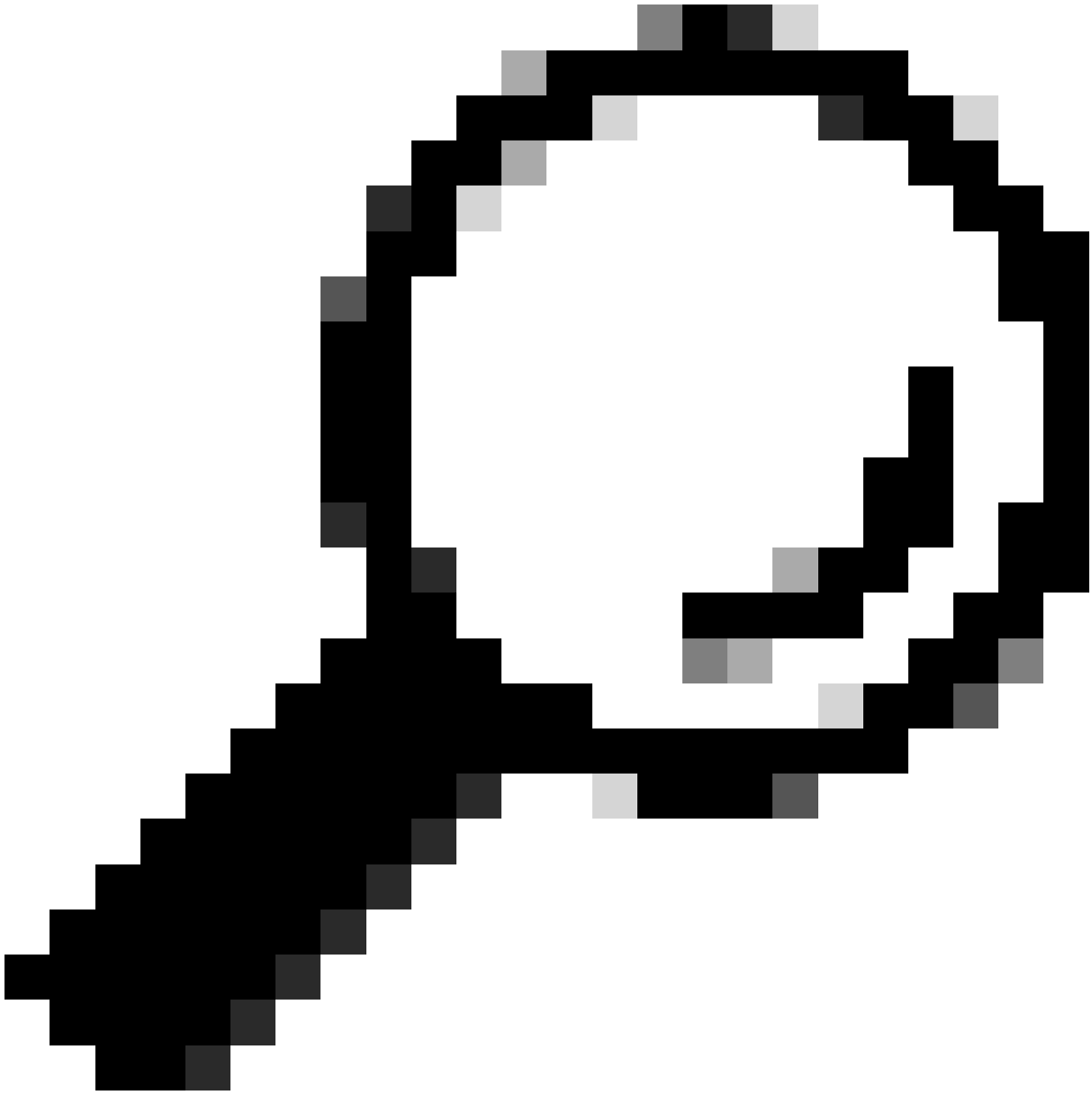
Guide de Secure Network Analytics Understanding External Connections

Table des matières

Introduction

Utilisez ce guide pour passer en revue les connexions externes requises pour que certaines fonctionnalités Secure Network Analytics fonctionnent rapidement. Ces connexions externes peuvent être des domaines ou des points de terminaison. Les domaines sont des noms utilisés pour identifier des ressources sur Internet, généralement des sites Web ou des services ; et les terminaux sont des périphériques ou des noeuds réels qui communiquent sur un réseau. Étant donné que ce guide est axé sur les services Web, ceux-ci seront affichés sous forme d'URL. Le tableau répertorie les URL de connexion externe par ordre alphabétique.



Conseil : Le tableau répertorie les URL de connexion externe par ordre alphabétique.

Connexions externes

URL de connexion externe	Objectif
https://analytics.int.obsrvbl.com	Utilisé par Secure Network Analytics pour l'échange de données télémétriques avec les

	services Secure Cloud Analytics.
https://api.apj.sse.itd.cisco.com	Requis par Cisco pour le transit de données vers Amazon Web Services (AWS) pour la région Asie-Pacifique, Japon et Chine (APJC). Utilisé lors du transfert d'alertes à Cisco XDR et également pour les mesures de service client.
https://api.eu.sse.itd.cisco.com	Requis par Cisco pour le transit de données vers Amazon Web Services (AWS) pour la région Europe (UE). Utilisé lors du transfert d'alertes à Cisco XDR et également pour les mesures de service client.
https://api-sse.cisco.com	Requis par Cisco pour le transfert de données vers Amazon Web Services (AWS) pour la région des

	États-Unis. Utilisé lors du transfert d'alertes à Cisco XDR et également pour les mesures de service client/de réussite.
https://apix.cisco.com	Utilisé par Secure Network Analytics pour la fonction de téléchargement direct de logiciels.
https://dex.sse.itd.cisco.com	Requis pour l'envoi et la collecte des indicateurs de réussite du client
https://est.sco.cisco.com	Requis pour l'envoi et la collecte des indicateurs de réussite du client
https://eventing-ingest.sse.itd.cisco.com	Requis pour l'envoi et la collecte des indicateurs de réussite du client
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	Requis par Threat Feed, utilisé pour les alertes et les observations Secure Network Analytics, lorsque l'option Analytics est

	activée.
https://id.cisco.com	Utilisé par Secure Network Analytics pour la fonction de téléchargement direct de logiciels.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	Requis par Threat Feed, utilisé pour les alertes et les observations Secure Network Analytics, lorsque l'option Analytics est activée.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	Requis par Threat Feed, utilisé pour les alertes et les observations Secure Network Analytics, lorsque l'option Analytics est activée.
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	Requis par le flux Secure Network Analytics Threat Intelligence, utilisé pour les alarmes et les événements de sécurité Secure Network Analytics. Cela nécessite la licence Secure Network

	Analytics Threat Intelligence Feed.
https://mx*.sse.itd.cisco.com	Requis pour l'envoi et la collecte des indicateurs de réussite du client
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	Permet d'accéder aux informations MITER pour les alertes lorsque Analytics est activé.
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	Permet d'accéder aux informations MITER pour les alertes lorsque Analytics est activé.
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	Permet d'accéder aux informations MITER pour les alertes lorsque Analytics est activé.
https://s3.amazonaws.com/onconfig/global-blacklist	Flux de menaces requis, utilisé pour les alertes et les observations Secure Network Analytics, lorsque l'analyse est activée.

https://sensor.anz-prod.obsrvbl.com	Requis par Cisco pour le transit de données vers Amazon Web Services (AWS) pour la région Asie-Pacifique, Japon et Chine (APJC). Utilisé lors du transfert d'alertes à Cisco XDR et également pour les mesures de service client.
https://sensor.eu-prod.obsrvbl.com	Requis par Cisco pour le transit de données vers Amazon Web Services (AWS) pour la région Europe (UE). Utilisé lors du transfert d'alertes à Cisco XDR et également pour les mesures de service client.
https://sensor.ext.obsrvbl.com	Requis par Cisco pour le transfert de données vers Amazon Web Services (AWS) pour la région des États-Unis. Utilisé lors du transfert

	d'alertes à Cisco XDR et également pour les mesures de service client.
smartreceiver.cisco.com	Utilisé pour accéder à Cisco Smart Software Licensing. Pour plus d'informations, reportez-vous au Smart Licensing Guide. D'autres licences hors ligne sont disponibles, si vous le souhaitez. Reportez-vous aux notes de version pour plus de détails.
https://software.cisco.com	Utilisé par Secure Network Analytics pour la fonction de téléchargement direct de logiciels.
https://www.cisco.com	Requis pour le domaine Cisco, qui est utilisé pour les licences Smart, le proxy cloud et les tests de connexion de pare-feu.

Additional Information

Pour savoir comment et pourquoi des connexions de domaine et de point d'extrémité spécifiques sont utilisées, reportez-vous aux rubriques suivantes :

- Cisco Secure Service Exchange (SSE)
- Téléchargements logiciels directs (bêta)
- Cadre ATT&CK® MITER
- Flux de menaces

Cisco Secure Service Exchange (SSE)

Les terminaux SSE sont utilisés pour le transfert de données vers Amazon Web Services (AWS), par Cisco pour les mesures de service client, et également pour le transfert d'alertes vers Cisco XDR. Ceux-ci varient
en fonction de la région et des hôtes. Ces points d'extrémité sont détectés dynamiquement à l'aide d'un mécanisme de découverte de service fourni par le connecteur SSE. Lors de la publication des détections sur Cisco XDR, Secure Network Analytics tente de découvrir un service intitulé « xdr-data-platform » et son point d'extrémité API « Events ».

Région et hôtes

Selon la région des environnements de production, les hôtes sont les suivants.

USA :

- https://api-sse.cisco.com
- https://sensor.ext.obsrvbl.com

UE :

- https://api.eu.sse.itd.cisco.com
- https://sensor.eu-prod.obsrvbl.com

APJC:

- https://api.apj.sse.itd.cisco.com
- https://sensor.anz-prod.obsrvbl.com

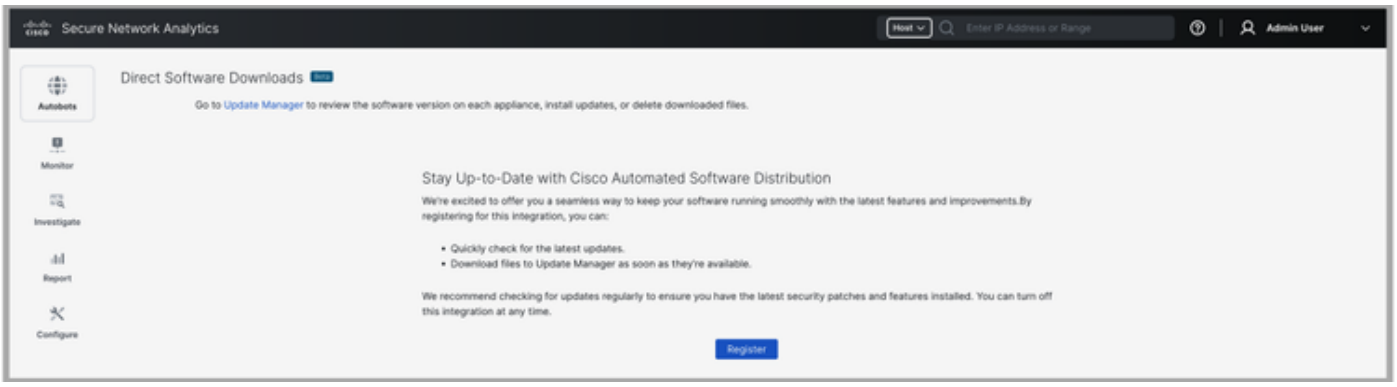
Téléchargements logiciels directs (bêta)

Les connexions suivantes sont utilisées par la fonction de téléchargement direct de logiciels :

- https://apix.cisco.com
- https://software.cisco.com

- https://id.cisco.com

Pour utiliser cette nouvelle fonctionnalité afin de télécharger des logiciels et des fichiers de mise à jour de correctifs directement sur votre gestionnaire de mise à jour, assurez-vous que vous vous êtes inscrit à l'aide de votre ID utilisateur cisco.com (CCOID).
1. Connectez-vous au gestionnaire.
2. Dans le menu principal, choisissez Configure > Global > Central Management.
3. Cliquez sur l'onglet Gestionnaire de mise à jour.
4. Cliquez sur le lien Direct Software Downloads pour ouvrir la page d'inscription.
5. Cliquez sur le bouton Register pour lancer le processus d'enregistrement.



6. Cliquez sur le lien fourni.
7. La page Activate Your Device (Activer votre périphérique) s'affiche. Cliquez sur Next pour continuer.
8. Connectez-vous avec votre ID utilisateur cisco.com (CCOID).
9. Vous recevrez un message « Device Activated » une fois votre activation terminée.
10. Retournez à la page Téléchargements logiciels directs de votre gestionnaire et cliquez sur Continuer.
11. Cliquez sur les liens des contrats de licence d'utilisation et de licence K9 pour lire et accepter les conditions. Une fois les conditions acceptées, cliquez sur Continue.

Pour plus d'informations sur les téléchargements logiciels directs, contactez l'assistance Cisco

Cadre ATT&CK® MITER

Le cadre MITER ATT&CK® est une base de connaissances accessible au public sur les tactiques et techniques de l'adversaire, basée sur des observations du monde réel. Lorsque vous avez activé l'analytique dans Secure Network Analytics, les tactiques et techniques MITER vous aident à détecter et à contrer les menaces de cybersécurité.

To make sure Analytics is enabled, choose **Configure** > **Detection** > **Analytics** from the main menu, then click *Analytics On* Analytics On .

Les connexions suivantes permettent à Secure Network Analytics d'accéder aux informations

MITER
pour les alertes :

- https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
- https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobileattack.json
- https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterpriseattack.json

Flux de menaces

Le flux Cisco Secure Network Analytics Threat (anciennement Stealthwatch Threat Intelligence Feed) fournit des données provenant du flux global Threat Feed sur les menaces qui pèsent sur votre réseau. Le flux est mis à jour fréquemment et inclut des adresses IP, des numéros de port, des protocoles, des noms d'hôtes et des URL connus pour être utilisés pour des activités malveillantes. Les groupes d'hôtes suivants sont inclus dans le flux : serveurs de commande et de contrôle, bogons et Tors.

Pour activer Threat Feed dans Central Management, suivez les instructions de l'aide.

1. Connectez-vous à votre manager principal.
2. Sélectionnez Configure > Global > Central Management.
3. Cliquez sur l'icône (Aide). Sélectionnez Aide.
4. Sélectionnez Appliance Configuration > Threat Feed.

Pour plus d'informations sur Threat Feed, reportez-vous au Guide de configuration du système.

Contacter le support

Si vous avez besoin d'une assistance technique, effectuez l'une des opérations suivantes :

- Contactez votre partenaire Cisco local
- Contacter le support Cisco
- Pour ouvrir un dossier par le Web : http://www.cisco.com/c/en/us/support/index.html
- Pour l'assistance téléphonique : 1-800-553-2447 (ÉTATS-UNIS)
- Pour les numéros d'assistance internationaux : https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.