Réalisé par : Mikkel Almonte-Ringaud - Michel Wang - Antoine Berteloot
Sasha Coulombel - Maxime Chagnon

Rapport - SAé S4.01B : Réseaux

INFORMATIONS COMPLÉMENTAIRES

2e année de BUT Informatique

ENCADRANTS : MARIA CRISTINA ONETE - THOMAS HUGEL

DATE DE RENDU : 29 MARS 2025

Université de Limoges

Sommaire

1. Introduction

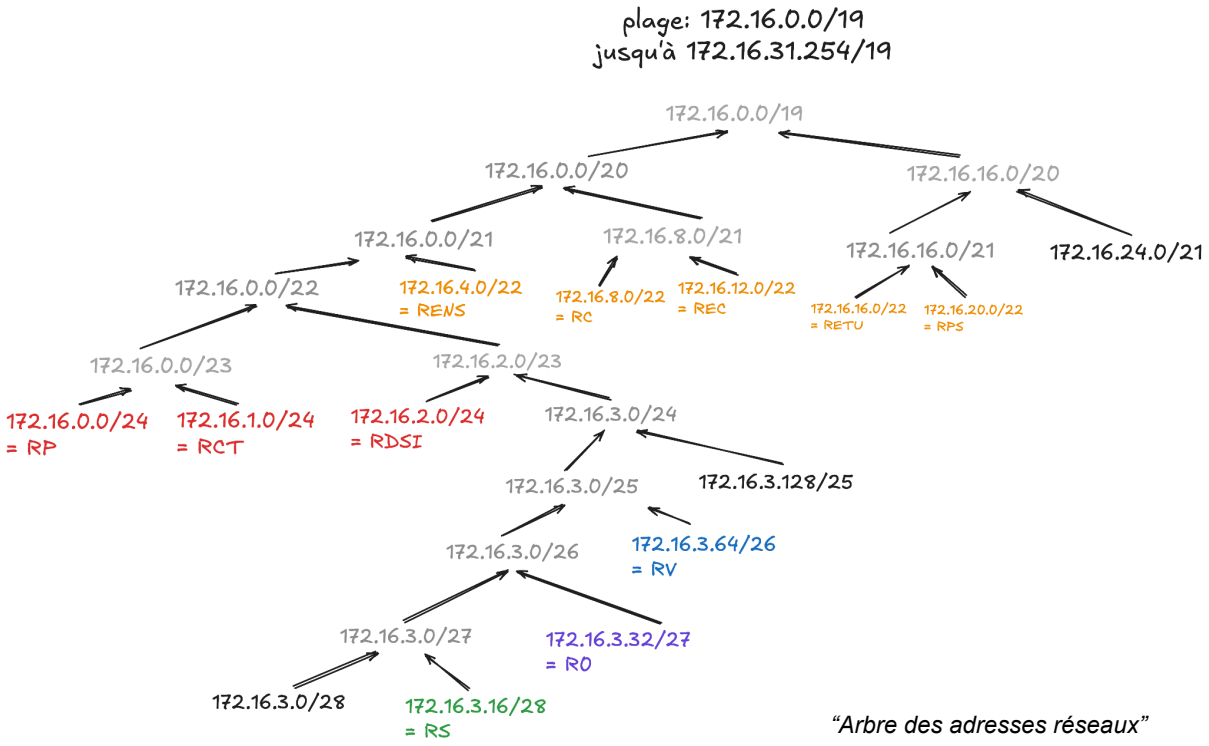
Ce rapport concerne la SAÉ 4.01B ayant pour objectif de renforcer la sécurité du réseau du Centre Hospitalier Universitaire (CHU).

À la suite de la SAÉ 3.01B, nous étendons ici l’architecture réseau en introduisant explicitement une zone démilitarisée et en segmentant l’accès internet en trois routeurs distincts selon la priorité d'accès.

De plus nous accorderons une grande importance à la sécurisation stricte des accès, en particulier via une configuration distante par la DSI, ainsi qu'à la réalisation et à l'automatisation de tests pour assurer l'efficacité du filtrage réalisé.

2. Analyse de la topologie et classification des priorités

Topologie existante (SAÉ 3.01B)



"Arbre des adresses réseaux"

Classification actualisée des priorités d'accès (SAÉ 4.01B)

Afin d'éviter cette vulnérabilité, nous avons segmenté l'accès Internet via trois routeurs distincts selon les priorités suivantes :

Sous-Réseau	Priorité d'accès
Serveurs critiques : (S, DNS, MAIL, AUX, BDD) Réseau : DSI, S	Infrastructure **critique** et de **haute priorité**
Réseau : Chercheurs, Enseignants Chercheurs, Enseignants, Étudiants,	Accès éducatif/universitaire (**priorité moyenne**)
Réseau : Comptabilité, Patients, Personnel Soignants, Visiteurs	Accès à **basse priorité**

Cette nouvelle configuration élimine le point unique de défaillance initialement présent.

3. Accès strictement nécessaires

Tableau des accès

À partir de la nouvelle topologie réseau définie précédemment , nous reprenons les accès définis dans la SAé 3.01B, tout en intégrant les nouvelles contraintes de la SAÉ 4.01B.

Réseau	Accès autorisés (protocoles & ports exacts)
Patients & Visiteurs	Accès au **serveur S** pour consultation du site public uniquement en HTTPS (TCP/443). Accès à **Internet via DNS** (UDP/53), HTTP(S) à travers le routeur à basse priorité.
Étudiants & Enseignants	Accès au **serveur MAIL** pour la **messagerie** (SMTP/25, IMAP/143, …). Accès au **serveur S** (**site public** & **intranet** en HTTPS 443). Accès à Internet (DNS 53, HTTP(S)) via le routeur éducatif. Configuration distante sécurisée par la DSI (SSH 22).
Chercheurs & Enseignants-chercheurs	Accès **serveur MAIL** (SMTP/25, IMAP/143. …). Accès **serveur S**, site public & intranet (HTTPS 443). Accès sécurisé **BDD** (SFTP TCP/22). Accès à **Internet** (DNS 53, HTTP(S)) via le routeur éducatif. Configuration distante sécurisée par la DSI (SSH 22)
Personnel soignant	Accès **serveur MAIL** (SMTP/25, IMAP/143, …). Accès **serveur S** : site public/intranet (HTTPS 443) + application gestion RDV (TCP/1224 corrigé). Accès **Internet** (DNS 53, HTTP(S)) via routeur critique. Configuration distante sécurisée par la DSI (SSH 22).
Comptabilité	Accès **serveur MAIL** (SMTP/25, IMAP/143, …). Accès **serveur S** : site public uniquement (HTTPS 443) + application gestion RDV (TCP/1224). Accès **Internet** (DNS 53, HTTP(S)) via routeur critique. Configuration distante sécurisée par la DSI (SSH 22).
DSI	Accès à **ICMP** (ping) sur toutes les machines. Accès à **tous les services sauf la BDD**. Accès à **Internet** (DNS 53, HTTP(S)) via routeur critique.
RSSI	Accès **complet DSI**. Accès **total à la BDD** (MySQL 3306/TCP).

Résumé des ajouts

- Séparation de l'accès internet en 3 routeurs distincts selon les priorités
- Une Zone Démilitarisée pour les serveurs sensibles

4. Filtrage implémenté sous Kathará

Nous avons traduit ces analyses en règles **iptables** strictes sur Kathará. Par exemple, sur le routeur des enseignants chercheurs, on vérifie la source et la destination pour les mails.

```
45  # ------------------------------------------------------------------------------
46
47  # SMTP
48  iptables -A FORWARD -s $THIS_NET -d $MAIL_SERVER -p tcp --dport 25 -j ACCEPT
49
50  # SUBMISSION
51  iptables -A FORWARD -s $THIS_NET -d $MAIL_SERVER -p tcp --dport 587 -j ACCEPT
52
53  # SMTPS
54  iptables -A FORWARD -s $THIS_NET -d $MAIL_SERVER -p tcp --dport 465 -j ACCEPT
55
56  # IMAP
57  iptables -A FORWARD -s $THIS_NET -d $MAIL_SERVER -p tcp --dport 143 -j ACCEPT
58
59  # IMAPS
60  iptables -A FORWARD -s $THIS_NET -d $MAIL_SERVER -p tcp --dport 993 -j ACCEPT
61
62  # POP3
63  iptables -A FORWARD -s $THIS_NET -d $MAIL_SERVER -p tcp --dport 110 -j ACCEPT
64
65  # POP3S
66  iptables -A FORWARD -s $THIS_NET -d $MAIL_SERVER -p tcp --dport 995 -j ACCEPT
67
68  # ------------------------------------------------------------------------------
69
70  # SFTP
71  iptables -A FORWARD -s $THIS_NET -d $DB_SERVER -p tcp --dport 22 -j ACCEPT
72
```

On drop toutes les connexions possibles et on vient ajouter les accès petit à petit.

```
15
16  iptables -P FORWARD DROP
17  iptables -P OUTPUT DROP
18  iptables -P INPUT DROP
19
```

```
24
25  # ------------------------------------------------------------------------------
26
27  # PING (ICMP)
28  iptables -A FORWARD -s $DSI_NET -p icmp --icmp-type echo-request -j ACCEPT
29  iptables -A FORWARD -s $DSI_NET -p icmp --icmp-type echo-reply -j ACCEPT
30
31  # DNS
32  iptables -A FORWARD -s $THIS_NET -d $DNS_SERVER -p udp --dport 53 -j ACCEPT
33
34  # ------------------------------------------------------------------------------
35
36  # HTTP
37  iptables -A FORWARD -s $THIS_NET -p tcp --dport 80 -j ACCEPT
38
39  # HTTPS
40  iptables -A FORWARD -s $THIS_NET -p tcp --dport 443 -j ACCEPT
41
```

Ces règles assurent un contrôle précis et renforcent la sécurité conformément à l'analyse effectuée.

5. Identification des cas de test des filtrages

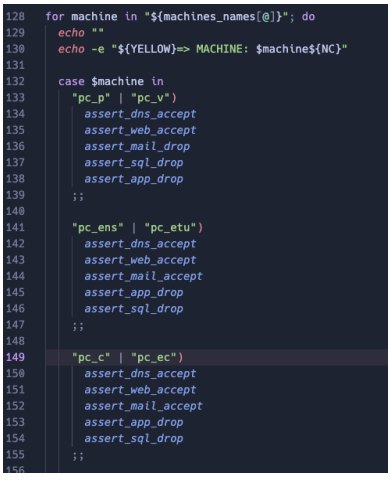
Nous avons identifié précisément les cas de tests suivants pour vérifier l'efficacité du filtrage mis en place :

Cas de test	Résultat attendu
Accès aux mails sur le réseau Personnel Soignants et Comptabilité	Autorisé
Accès à la base de données sur le réseau Personal Soignants	Interdire
Accès aux mails sur le réseau visiteur ou patients	Interdire
Accès aux ping sur toutes les machines en dehors du réseau DSI	Autorisé
Accès au site web infra depuis le réseau Chercheurs et Enseignants Chercheurs	Interdire

Ces cas couvrent quelques règles critiques de sécurité que nous avons implémentées.

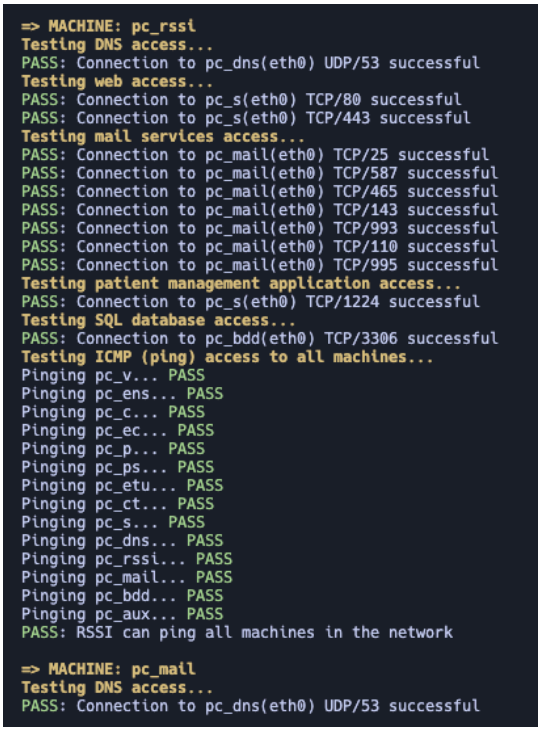
6. Implémentation de tests automatisés

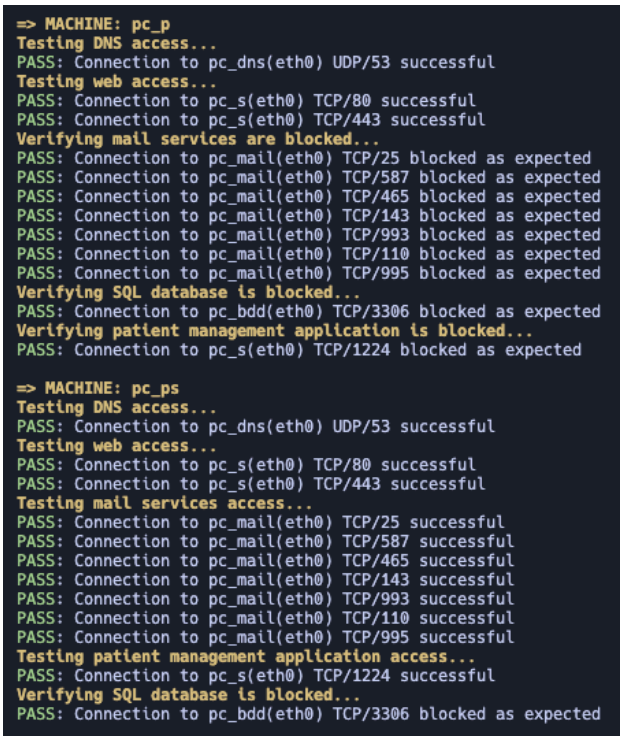
Pour automatiser les vérifications régulières de nos règles de sécurité, nous avons créé un script simple. Par exemple, …



Pour chaque machine, on définit ses assertions.

L'exécution régulière de ce script garantit la conformité permanente des règles définies et une détection rapide d'éventuelles anomalies.





7. Comparaison avec SAÉ 3.01B

Le tableau suivant résume les modifications effectuées entre la SAÉ 3.01B et la SAÉ 4.01B, en précisant leurs impacts directs sur la sécurité globale de l'infrastructure réseau du CHU :

Critère	SAÉ 3.01B	SAÉ 4.01B	Impact sur la sécurité
Séparation du routage vers Internet	Un **seul routeur commun (R0)**, représentant un risque majeur de point unique de défaillance.	Séparation en t**rois routeurs distincts** selon la priorité d'accès : infrastructure critique (**haute**), éducative/universitaire (**moyenne**), non prioritaire (**basse**).	Supprime le risque lié à un **point unique de défaillance** Renforce la disponibilité et la résilience globale.
Normes et bonnes pratiques de **sécurité**	Application générale des bonnes pratiques de **sécurité sans contrainte spécifique** détaillée.	Application explicitement renforcée des **normes de sécurité** et **bonnes pratiques architecturales par segmentation** claire (**Zone dématérialisée** explicite).	Sécurité accrue, renforcement structurel contre les attaques.
Tests **automatisés** de sécurité	**Non exigées** explicitement, la vérification de l'efficacité du filtrage était principalement **manuelle**.	Exigence explicite de **scripts automatisés** vérifiant régulièrement et automatiquement la conformité stricte des règles de filtrage définies.	Garantit une sécurité continue et permanente. Détection rapide d'anomalies ou d'erreurs éventuelles dans les configurations.

8. Conclusion

Cette SAÉ4.01B a permis de renforcer efficacement la sécurité réseau du CHU en éliminant le risque de point unique de défaillance grâce à la segmentation claire en trois routeurs distincts.

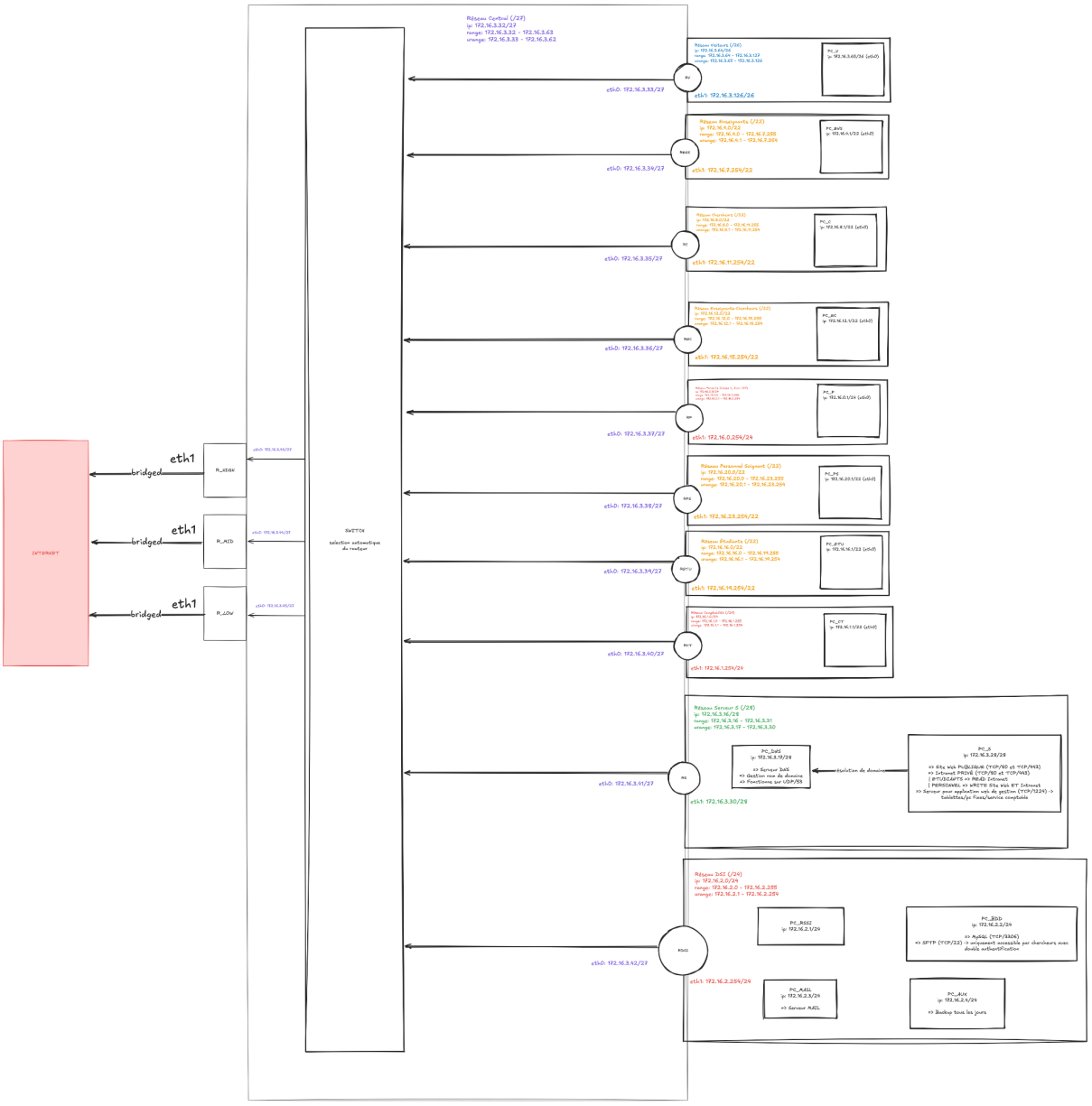
L'introduction d'une zone démilitarisée explicite et d'autres améliorent nettement la protection des ressources sensibles.

Enfin, l'automatisation des tests garantit un contrôle automatisé et fiable des configurations, assurant donc ainsi la sécurité.

9. Schéma à part

Figures de notre votre infrastructure

Disponible en taille d'origine sur le GitHub de la SAE :
https://raw.githubusercontent.com/Vexcited/IUT-SAE4.01B/refs/heads/main/infrastructure.png



"Schéma de la nouvelle infrastructure réseau"

Figures des accès strictement nécessaires que notre filtrage doit permettre

```
"pc_p" | "pc_v")
  assert_dns_accept
  assert_web_accept
  assert_mail_drop
  assert_sql_drop
  assert_app_drop
;;
```

```
"pc_ens" | "pc_etu")
  assert_dns_accept
  assert_web_accept
  assert_mail_accept
  assert_app_drop
  assert_sql_drop
;;
```

```
"pc_c" | "pc_ec")
  assert_dns_accept
  assert_web_accept
  assert_mail_accept
  assert_app_drop
  assert_sql_drop
;;
```

```
"pc_ps" | "pc_ct")
  assert_dns_accept
  assert_web_accept
  assert_mail_accept
  assert_app_accept
  assert_sql_drop
;;
```

```
"pc_s")
  assert_dns_accept
  assert_mail_drop
  assert_sql_accept
;;
```

```
"pc_rssi")
  assert_dns_accept
  assert_web_accept
  assert_mail_accept
  assert_app_accept
  assert_sql_accept
```

Le PC RSSI a notamment le droit de ping toutes les machines sur tous les réseaux.