Sentinelle Routage

Surveillance BGP / RPKI & rapports de sécurité du routage — sentinelle-routage.fr

C

Rapport de sécurité du routage AS64496

État des lieux initial (T0) — entrée en surveillance continue

RAPPORT D'EXEMPLE — réseau fictif, données illustratives

Client	**Opérateur Exemple SAS (fictif)**
Ressource	**AS64496 (ASN de documentation) — 6 préfixes annoncés**
Formule	**Fondateur — surveillance continue 24/7**
Surveillance active depuis	**1er juillet 2026 (illustratif)**
Date du rapport	**Juillet 2026**
Note santé routage	**C — hygiène moyenne, angles morts à corriger (détail p. 2)**

Rapport d'exemple — réseau fictif (AS64496, ressources de documentation). Structure et grille identiques aux rapports clients réels.

1. Synthèse

AS64496 présente une **hygiène de routage moyenne, typique d'un opérateur qui a commencé le travail RPKI sans le finir** : visibilité mondiale parfaite et IRR complet, mais la moitié seulement des annonces est correctement protégée. Trois problèmes distincts coexistent : **un préfixe en statut INVALID** (rejeté par les opérateurs qui valident), **deux préfixes sans aucun ROA**, et **un ROA trop permissif** qui ouvre la porte à un détournement par sous-préfixe.

6	50 %	1	100 %
préfixes annoncés (3 IPv4 + 3 IPv6)	couverture RPKI valide (3/6 préfixes)	préfixe INVALID	visibilité RIS (v4 et v6)

Le plus urgent. `2001:db8:30::/48` est annoncé en **INVALID** : le ROA couvrant (`2001:db8::/32`, maxLength 40) n'autorise pas une annonce en /48. Une part majoritaire des grands transitaires rejette automatiquement ces routes (ROV) : ce préfixe est déjà **partiellement injoignable** depuis certains réseaux, silencieusement. C'est le symptôme classique d'un ROA créé puis oublié lors d'une redécoupe de l'espace.

La bonne nouvelle. Les trois corrections sont **simples, gratuites et rapides** (~45 minutes au total via le portail du RIR, plan d'action p. 5). Elles feraient passer la note de **C** à **A/A-** au prochain cycle d'évaluation.

Points forts relevés

Visibilité RIS de 100 % sur les deux familles ; objets route/route6 IRR présents pour les 6 préfixes ; contact abuse publié et à jour (abuse@exemple.example) ; ROA IPv4 strict et conforme RFC 9319 sur `192.0.2.0/24`.

Rapport d'exemple — réseau fictif (AS64496, ressources de documentation).

2. État du routage observé

Origine : AS64496 (Opérateur Exemple SAS), premier préfixe observé en mars 2022. Transit : AS64511 (Transit Exemple). Les rôles et la topologie sont illustratifs.

Préfixes annoncés et statut RPKI (6)

Préfixe	Famille	Statut RPKI	ROA (origine / maxLength)	IRR
192.0.2.0/24	IPv4	VALID	AS64496 / 24	RIPE
198.51.100.0/24	IPv4	VALID ROA PERMISSIF	AS64496 / 32 ⚠	RIPE
203.0.113.0/24	IPv4	SANS ROA	—	RIPE
2001:db8:10::/48	IPv6	VALID	AS64496 / 48	RIPE
2001:db8:20::/48	IPv6	SANS ROA	—	RIPE
2001:db8:30::/48	IPv6	INVALID	2001:db8::/32 · AS64496 / 40 (trop courte)	RIPE

Visibilité : chaque préfixe est vu par l'intégralité des collecteurs RIS full-feed. « SANS ROA » (RPKI *not found*) : le préfixe n'est couvert par aucune Route Origin Authorization — l'annonce n'est ni validée ni invalidée par la RPKI. « INVALID » : un ROA couvre le préfixe mais n'autorise pas cette annonce (ici, longueur /48 > maxLength 40).

Voisinage BGP observé

AS voisin	Opérateur	Rôle observé	Cohérence IRR
AS64511	Transit Exemple (fictif)	Amont (transit)	Export documenté ; import à documenter
AS64497	Client Exemple (fictif)	Aval (client)	Import/export à documenter

3. Analyse RPKI

Ce qui est en place

Trois ROA publiés couvrent quatre des six préfixes annoncés. Le ROA de `192.0.2.0/24` (maxLength strictement égale à la longueur annoncée) et celui de `2001:db8:10::/48` sont la configuration recommandée (RFC 9319) : ils n'ouvrent aucune surface d'attaque de type *forged-origin sub-prefix hijack*.

Problème n°1 — un préfixe INVALID

`2001:db8:30::/48` est couvert par le ROA du bloc parent (`2001:db8::/32`, maxLength 40) qui n'autorise pas d'annonce plus longue que /40. L'annonce actuelle en /48 est donc **rejetée par tous les réseaux qui font du ROV**. Deux corrections possibles : compléter le ROA (ajouter `2001:db8:30::/48`, origine AS64496), ou ramener l'annonce à une longueur autorisée. La première est en général la bonne.

Problème n°2 — deux préfixes sans ROA

`203.0.113.0/24` et `2001:db8:20::/48` relèvent du statut *not found* : en cas d'annonce concurrente par un tiers (erreur ou usurpation), les validateurs RPKI considéreraient les deux annonces comme équivalentes, et les mécanismes de rejet automatique ne protégeraient pas. La détection reposerait uniquement sur la surveillance des annonces — c'est ce que fait Sentinelle Routage — mais sans la capacité de blocage préventif qu'apportent les ROA.

Problème n°3 — un ROA trop permissif

Le piège de la maxLength. Le ROA de `198.51.100.0/24` autorise des annonces jusqu'au **/32** alors que seul le /24 est annoncé. Conséquence : un attaquant qui usurpe le numéro d'AS64496 peut annoncer par exemple `198.51.100.128/25` — une annonce **RPKI-VALID** aux yeux de tous les validateurs, qui gagne au longest-prefix match et détourne la moitié du trafic (*forged-origin sub-prefix hijack*, le scénario que la RFC 9319 vise précisément). Correction : ramener la maxLength à la longueur réellement annoncée (/24).

Recommandation centrale. Trois gestes au portail du RIR : compléter le ROA du /48 INVALID, créer les 2 ROA manquants (maxLength stricte), et resserrer la maxLength du ROA permissif. Aucun de ces gestes ne présente de risque pour un espace annoncé de manière stable.

4. Lecture MANRS et préparation NIS2

Positionnement vis-à-vis des 4 actions MANRS (opérateurs réseau)

Action MANRS	État observé	Constat
1. Filtrage des annonces incorrectes	Partiel	Côté « être filtrable » : IRR complet, mais l'INVALID actif et les ROA manquants limitent l'efficacité du filtrage que vos amonts peuvent appliquer. Le filtrage appliqué à votre aval (AS64497) n'est pas évaluable depuis les données publiques.
2. Anti-usurpation (anti-spoofing)	À documenter	Non observable depuis l'extérieur. À documenter : uRPF/ACL aux bordures, test CAIDA Spoofer recommandé pour produire une preuve datée.
3. Coordination (contacts joignables)	En place	Contact abuse publié et cohérent, objets registre à jour.
4. Validation globale (IRR / RPKI)	Partiel	IRR : 6/6 préfixes documentés — excellent. RPKI : 3/6 dont 1 INVALID et 1 ROA permissif — l'écart principal, entièrement rattrapable (§3).

Préparation NIS2 — lecture prudente

La directive (UE) 2022/2555 « NIS2 », en cours de transposition en droit français, attend des entités concernées une gestion documentée des risques de sécurité des réseaux et des systèmes d'information (art. 21), incluant la sécurité de l'infrastructure. Que votre structure soit ou non directement assujettie, vos clients peuvent l'être : la capacité à **démontrer la maîtrise de votre routage** — ROA complets, surveillance continue tierce, rapports datés et archivés — constitue un élément de preuve concret et peu coûteux dans un dossier de préparation ou une réponse à un questionnaire fournisseur.

Ce rapport documente un état observé et une démarche de surveillance ; il ne constitue ni une attestation de conformité NIS2 (la loi de transposition française n'est pas promulguée à date), ni une certification MANRS.

5. Surveillance et plan d'action

Surveillance Sentinelle Routage

Dans un rapport réel, cette section récapitule la période de surveillance écoulée : flux temps réel RIS Live (annonces/retraits vus par les collecteurs du RIPE NCC), contrôles périodiques RIPEstat et validation RPKI, et la liste datée des événements détectés (changement d'origine inattendu, annonce plus spécifique, passage INVALID, perte de visibilité) avec les alertes envoyées (email, Telegram). Pour ce réseau fictif : **1 événement illustratif** — le passage en INVALID de `2001:db8:30::/48` aurait été détecté et notifié en moins de deux minutes.

Plan d'action priorisé

#	Action	Effort	Impact
1	Compléter le ROA de `2001:db8:30::/48` (origine AS64496) pour sortir de l'INVALID	10 min	**Majeur** — restaure la joignabilité depuis les réseaux qui filtrent
2	Créer les 2 ROA manquants (`203.0.113.0/24`, `2001:db8:20::/48`), maxLength stricte	15 min	Supprime l'angle mort hijack d'origine
3	Resserrer la maxLength du ROA de `198.51.100.0/24` (/32 → /24)	5 min	Ferme le *forged-origin sub-prefix hijack* (RFC 9319)
4	Documenter les imports dans l'objet aut-num (cohérence IRR avec AS64511 et AS64497)	15 min	Hygiène registre, lisibilité pour les pairs
5	Documenter l'anti-usurpation (MANRS action 2) : état uRPF/ACL + test CAIDA Spoofer daté	À planifier	Complète le dossier MANRS/NIS2

Note attendue après les actions 1 à 3 : **A/A-** au prochain cycle d'évaluation.

Méthodologie et sources

Rapport d'EXEMPLE : l'ASN (RFC 5398), les préfixes IPv4 (RFC 5737) et IPv6 (RFC 3849) sont des ressources de documentation ; les constats sont illustratifs. Dans un rapport réel, les données sont collectées sur les informations publiquement observables : RIPE NCC — Routing Information Service (RIS) et RIPEstat Data API (identifiant d'application « sentinelle-routage ») ; validation RPKI : Routinator (NLnet Labs) ; registres IRR. Les rapports réels contiennent des informations issues du RIPE NCC, utilisées conformément à ses conditions. La note de santé reprend la grille publique du vérificateur sentinelle-routage.fr, appliquée aux mêmes données. Cycle : mensuel, ou sur événement notable.

Sentinelle Routage — service opéré par N&R Consulting. Contact : netrconsulting@gmail.com — https://sentinelle-routage.fr