Listes de Contrôle d'Accès (ACL) – Suite de l'Atelier

Atelier pédagogique réseau

Table des matières

1 Introduction

Ce document constitue la suite de l'atelier consacré aux **Listes de Contrôle d'Accès (ACL)**. Vous allez approfondir vos compétences en matière de filtrage réseau, d'organisation des flux, et de sécurisation d'une architecture multi-réseaux.

L'objectif de ce document est de vous accompagner dans la construction progressive d'une politique de sécurité interne cohérente. Toutes les exigences doivent être réalisées en vous appuyant sur les informations d'adressage du réseau étudié.

Vous trouverez ci-dessous :

— un rappel de la topologie du réseau ;

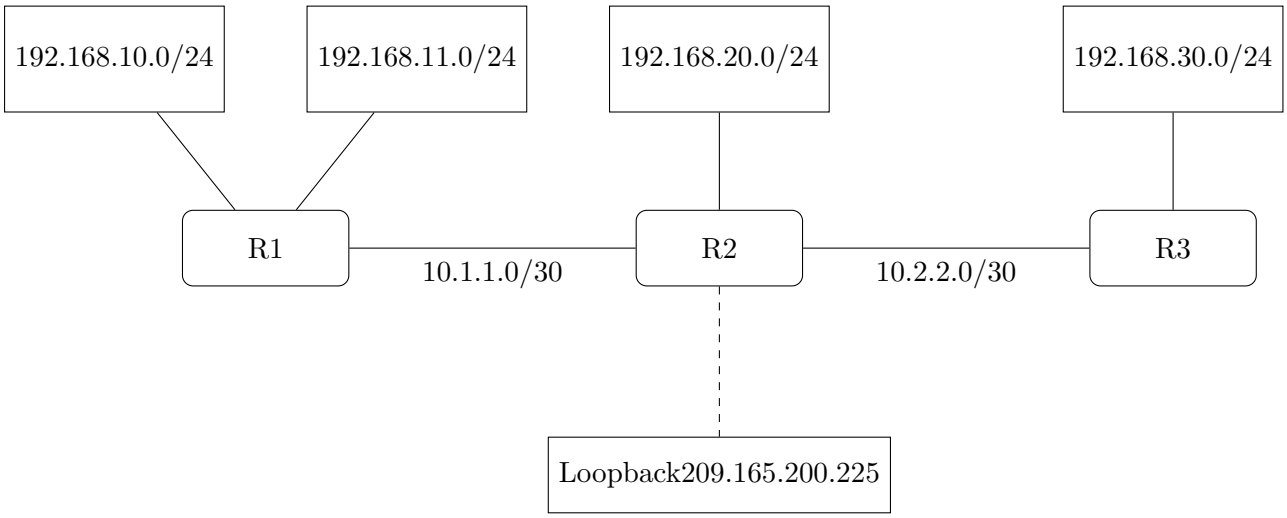
— un ensemble d'exigences à réaliser ;

— une logique de scénario cohérente aboutissant à une politique ACL complète.

Toutes les ACL doivent être testées, documentées et analysées.

2 Topologie du réseau

La figure suivante représente la topologie simplifiée utilisée pour cet atelier. Les adresses IP correspondent à celles du premier atelier.



3 Objectifs

À l'issue de cet atelier, vous serez capables de :

— analyser les besoins de sécurité d'un réseau multi-segmenté ;

— formuler et concevoir une politique ACL complète ;

— appliquer un ensemble cohérent de règles selon les besoins fonctionnels ;

— renforcer progressivement la sécurité du réseau interne ;

— documenter et valider l'impact des filtrages appliqués.

4 Exigences

Les exigences suivantes s'inscrivent dans un scénario unique visant à élaborer progressivement une politique ACL cohérente et sécurisée. Vous devez réaliser chaque exigence dans l'ordre, en vérifiant et en documentant les effets obtenus.

4.1 Cloisonnement initial des réseaux

E1. Interdire tout accès provenant du réseau **192.168.11.0/24** vers le réseau **192.168.30.0/24**.

E2. Interdire tout accès provenant de l'hôte **192.168.11.10** vers le réseau **192.168.10.0/24**.

E3. Interdire toute communication entre l'hôte **192.168.30.2** et l'hôte **192.168.10.2**, sauf vers les adresses du réseau **192.168.20.0/24**.

E4. Bloquer tout accès du réseau **192.168.30.0/24** vers l'hôte **192.168.20.254**.

4.2 Contrôle des protocoles et services

E5. Autoriser uniquement les accès HTTP et HTTPS provenant du réseau **192.168.10.0/24** vers l'hôte **192.168.20.254**, et bloquer tout autre protocole vers cette destination.

E6. Autoriser uniquement les requêtes DNS provenant de l'hôte **192.168.10.10** vers **192.168.20.254**, et bloquer toutes les réponses DNS provenant d'autres adresses.

E7. Interdire tout accès Telnet à l'hôte **192.168.20.1**, sauf si la source est **192.168.30.2**.

E8. Autoriser uniquement les messages ICMP de type *echo-request*, *echo-reply* et *destination-unreachable* entre les réseaux **192.168.30.0/24** et **192.168.10.0/24**.

4.3 Sécurité avancée des flux internes

E9. Interdire tout accès TCP provenant du réseau **192.168.20.0/24** vers le réseau **192.168.30.0/24**, tout en permettant le trafic UDP.

E10. Interdire le trafic SMTP provenant de **192.168.10.0/24**, tout en permettant POP3 et IMAP.

E11. Interdire les connexions FTP actives entre l'hôte **192.168.30.10** et **192.168.20.254**, tout en autorisant le FTP passif.

E12. Autoriser le réseau **192.168.10.0/24** à contacter l'adresse **209.165.200.225** uniquement en HTTPS.

4.4 Protection contre les comportements suspects

E13. Bloquer tout paquet TCP avec drapeau SYN provenant de **192.168.30.10** vers le réseau **192.168.10.0/24**.

E14. Interdire tout trafic contenant des adresses privées invalides en provenance du réseau **192.168.20.0/24**.

E15. Refuser tout trafic appartenant à **192.168.10.0/24** lorsqu'il traverse une liaison série inter-routeurs.

E16. N'autoriser l'accès SSH à l'hôte **192.168.20.1** qu'à partir de l'adresse **192.168.10.10**.

4.5 Politique finale unifiée

E17. Mettre en place une politique garantissant l'isolation complète entre les réseaux **192.168.10.0/24**, **192.168.11.0/24** et **192.168.30.0/24**, tout en autorisant leurs accès contrôlés au réseau **192.168.20.0/24**.

E18. Interdire tout accès vers l'adresse **209.165.200.225** sauf les connexions HTTPS provenant de **192.168.10.0/24**.

E19. Interdire tout trafic provenant de **10.2.2.0/30** vers le réseau **192.168.11.0/24**.

E20. Limiter les flux autorisés du réseau à :

- HTTP/HTTPS vers **192.168.20.254** ;
- DNS entre **192.168.10.10** et **192.168.20.254** ;
- SSH uniquement depuis **192.168.10.10** ;
- ICMP restreint entre **192.168.10.0/24** et **192.168.30.0/24**.

4.6 Optimisation et audit

E21. Identifier les règles redondantes portant sur les réseaux **192.168.10.0/24**, **192.168.11.0/24** et **192.168.20.0/24** et les optimiser.

E22. Réordonner la politique afin que les accès spécifiques **192.168.10.10**, **192.168.11.10** et **192.168.30.10** soient évalués avant les règles générales.

E23. Vérifier l'absence de contradictions dans l'ensemble de la politique écrite.

E24. Rédiger un audit listant les risques restants et les recommandations d'amélioration.

5 Conclusion

Vous venez d'élaborer une politique ACL complète, structurée et cohérente. Les exigences proposées vous ont permis de renforcer progressivement la sécurité du réseau, d'identifier les flux critiques, de contrôler les protocoles autorisés et d'isoler efficacement les différents segments.

Ce travail constitue une base solide pour aborder des scénarios de sécurité plus avancés et pour analyser des architectures réseau complexes dans un contexte professionnel.