11/03/2025

TP PARE-FEU PROXY

BTS SIO SISR 2e année

Anne-Lou DELAGE-DAVIES

Kyllian AUCHER

Table des matières

Toutes les questions du doc :

- *Configurez la route par défaut qui est 192.168.30.254 (c'est l'adresse de routeur). Pourquoi faut-il renseigner la route par défaut ?*

La route par défaut permet d'indiquer au pare-feu vers quel routeur envoyer les paquets destinés à des réseaux non connus. Sans cette route, les paquets destinés à Internet ou à des réseaux externes ne pourraient pas être acheminés correctement.

- *Que fait la règle de filtrage 10 par défaut ? Le poste étudiant peut-il accéder au poste serveur sur n'importe quel port ? Les postes serveurs et étudiants ont-ils accès à internet ? Les postes d'internet ont-ils accès aux postes étudiants et serveurs ?*

Que fait cette règle par défaut ?

Généralement, la règle 10 (ou 9 sur une version précédente) est une règle implicite de refus total. Elle bloque tout le trafic qui n'a pas été explicitement autorisé par les règles précédentes.

Le poste étudiant peut-il accéder au poste serveur sur n'importe quel port ?

Non, sauf si une règle spécifique autorise cet accès sur des ports définis. Par défaut, un pare-feu bien configuré bloque ces communications inter-segments.

Les postes serveurs et étudiants ont-ils accès à Internet ?

Cela dépend des règles mises en place. S'il n'y a pas de règle explicite autorisant l'accès à Internet (HTTP, HTTPS, DNS, etc.), alors l'accès sera bloqué.

Les postes d'Internet ont-ils accès aux postes étudiants et serveurs ?

Par défaut, non. Un pare-feu est configuré pour refuser tout trafic entrant non sollicité afin de protéger le réseau interne.

- *Que fait cette ligne ? Pourquoi faut-il la mettre ? Est-ce préconisé par l'ANSSI ?*

Cette ligne est essentielle pour empêcher les connexions non sécurisées et éviter les risques liés aux flux non contrôlés.

L'ANSSI recommande généralement de mettre une règle de blocage explicite en fin de politique de filtrage pour assurer une protection complète du réseau.

- *Quelles différences entre QoS de réservation et de débits ? Quels intérêts de mettre en place ces 2 QoS ?*

QoS de réservation (ex: 10 Mb/s pour les serveurs) : garantit un minimum de bande passante pour un type de trafic ou un segment réseau, même en cas de forte charge.

QoS de débit (ex: 8 Mb/s max pour les étudiants) : limite la bande passante disponible pour éviter une surconsommation et préserver le bon fonctionnement du réseau.

Intérêt de ces deux QoS :

La réservation permet de garantir un service stable pour les applications critiques comme les serveurs.

La limitation empêche un réseau (ex: étudiants) de monopoliser la bande passante.

- *Depuis votre poste étudiant, que se passe t'il si vous accédez à https:// www.google.com ? Comment se fait-il que vous n'y accédiez pas alors que vous avez bloqué que les sites de banques en HTTPS ?*

On ne peut pas y accéder car la communication est déchiffrée or Google nécessite un certificat reconnu, il faudrait alors installer le certificat du pare-feu directement sur chaque poste localement afin que le navigateur le reconnaisse.

- *Depuis votre poste étudiant, que se passe t'il si vous accédez à https:// www.google.com ? Que se passe t'il si vous accédez à https://home.barclays ? Est- ce le résultat attendu ?*

On peut désormais y accéder car il n'y a pas de déchiffrage donc le certificat est reconnu. On ne peut cependant pas accéder au site de banque puisque celui-ci a été bloqué.

- *Que préconise l'ANSSI au sujet de la dernière règle ? Si vous respectez cette préconisation, est-il nécessaire d'avoir rajouté la règle précédente bloquez le flux du réseau étudiant de l'autre site vers votre réseau étudiant ? Pourquoi ? Faites valider. Que se passe t'il si vous enlevez la passerelle sur vos stations ? Que se passe t'il si vous enlevez les routes sur les pares-feux ?*

L'ANSSI recommande généralement une politique de refus par défaut avec des exceptions définies.

Si cette politique est suivie, la règle bloquant les flux étudiants vers leur propre réseau peut devenir redondante, car elle serait déjà implicitement interdite.

Sans passerelle sur les stations → Aucune communication avec d'autres sous-réseaux ni Internet.

Sans routes sur les pares-feux → Les paquets ne pourront pas être routés vers les autres réseaux, bloquant les connexions inter-labos.

- *Est-il envisageable d'autoriser telnet ? Pourquoi ?*

Non, Telnet est un protocole non sécurisé car il transmet les identifiants en clair. Il est préférable d'utiliser SSH, qui chiffre les communications.

L'ANSSI déconseille fortement l'utilisation de Telnet en raison de ses failles de sécurité.

1. Introduction

Ce TP a pour objectif de mettre en place un pare-feu et un proxy afin de contrôler et sécuriser les flux réseaux selon les recommandations de l'ANSSI. Pour cela, nous allons configurer un pare-feu Stormshield en appliquant des règles de filtrage avancées permettant de contrôler l'accès aux ressources du réseau, limiter les menaces extérieures et optimiser les performances.

Nous nous concentrerons sur la mise en place de la qualité de service (QoS), la définition des stratégies de filtrage et l'application de restrictions d'accès pour les différents utilisateurs du réseau. L'objectif est d'acquérir une compréhension approfondie de la gestion des flux réseau et de la sécurité informatique.

2. Objectif

Configurer un pare-feu en respectant les bonnes pratiques de sécurité afin de protéger le réseau contre les cyberattaques et les intrusions.

Mettre en place une stratégie de filtrage des accès en fonction des utilisateurs et des services autorisés.

Implémenter des règles de QoS pour garantir une distribution équilibrée de la bande passante et améliorer les performances du réseau.

Restreindre l'accès à certains sites web grâce au filtrage URL et SSL afin d'éviter l'utilisation inappropriée des ressources Internet.

Assurer la connectivité entre différents laboratoires tout en appliquant des contrôles stricts sur les flux de données autorisés.

3. Matériel et logiciels utilisés

Matériel :

- Pare-feu Stormshield, assurant la protection et le filtrage du réseau.
- Poste administrateur, utilisé pour configurer et superviser le pare-feu.
- Poste étudiant, simulant un utilisateur réel du réseau avec accès restreint.
- Serveur local, hébergeant des services internes et soumis à des règles de filtrage.
- Câbles RJ45 pour les connexions physiques entre les équipements.

Logiciels :

- Interface d'administration Stormshield, permettant de configurer et surveiller le pare-feu.
- Navigateur web pour accéder à l'interface de gestion en HTTPS.
- Putty pour les connexions SSH et l'administration en ligne de commande.

4. Prérequis techniques

Remise à l'état usine du pare-feu : Avant toute configuration, il est essentiel de réinitialiser le pare-feu à ses paramètres d'usine pour éviter toute configuration préexistante pouvant altérer les tests.

Connexion initiale à l'interface d'administration : Le pare-feu doit être accessible via son interface web en HTTPS pour les paramétrages initiaux.

Compréhension des règles de filtrage et des objets réseau : La configuration repose sur la création et l'application de règles de filtrage adaptées aux différents segments du réseau.

Notions de routage et de NAT : Une bonne connaissance des mécanismes de routage et de traduction d'adresse réseau (NAT) est requise pour configurer correctement la connectivité entre les différents segments du réseau.

5. Connexion au pare-feu

Pour garantir une configuration propre et éviter les conflits, il est nécessaire de réinitialiser le pare-feu à son état d'usine. Cette opération se fait en maintenant le bouton **Reset** enfoncé pendant **10 secondes**. Sur certains modèles, un bip sonore indique que la réinitialisation a été prise en compte. Une fois redémarré, le pare-feu charge sa configuration par défaut.

Dans cette configuration d'usine :

- La première interface du pare-feu est **OUT** (connexion à Internet).
- La seconde interface est **IN** (connexion aux postes internes).
- Les interfaces restantes sont **DMZx** (utilisées pour les réseaux isolés comme les serveurs accessibles depuis l'extérieur).

L'ensemble des interfaces est inclus dans un **bridge** dont l'adresse IP est **10.0.0.254/8**. Un **serveur DHCP** est actif sur toutes les interfaces du bridge et distribue des adresses IP comprises entre **10.0.0.10 et 10.0.0.100**.

Accès à l'interface d'administration

Pour accéder à l'interface d'administration du pare-feu, il faut :

1. **Connecter un poste administratif** à une interface interne du pare-feu (IN ou DMZ).
2. **Ouvrir un navigateur web** et entrer l'URL suivante : https://10.0.0.254/admin.
3. **S'authentifier** avec les identifiants par défaut :
    - **Utilisateur :** admin
    - **Mot de passe :** admin

Une fois connecté, il est fortement recommandé de modifier ces identifiants pour renforcer la sécurité. À partir de l'interface graphique, on pourra ensuite configurer le pare-feu, définir des règles de filtrage et ajuster les paramètres réseau.

6. Configuration générale

Avant de procéder aux paramétrages avancés, il est essentiel de personnaliser la configuration du pare-feu pour s'assurer qu'il répond aux exigences du laboratoire :

1. **Paramètres système** (Menu Configuration → Système → Configuration) :
    - Renommer le pare-feu en suivant la convention pare-feu-[lettre_du_labo].
    - Définir la langue par défaut en français pour les journaux et la disposition du clavier.

    - Appliquer une politique de mot de passe stricte et modifier le mot de passe administrateur par défaut.
    - Synchroniser l'heure du pare-feu avec celle du poste administrateur.
    - Désactiver la déconnexion automatique sur l'interface d'administration pour éviter toute interruption lors des configurations.
    - Activer SSH et configurer l'authentification par mot de passe.
2. **Gestion des utilisateurs** (Menu Configuration → Système → Administrateurs) :
    - Modifier immédiatement le mot de passe du compte admin pour renforcer la sécurité.
3. **Vérification des licences et mises à jour** (Menu Configuration → Système → Licence et Maintenance) :
    - S'assurer que les licences sont valides et que les mises à jour automatiques sont activées.
4. **Configuration des logs et de la supervision** (Menu Configuration → Notifications → Traces – Syslog – IPFIX) :
    - Activer la collecte des journaux sur un stockage interne pour assurer une meilleure traçabilité des événements réseau.
5. **Sauvegarde de la configuration** :
    - Une fois la configuration initiale terminée, effectuer une sauvegarde complète afin de pouvoir restaurer rapidement le système en cas de problème.

7. Configuration du pare-feu

La configuration du pare-feu est une étape clé pour assurer la segmentation et la sécurité du réseau.

1. Configuration des interfaces

Dans le menu **Configuration → Réseaux → Interface**, nommez les interfaces comme suit :

- **Interface 1** : out (liaison vers Internet)
- **Interface 2** : etudiant (réseau des étudiants)
- **Interface 3** : serveur (réseau des serveurs)

2. Création des objets réseau

Dans le menu **Configuration → Objets → Objets réseau → Machines**, créez les objets suivants :

- Un objet pour votre **serveur de labo**, nommé serveur-labo-[lettre_du_labo].
- Un objet pour les **serveurs des autres labos**, en suivant le même format (serveur-labo-A, serveur-labo-B, etc.).
- Un objet pour le **poste pédagogique** utilisé pour l'administration.

Ensuite, dans **Configuration → Objets → Objets réseau → Groupes**, créez un groupe nommé groupe-serveurs, dans lequel vous placerez tous les serveurs des différents labos.

3. Configuration du routage

Ajoutez une route par défaut pointant vers **192.168.30.254** (passerelle). Cette route est essentielle pour permettre aux machines du réseau d'accéder à Internet et aux autres labos.

4. Connexions et tests

- Reliez les **postes étudiant et serveur** aux interfaces du pare-feu.
- Vérifiez que les machines du réseau obtiennent bien une adresse IP via DHCP.
- Effectuez un **test de connectivité** en lançant des **pings** depuis les postes étudiant et serveur vers l'adresse du pare-feu (10.0.0.254).

8. Paramétrage des flux et filtrage

1. Objectif

L'objectif de cette étape est de configurer une politique de filtrage des flux afin de sécuriser les communications entre les différents segments du réseau. Cela permet de limiter les accès aux ressources selon les besoins et de garantir une meilleure protection des infrastructures.

2. Configuration de la politique de filtrage

Les paramétrages des flux s'effectuent dans **Configuration → Politique de sécurité → Filtrage et NAT → Onglet Filtrage**.

1. Sélectionnez la dernière règle de filtrage disponible (règle **10** pour la version 4 de Stormshield et **9** pour la version 3).
2. Renommez-la en **mon-filtrage**.
3. Activez cette politique pour qu'elle soit appliquée immédiatement.

3. Analyse des accès par défaut

Avant de modifier les règles, il est important d'analyser le comportement du pare-feu avec la configuration par défaut :

- **Le poste étudiant peut-il accéder au poste serveur sur n'importe quel port ?**
- **Les postes serveurs et étudiants ont-ils un accès à Internet ?**
- **Les postes extérieurs peuvent-ils accéder aux postes étudiants et serveurs ?**

Ces questions permettent d'identifier les éventuels risques de sécurité liés aux réglages par défaut du pare-feu.

4. Modification des règles de filtrage

Afin de renforcer la sécurité du réseau, nous allons appliquer les règles suivantes :

Autoriser :

- L'accès du poste étudiant à Internet, limité aux **ports HTTP (80) et HTTPS (443)**.
- L'accès du poste étudiant aux ressources du serveur de laboratoire via les **ports regroupés dans le groupe "plugins"**.

Interdire :

- Tout accès du serveur du laboratoire vers Internet, afin de prévenir toute fuite de données ou compromission.

5. Ajout d’une règle de sécurité finale

À la fin de votre politique de filtrage, ajoutez une règle explicite bloquant tout trafic non autorisé.

Cette règle garantit qu'aucun flux indésirable ne traverse le pare-feu et respecte ainsi les recommandations de l'ANSSI.

Pourquoi cette règle est-elle importante ?

- Elle empêche toute connexion non prévue par les règles précédentes.
- Elle réduit les risques de contournement des politiques de filtrage.
- Elle constitue une mesure de protection essentielle en cybersécurité.

6. Validation et tests

Une fois la configuration des règles de filtrage terminée, procédez aux vérifications suivantes :

1. **Test de navigation Internet** depuis le poste étudiant : seuls les sites en HTTP et HTTPS doivent être accessibles.
2. **Test de connexion au serveur** : l’accès doit être possible uniquement via les ports définis dans le groupe "plugins".
3. **Test d’accès depuis le serveur vers Internet** : la connexion doit être refusée.
4. **Test d’accès depuis l’extérieur vers les postes internes** : toute tentative de connexion doit être bloquée.

Ces tests permettent de confirmer que les règles sont bien appliquées et que le réseau est sécurisé conformément aux exigences du TP.

9. Paramétrage du filtrage horaire

1. Objectif

L’objectif est de restreindre l’accès à Internet du poste étudiant à une plage horaire définie, soit entre **12h00 et 14h00**. Cette configuration permet de contrôler les usages du réseau et de limiter l’accès en dehors des heures prévues.

2. Création de l’objet temps

Le filtrage horaire repose sur la création d’un objet temps qui définit les heures autorisées. Cette opération s’effectue dans le menu **Configuration → Objets → Objets réseaux → Objets temps**.

1. Créez un nouvel objet temps et nommez-le **mon-objet-temps**.
2. Définissez la plage horaire **de 12h00 à 14h00**.
3. Enregistrez et appliquez les modifications.

3. Association de l’objet temps à la règle de filtrage

Une fois l’objet temps créé, il doit être intégré à la politique de filtrage existante pour appliquer la restriction horaire sur le trafic Internet du poste étudiant.

1. Rendez-vous dans **Configuration → Politique de sécurité → Filtrage et NAT → Onglet Filtrage**.

2. Ouvrez la règle de filtrage correspondant à l'accès Internet du poste étudiant en double-cliquant dessus.
3. Dans **Actions → Général**, localisez le paramètre **Programmation horaire**.
4. Sélectionnez **mon-objet-temps** comme critère de validation de la règle.
5. Enregistrez et appliquez les modifications.

4. Validation et tests

Pour s'assurer du bon fonctionnement du filtrage horaire, effectuez les tests suivants :

1. **Avant 12h00 et après 14h00** : Le poste étudiant ne doit pas pouvoir accéder à Internet.
2. **Entre 12h00 et 14h00** : La navigation sur les sites en HTTP et HTTPS doit être autorisée.
3. **Vérification des logs** : Consultez les journaux du pare-feu pour confirmer l'application des règles horaires.

Cette configuration garantit une gestion efficace des accès Internet en fonction des besoins et des contraintes du réseau.

10. Paramétrage de la QoS

1. Objectif

L'objectif est de garantir une répartition optimisée de la bande passante entre les différents segments du réseau. Le réseau serveur nécessite une **réservation de bande passante** pour assurer une disponibilité constante des services critiques, tandis que le réseau étudiant doit être soumis à une **limitation de débit** afin d'éviter toute congestion excessive.

2. Création des règles de QoS

La configuration de la QoS se déroule en deux étapes : la création des files d'attente et leur association aux règles de filtrage.

2.1 Création des files d'attente QoS

Dans **Configuration → Politique de sécurité → Qualité de service → Ajouter une file d'attente**, procédez comme suit :

1. **Création de la réservation de bande passante pour le réseau serveur** :
   - Nom : QWsrv
   - Type : **Réservation**
   - Bande passante garantie : **10 Mb/s**
2. **Création de la limitation de bande passante pour le réseau étudiant** :
   - Nom : QWetu
   - Type : **Limitation**
   - Débit maximal autorisé : **8 Mb/s**

Enregistrez et appliquez les modifications.

2.2 Association de la QoS aux règles de filtrage

Une fois les files d'attente créées, elles doivent être intégrées aux règles de filtrage pour qu'elles prennent effet.

1. Rendez-vous dans **Configuration → Politique de sécurité → Filtrage et NAT → Onglet Filtrage**.
2. Ouvrez la règle de filtrage correspondant au **trafic du réseau serveur** et assignez-lui la file d'attente QWsrv.
3. Ouvrez la règle de filtrage du **réseau étudiant** et appliquez-lui la file d'attente QWetu.
4. Enregistrez et appliquez les modifications.

3. Différences entre QoS de réservation et de limitation

- **QoS de réservation** : garantit une quantité minimale de bande passante pour un segment donné, indépendamment des autres flux présents sur le réseau.
- **QoS de limitation** : impose une restriction de débit maximal pour éviter qu'un réseau ne consomme trop de ressources et impacte la qualité du service global.

4. Intérêts de la mise en place de ces QoS

- **Optimisation des performances réseau** : la réservation assure que les serveurs critiques ne seront pas affectés par une saturation du réseau.
- **Équilibrage de la bande passante** : la limitation empêche une surconsommation excessive de la part des postes étudiants.
- **Amélioration de la stabilité du réseau** : évite les ralentissements imprévus et assure un fonctionnement fluide des applications sensibles.

5. Validation et tests

Une fois la configuration effectuée, réalisez les tests suivants :

1. **Sur le réseau serveur** :
    - Vérifiez que la bande passante réservée est bien allouée.
    - Simulez un trafic élevé et observez si la limite de 10 Mb/s est respectée.
2. **Sur le réseau étudiant** :
    - Effectuez un test de débit (ex. téléchargement d'un fichier volumineux) et assurez-vous que la limitation de 8 Mb/s est appliquée.
3. **Surveillance en temps réel** :
    - Consultez les graphiques de performance du pare-feu pour confirmer l'application des politiques de QoS.

Ces tests permettent de s'assurer que la gestion du trafic est conforme aux attentes et que les performances du réseau sont optimisées.

11. Mise en place du filtrage URL

1. Objectif

L'objectif est de bloquer certains sites en HTTP pour le réseau étudiant en utilisant le filtrage URL du pare-feu Stormshield.

2. Configuration du filtrage URL

2.1 Création d'une politique de filtrage URL

1. Accédez à **Configuration → Politique de sécurité → Filtrage URL → Onglet Filtrage URL**.
2. Sélectionnez la dernière règle de filtrage disponible (règle 10 pour la version 4 ou règle 9 pour la version 3 de Stormshield).
3. Renommez la règle en mon-filtrage-URL.

2.2 Création d'une liste noire

1. Allez dans **Configuration → Objets → Objets web → Onglet URL**.
2. Ajoutez une **catégorie personnalisée** et nommez-la ma-liste-noire.
3. Dans la fenêtre de droite, cliquez sur **Ajouter une URL** et entrez : notionsinformatique.free.fr/*.

2.3 Application du filtrage URL

1. Retournez dans **Configuration → Politique de sécurité → Filtrage URL → Onglet Filtrage URL**.
2. Modifiez la règle mon-filtrage-URL comme suit :
    - **Première ligne** : Action = bloquer, Catégorie d'URL = ma-liste-noire.
    - **Deuxième ligne** : Action = passer, Catégorie d'URL = any.
3. Enregistrez et appliquez les modifications.

2.4 Association du filtrage au réseau étudiant

1. Accédez à **Configuration → Politique de sécurité → Filtrage et NAT**.
2. Sélectionnez la règle concernant le réseau étudiant.
3. Double-cliquez dessus et allez dans l'onglet **Inspection**.
4. Pour le filtrage URL, sélectionnez mon-filtrage-URL.
5. Enregistrez et appliquez les modifications.

3. Validation des tests

Depuis un poste étudiant :

- Essayez d'accéder au site http://notionsinformatique.free.fr/ et vérifiez qu'il est bien bloqué.
- Testez l'accès à d'autres sites pour s'assurer qu'ils restent accessibles.
- Consultez les journaux du pare-feu pour confirmer le blocage.

12. Filtrage SSL

1. Objectif

L'objectif du filtrage SSL est de contrôler et de restreindre l'accès aux sites web utilisant HTTPS. Comme les connexions HTTPS sont chiffrées, il est nécessaire d'inspecter ces flux pour identifier et bloquer certaines catégories de sites sans compromettre la sécurité globale du réseau.

Le filtrage SSL permet de :

- Déchiffrer certains flux pour analyser leur contenu.
- Bloquer l'accès à certaines catégories de sites sans nécessiter de déchiffrement.
- Assurer une meilleure protection du réseau contre les menaces web.

2. Mise en place du filtrage SSL

2.1 Création d'une politique de filtrage SSL

1. Accédez à **Configuration → Politique de sécurité → Filtrage SSL → Onglet Filtrage SSL**.
2. Sélectionnez la dernière règle de filtrage disponible (règle 10 pour la version 4 ou règle 9 pour la version 3 de Stormshield).
3. Renommez la règle en `mon-filtrage-SSL`.

2.2 Premier cas : Déchiffrement des flux SSL

Le déchiffrement des flux SSL permet au pare-feu d'inspecter le contenu des communications HTTPS. Cela est utile pour identifier et bloquer des sites interdits en HTTPS.

1. Sélectionnez votre règle `mon-filtrage-SSL`.
2. **Première ligne** :
    - **Action** : `déchiffrer`
    - **Catégorie** : `by proxyssl_bypass`
3. **Deuxième ligne** :
    - **Action** : `passer sans déchiffrer`
    - **Catégorie** : `any`
4. Enregistrez et appliquez les modifications.

Une fois ce filtrage activé, les flux SSL seront interceptés et analysés par le pare-feu, ce qui peut entraîner des avertissements de certificat sur les navigateurs des utilisateurs. Pour éviter ces alertes, il est nécessaire d'installer le certificat de confiance du pare-feu sur les postes clients.

2.3 Deuxième cas : Non-déchiffrement des flux SSL

Si l'on ne souhaite pas déchiffrer les flux SSL pour des raisons de confidentialité, il est possible de bloquer certains sites directement en fonction de leur catégorie sans inspection du contenu.

1. Sélectionnez votre règle `mon-filtrage-SSL`.
2. **Première ligne** :
    - **Action** : `bloquer sans déchiffrer`
    - **Catégorie d'URL** : `banque`
3. **Deuxième ligne** :

   - **Action** : `passer sans déchiffrer`
   - **Catégorie** : `any`
4. Enregistrez et appliquez les modifications.

Ce paramétrage empêche l'accès aux sites bancaires en HTTPS sans intercepter ni analyser le contenu des flux SSL.

3. Association du filtrage SSL au réseau étudiant

1. Accédez à **Configuration → Politique de sécurité → Filtrage et NAT**.
2. Cliquez sur **Nouvelle règle → Règle d'inspection SSL**.
3. Dans la fenêtre suivante :
   - **Machines sources** : Sélectionnez votre réseau étudiant.
   - **Politiques de filtrage SSL** : Sélectionnez `mon-filtrage-SSL`.
   - **Destination** : Bloquer vers Internet.
4. Cliquez sur **Terminer**.
5. Enregistrez et appliquez les modifications.

4. Validation des tests

4.1 Test du premier cas (déchiffrement SSL)

- Depuis un poste étudiant, essayez d'accéder à `https://www.google.com`.
- Vérifiez si le site s'ouvre correctement ou si un message d'alerte SSL apparaît.
- Pourquoi l'accès à Google peut-il être impacté alors que seuls les sites bancaires sont censés être bloqués ?

4.2 Test du deuxième cas (non-déchiffrement SSL)

- Depuis un poste étudiant, essayez d'accéder à `https://www.google.com`.
- Testez également `https://home.barclays`.
- Confirmez que l'accès à Google est autorisé mais que Barclays est bloqué.

5. Conclusion

Le filtrage SSL est un outil puissant pour sécuriser les accès web tout en maintenant un contrôle strict sur les catégories de sites autorisées. Le choix entre déchiffrement et non-déchiffrement dépend des besoins en sécurité et confidentialité du réseau.

- **Avantages du déchiffrement** :
  - Permet une analyse approfondie des flux HTTPS.
  - Bloque efficacement les sites interdits.
  - Protège contre les malwares et sites de phishing.
- **Inconvénients du déchiffrement** :
  - Peut entraîner des alertes de certificat sur les navigateurs.
  - Nécessite l'installation du certificat de confiance sur les postes clients.
- **Avantages du non-déchiffrement** :
  - Respecte la confidentialité des utilisateurs.
  - Ne nécessite pas de configuration supplémentaire sur les clients.
- **Inconvénients du non-déchiffrement** :
  - Moins efficace pour bloquer certains sites en HTTPS.
  - Peut être contourné par des services de proxy.

13. Connexion entre 2 labos

Les labos vont travailler par binôme :

- Labo-A avec Labo-B
- Labo-C avec Labo-D
- Labo-E avec Labo-F

Objectif Labo-A et Labo-B

Les réseaux étudiant-A et serveur-A doivent accéder aux réseaux étudiant-B et serveur-B, et inversement.

Configuration de l'interface réseau

1. Reliez les interfaces **out** des deux pare-feux ensemble.
2. Configurez l'interface **out** de votre pare-feu selon le schéma réseau fourni.
3. Créez les objets réseau nécessaires :
    - **FW_lettre-du-site-à-joindre** avec l'adresse IP du pare-feu correspondant.
    - **labo-etu-du-site-à-joindre** représentant les réseaux étudiants de l'autre site.

1ère étape : Configuration des routes

1. Supprimez la route par défaut.
2. Configurez des **routes statiques** permettant aux réseaux étudiant et serveur de joindre les réseaux correspondants du site distant.
3. Accédez au menu : **Configuration -> Réseau -> Routes statiques -> Ajouter**.
4. Configurez chaque route :
    - Destination : l'objet réseau du serveur de l'autre site.
    - Interface : **out** (reliée aux pare-feux des sites partenaires).
    - Passerelle : l'objet pare-feu du site distant.

2ème étape : Règles de filtrage

1. **Autoriser** les flux des réseaux étudiant et serveur vers leurs homologues sur l'autre site.
2. **Autoriser** le flux du réseau étudiant distant vers votre réseau serveur.
3. **Bloquer** le flux du réseau étudiant distant vers votre réseau étudiant.

Tests :

- Que se passe-t-il si vous **enlevez la passerelle** sur vos stations ?
- Que se passe-t-il si vous **supprimez les routes** sur les pare-feux ?

14. Connexions entre les labos

Objectifs

1. Les postes étudiants des autres labos doivent accéder à votre **réseau serveur** uniquement sur les ports **Samba, HTTPS, DNS et DHCP**.
2. Votre réseau étudiant doit pouvoir accéder aux réseaux des autres labos.
3. Les réseaux étudiants des autres labos ne doivent **pas** accéder à votre réseau étudiant.
4. Les serveurs des autres labos doivent accéder à votre **réseau serveur** uniquement sur les ports **SSH et RDP**.

Règles de filtrage

1. **Autoriser** l'accès des postes étudiants externes vers le réseau serveur local sur **Samba, HTTPS, DNS et DHCP**.
2. **Autoriser** les flux depuis votre réseau étudiant vers les réseaux étudiants des autres labos.
3. **Bloquer** l'accès des étudiants des autres labos à votre réseau étudiant.
4. **Autoriser** l'accès des serveurs distants à votre serveur uniquement sur **SSH et RDP**.

Pour autoriser seulement le ping, il faut autoriser directement le protocole dans les règles de filtrage et non faire par port comme précédemment.

Conclusion

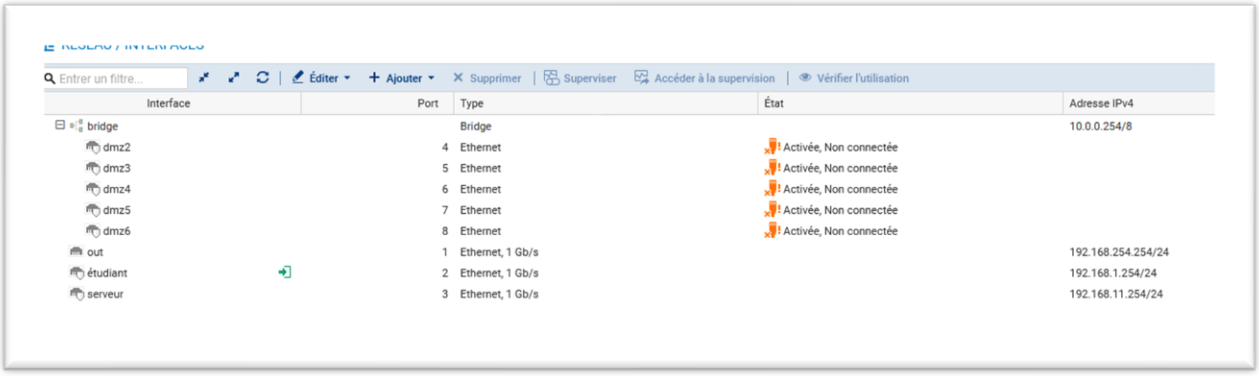
Ce TP nous a permis de configurer et sécuriser un pare-feu ainsi qu'un proxy pour gérer les connexions entre différents réseaux. Nous avons mis en place des routes statiques et défini des règles de filtrage précises afin de contrôler les flux entre les postes étudiants, les serveurs et les réseaux distants.

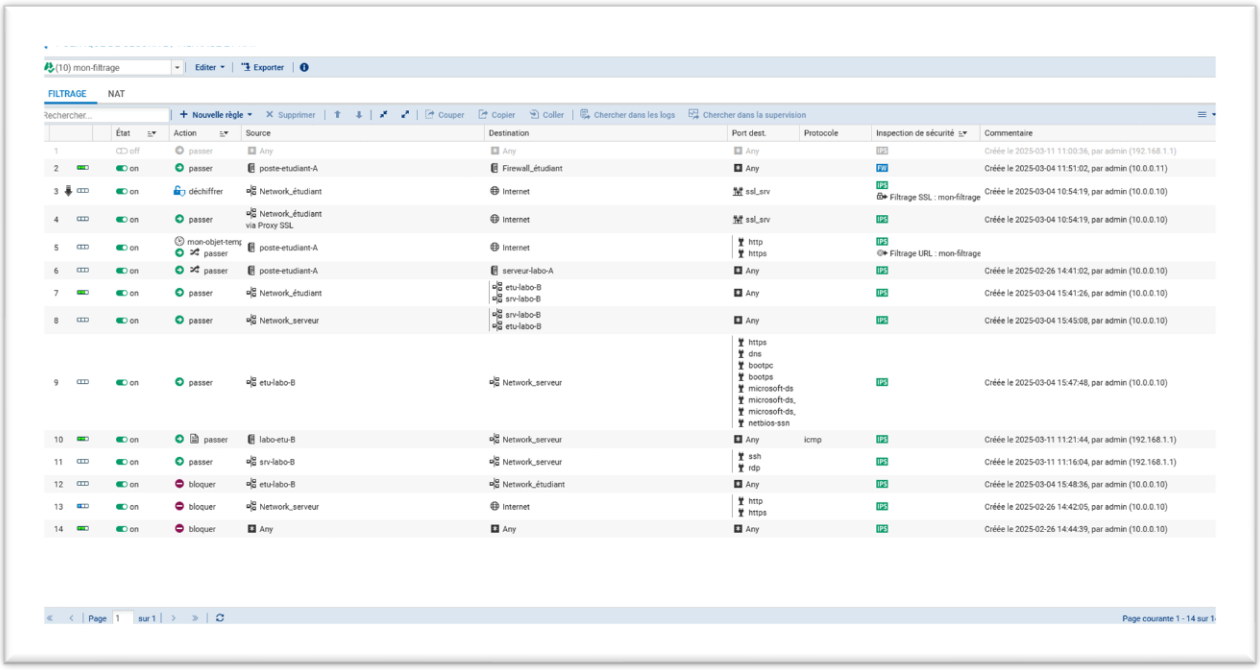
Nous avons également abordé les bonnes pratiques en matière de sécurité, notamment en suivant les recommandations de l'ANSSI, comme la politique de refus par défaut et la restriction des protocoles non sécurisés comme Telnet.

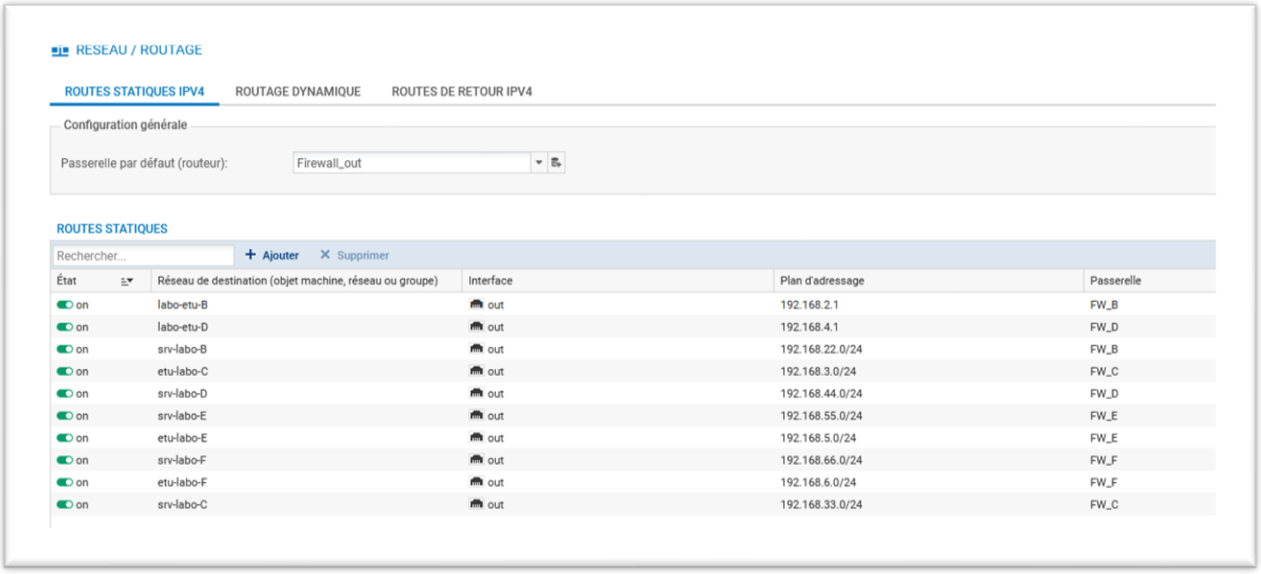
Les tests réalisés nous ont permis de valider les configurations et de comprendre l'impact des routes et des passerelles sur la communication réseau. Enfin, ce TP nous a sensibilisés à l'importance d'un contrôle strict des accès pour garantir la sécurité des infrastructures.

Annexes :


URL
NOM DE CERTIFICAT (CN)
GROUPE DE CATÉGORIES
BASE D'URL
Ajouter une catégorie personnalisée
Supprimer
Vérifier l'utilisation
Vérifier la classification d'une URL
Classifier
Caractères autorisés
Les caractères autorisés sont : [a-z] [A-Z] [0-9]
Exemple d'URL : www.google.com/* ou *.yahoo.com/*
CATÉGORIE D'URL : MA-LISTE-NOIRE
Ajouter une URL
Supprimer
URL
Commentaire
notionsinformatiques.free.fr/*


Entrer un filtre...
Éditer
Ajouter
Supprimer
Superviser
Accéder à la supervision
Vérifier l'utilisation
Interface
Port
Type
État
Adresse IPv4
bridge
Bridge
10.0.0.254/8
dmz2
4
Ethernet
Activée, Non connectée
dmz3
5
Ethernet
Activée, Non connectée
dmz4
6
Ethernet
Activée, Non connectée
dmz5
7
Ethernet
Activée, Non connectée
dmz6
8
Ethernet
Activée, Non connectée
out
1
Ethernet, 1 Gb/s
192.168.254.254/24
étudiant
2
Ethernet, 1 Gb/s
192.168.1.254/24
serveur
3
Ethernet, 1 Gb/s
192.168.11.254/24


(10) mon-filtrage
Editer
Exporter
FILTRAGE
NAT
Nouvelle règle
Supprimer
Couper
Copier
Coller
Chercher dans les logs
Chercher dans la supervision
État
Action
Source
Destination
Port dest.
Protocole
Inspection de sécurité
Commentaire


RESEAU / ROUTAGE
ROUTES STATIQUES IPV4
ROUTAGE DYNAMIQUE
ROUTES DE RETOUR IPV4
Configuration générale
Passerelle par défaut (routeur):
Firewall_out
ROUTES STATIQUES
Rechercher...
Ajouter
Supprimer
État
Réseau de destination (objet machine, réseau ou groupe)
Interface
Plan d'adressage
Passerelle
on labo-etu-B out 192.168.2.1 FW_B
on labo-etu-D out 192.168.4.1 FW_D
on srv-labo-B out 192.168.22.0/24 FW_B
on etu-labo-C out 192.168.3.0/24 FW_C
on srv-labo-D out 192.168.44.0/24 FW_D
on srv-labo-E out 192.168.55.0/24 FW_E
on etu-labo-E out 192.168.5.0/24 FW_E
on srv-labo-F out 192.168.66.0/24 FW_F
on etu-labo-F out 192.168.6.0/24 FW_F
on srv-labo-C out 192.168.33.0/24 FW_C