

Intégrez RevealX 360 à Netskope

Publié: 2025-03-28

Cette intégration vous permet de configurer des capteurs ExtraHop pour ingérer des paquets depuis votre solution Netskope afin de détecter les menaces, de découvrir et de surveiller les appareils et d'obtenir des informations sur le trafic.



Note: Voir l'article de blog [»Intégration Zero Trust depuis ExtraHop et Netskope«](#) pour en savoir plus sur le fonctionnement de cette intégration.

Activer l'ingestion de paquets Netskope

Vous pouvez activer l'ingestion de paquets Netskope sur un ou plusieurs capteurs du système ExtraHop



Note: Nous vous recommandons d'activer cette intégration sur les capteurs déployés dans le même type de stockage cloud que celui que vous configurez pour Netskope Cloud TAP, qui reçoit des paquets dans Microsoft Azure, Google Cloud Platform (GCP) ou Amazon Web Services (AWS).

Avant de commencer

- Tu dois [configurer Cloud TAP](#) dans votre environnement Netskope.
 - Votre compte utilisateur doit avoir [Privilèges d'administration du système et des accès](#).
 - Pour chaque sonde ExtraHop qui ingèrera des paquets Netskope :
 - Votre sonde ExtraHop doit exécuter la version 9.4 ou ultérieure du firmware.
 - Votre sonde ExtraHop doit être dédiée à l'ingestion de paquets Netskope.
 - Tu dois [configurer au moins une interface](#) sur votre sonde ExtraHop qui spécifie un mode incluant l'encapsulation GENEVE.
 - Vous ne pouvez configurer aucune interface sur votre sonde ExtraHop pour le mode Surveillance.
1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
 3. Dans la section Paramètres réseau, cliquez sur **Connectivité**.
 4. Dans la section Paramètres d'ingestion de paquets, sélectionnez **Ingérer des paquets depuis Netskope**.
 5. Cliquez **Enregistrer**, puis revenez à la page principale.
 6. Dans la section Paramètres de l'appliance, cliquez sur **Des services**.
 7. Sélectionnez **Récepteur de clé de session TLS**.
 8. Cliquez **Enregistrer**, puis revenez à la page principale.
 9. Dans la section Configuration du système, cliquez sur **Capturez**.
 10. Sélectionnez **Activer le stockage des clés de session SSL**.
 11. Cliquez **Enregistrer**, puis revenez à la page principale.
 12. Dans la section Paramètres de l'appliance, cliquez sur **Configuration en cours d'exécution**.
 13. Cliquez **Modifier la configuration**, puis spécifiez les entrées suivantes sous `netskope_decap`:

```
"ssl_sharing_secret_timeout_msec": 300000,  
"ssl_test_agents_connected": true,  
"ssl_secret_map_size": 131072,  
"ssl_secret_map_max_secrets": 1048576,  
"ssl_secret_max_per_bucket": 32,
```

14. Cliquez **Mettre à jour**.

Prochaines étapes


- À partir de la page Actifs, vous pouvez [rechercher des appareils sur des capteurs](#) intégré à Netskope pour visualiser le trafic et les détections observés à partir des données Netskope.
- Connectez-vous aux paramètres d'administration sur le [RevealX Enterprise](#) ou [RevealX 360](#) console pour vérifier l'état des capteurs intégrés à Netskope.

Vérifiez l'état des capteurs intégrés à Netskope

Depuis la console RevealX 360, vous pouvez consulter l'état des capteurs activés pour l'ingestion de paquets Netskope.

Avant de commencer

- Votre compte utilisateur doit avoir [Privilèges d'administration système](#).

1. Connectez-vous à RevealX 360.
2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Intégrations**.
3. Cliquez sur **Netskope** tuile.

La page d'intégration de Netskope affiche les informations suivantes :

- Le nombre et le nom des capteurs connectés qui sont configurés pour ingérer des paquets Netskope.
 - Qu'une sonde soit en ligne ou hors ligne.
 - L'horodateur du dernier paquet reçu.
4. Optionnel : Cliquez **Accéder aux capteurs** pour afficher les détails de configuration de chaque capteur, activer ou désactiver des capteurs ou mettre à niveau le microprogramme du capteur.