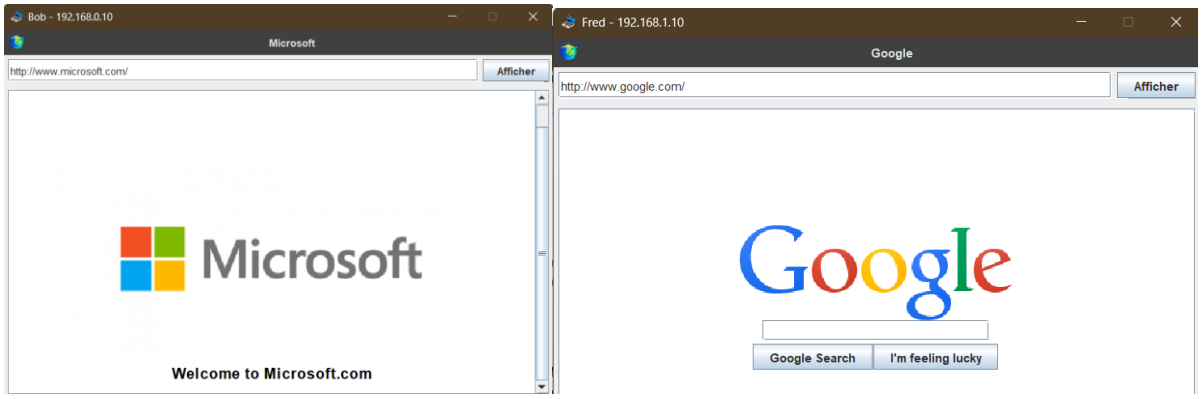
Nous avons implémenté un filtrage géographique en modifiant les règles HTTP des routeurs C et E :

- Routeur E : autoriser uniquement le réseau 192.168.0.0 (Privé A) vers Microsoft (9.9.9.8)
- Routeur C : autoriser uniquement le réseau 192.168.1.0 (Privé B) vers Google (8.8.8.7) Les tests confirment que Bob accède uniquement à Microsoft et Fred uniquement à Google.

ID	IP source	Masque	IP destination	Masque	Protocole	Port	Action
1	192.168.0.0	255.255.255.0	9.9.9.8	255.255.255.255	TCP	80	accepter

ID	IP source	Masque	IP destination	Masque	Protocole	Port	Action
1	192.168.1.0	255.255.255.0	8.8.8.7	255.255.255.0	TCP	80	accepter

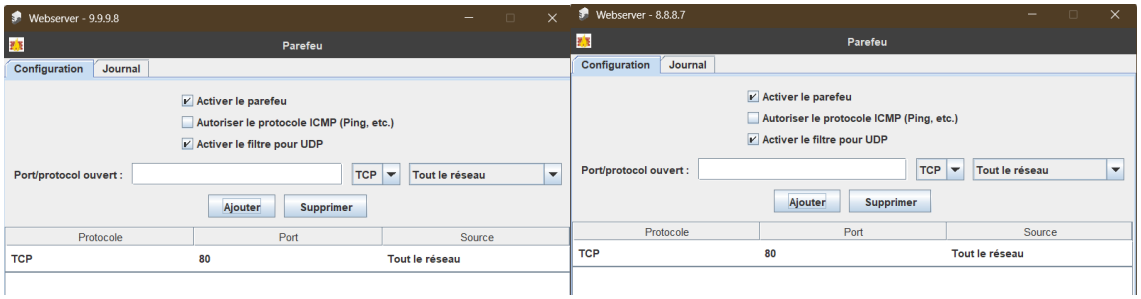


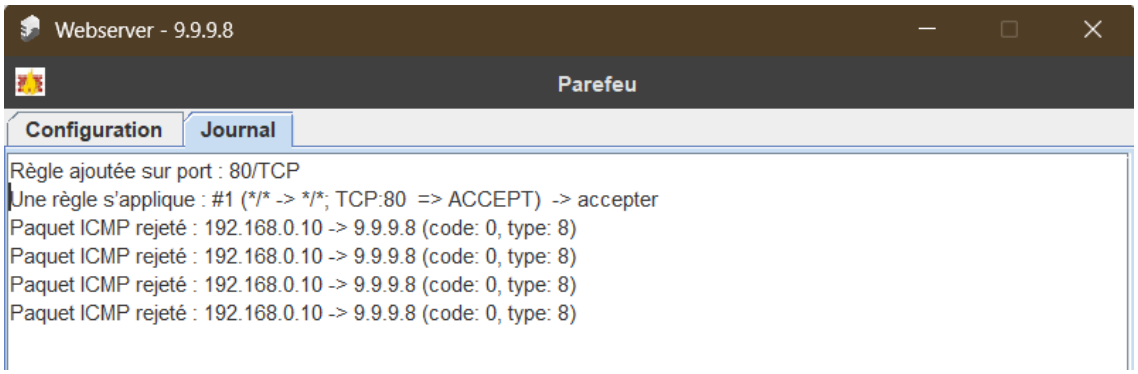


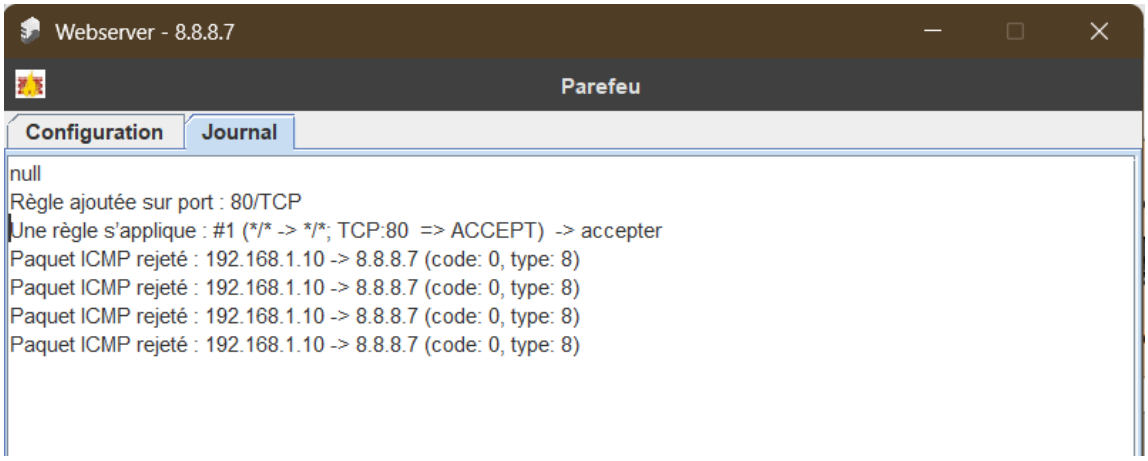
Question 17 :

Nous avons activé les pare-feux sur les serveurs web Microsoft et Google avec :

- Désactivation des réponses ICMP pour améliorer la sécurité
- Ouverture du port TCP 80 pour autoriser le trafic HTTP Les logs des pare-feux confirment que les connexions HTTP sont acceptées tandis que les requêtes ICMP sont bloquées.





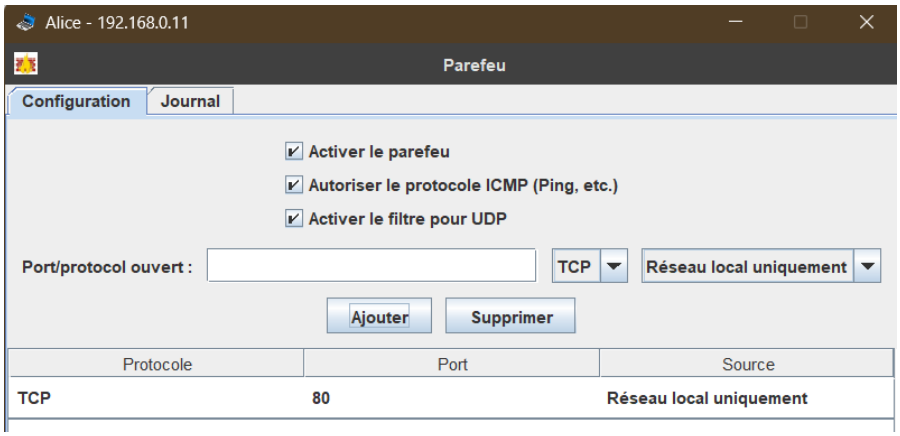


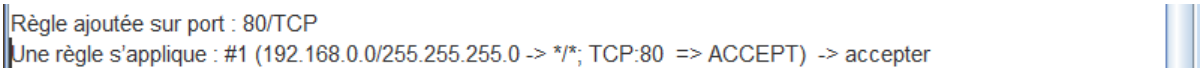
Question 18 :

Nous avons sécurisé les serveurs web personnels d'Alice et Fred en configurant leurs pare-feux pour :

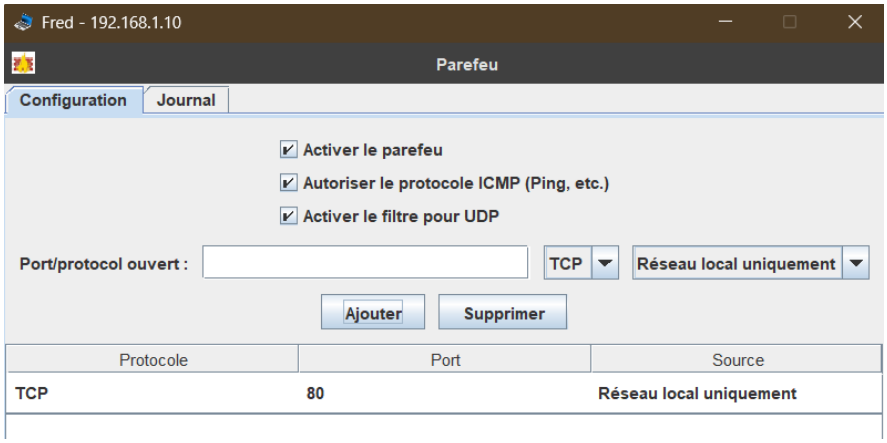
- Autoriser le trafic HTTP (port 80) uniquement depuis le réseau local
- Alice : accessible uniquement depuis le réseau 192.168.0.0 (Bob peut accéder)
- Fred : accessible uniquement depuis le réseau 192.168.1.0 (Jessica peut accéder)
- ICMP reste activé pour les tests réseau. Les logs confirment que les accès externes sont bloqués.

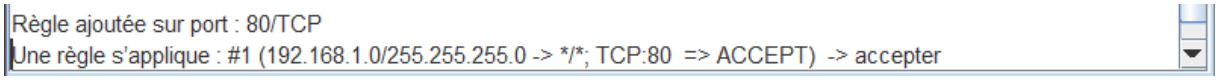
Pour Alice :





Pour Fred :





4. Et on fait tourner le routage…

Question 19 :

Le routage en anneau pose un problème : lorsqu'un paquet est envoyé vers une adresse inexistante, il devrait théoriquement tourner indéfiniment dans l'anneau. Le champ TTL (Time To Live) dans l'en-tête IP empêche cette boucle infinie en décrémentant à chaque saut et en détruisant le paquet quand il atteint 0. Dans notre configuration, le problème est évité car nous avons renseigné tous les réseaux explicitement dès le début mais sinon cela donnerait :

```
/> traceroute 3.4.5.6
Établissement de la connexion avec 3.4.5.6 (en 20 sauts max.).
 1    192.168.0.1
 2    10.0.1.1
 3    10.0.2.1
 4    10.0.3.1
 5    10.0.4.1
 6    192.168.0.1
 7    10.0.1.1
 8    10.0.2.1
 9    10.0.3.1
 10    10.0.4.1
 11    192.168.0.1
 12    10.0.1.1
 13    10.0.2.1
 14
```

Question 20 :

EXEMPLES DE TABLE SUR DEUX ROUTEURS :

ROUTEUR A :

IP Destination	Masque réseau	Passerelle suivante	Via l'interface
192.168.0.0	255.255.255.0	*	192.168.0.1
192.168.1.0	255.255.255.0	10.0.4.1	10.0.4.2
8.8.8.0	255.255.255.0	10.0.4.1	10.0.4.2
9.9.9.0	255.255.255.0	10.0.0.1	10.0.0.2
1.1.1.0	255.255.255.0	10.0.0.1	10.0.0.2
0.0.0.0	0.0.0.0	*	*

ROUTEUR C :

IP Destination	Masque réseau	Passerelle suivante	Via l'interface
8.8.8.0	255.255.255.0	*	8.8.8.1
192.168.1.0	255.255.255.0	10.0.1.1	10.0.1.2
192.168.0.0	255.255.255.0	10.0.1.1	10.0.1.2
1.1.1.0	255.255.255.0	10.0.2.1	10.0.2.2
9.9.9.0	255.255.255.0	10.0.2.1	10.0.2.2
0.0.0.0	0.0.0.0	*	*

Cette nouvelle méthode de routage optimise les chemins en choisissant la direction la plus courte pour atteindre chaque réseau. Au lieu de faire systématiquement tourner tous les paquets dans le même sens, chaque routeur sélectionne le voisin (horaire ou antihoraire) qui permet d'atteindre la destination avec le moins de sauts possibles. En réalité, nous avions déjà mis en place une partie de cette solution dès la Question 1, en renseignant manuellement chaque réseau dans les tables de routage.

Exemple pour le Routeur A :

- Pour atteindre le réseau Google (8.8.8.0), il passe par le Routeur B (2 sauts) plutôt que par E-D-C (3 sauts)
- Pour atteindre le réseau Microsoft (9.9.9.0), il passe par le Routeur E (1 saut) plutôt que par B-C-D-E (4 sauts)

La dernière ligne de chaque table (0.0.0.0 0.0.0.0 * *) est une route par défaut qui rejette tous les paquets dont la destination ne correspond à aucune route connue. Cela empêche les paquets destinés à des adresses inexistantes (comme 3.4.5.6) de tourner indéfiniment dans l'anneau. Sans cette route par défaut, un paquet inconnu serait transmis au routeur suivant, créant une boucle infinie jusqu'à l'expiration du TTL. Cette méthode améliore la sécurité et réduit la charge réseau inutile.