Premiers pas avec Snort 3 : Politiques d'analyse de réseau

Ce chapitre présente les principes de base des politiques d'analyse de réseau, les conditions préalables et la manière de gérer les politiques d'analyse de réseau. Il fournit également des informations sur la création de politiques d'analyse de réseau personnalisées et les paramètres de politique d'analyse de réseau.

Aperçu des politiques d'analyse de réseau

Les *politiques d'analyse de réseau* régissent de nombreuses options de prétraitement du trafic et sont appelées par les paramètres avancés de votre politique de contrôle d'accès. Le prétraitement lié à l'analyse de réseau a lieu après la mise en correspondance Security Intelligence et le déchiffrement SSL, mais avant le début de l'intrusion ou de l'inspection des fichiers.

Par défaut, le système utilise la politique d'analyse de réseau *Sécurité et connectivité équilibrées* pour prétraiter tout le trafic géré par une politique de contrôle d'accès. Cependant, vous pouvez choisir une autre politique d'analyse de réseau par défaut pour effectuer ce prétraitement. Pour votre commodité, le système offre un choix entre plusieurs politiques d'analyse de réseau non modifiables, qui sont réglées par Cisco Talos Intelligence Group (Talos). Vous pouvez également créer une politique d'analyse de réseau personnalisée avec des paramètres de prétraitement personnalisés.

Astuces Les politiques d'analyse de prévention des intrusions et de réseau fournies par le système portent le même nom, mais contiennent des configurations différentes. Par exemple, la politique d'analyse de réseau équilibrée, sécurité et connectivité, et la politique de prévention des intrusions, sécurité et connectivité équilibrées fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles de prévention des intrusions. Cependant, la politique d'analyse de réseau régit principalement les options de prétraitement, alors que la politique de prévention de prévention des intrusions régit principalement les règles de prévention des intrusions. Les politiques d'analyse de réseau et de prévention des intrusions travaillent ensemble pour examiner votre trafic.

Vous pouvez également adapter les options de prétraitement du trafic à des zones de sécurité, à des réseaux et à des VLAN spécifiques en créant plusieurs politiques d'analyse de réseau personnalisées, puis en les affectant au prétraitement du trafic. (Notez que ASA FirePOWER ne peut pas restreindre le prétraitement par VLAN.)

Gérer les politiques d'analyse du réseau

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Sous votre nom d'utilisateur dans la barre d'outils, le système affiche une arborescence des domaines disponibles. Pour changer de domaine, choisissez le domaine auquel vous souhaitez accéder.

Procédure

Étape 1 Choisissez un des chemins d'accès suivants pour accéder à la politique d'analyse de réseau.

- **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux**
- **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**
- **Policies (Politiques)** > **Intrusion (Intrusions)** > **Network Analysis Policies (Politiques d'analyse de réseau)**

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Gérer vos politiques d'analyse du réseau

- Compare (Comparer) : Cliquez sur **Compare Policies (Comparer les politiques)**; consultez *Comparer les politiques* dans le *Guide de configuration Cisco Secure Firewall Management Center*.

  Remarque Vous pouvez comparer uniquement les politiques Snort 2.

- Create (créer) : Si vous souhaitez créer une nouvelle politique d'analyse de réseau, cliquez sur **Create Policy** (Créer une politique).

Deux versions de la politique d'analyse de réseau sont créées, une **version Snort 2 et une versionSnort 3**.

- Pour la version Snort 2, consultez *Création de politique d'analyse de réseau personnalisée pour Snort 2* dans le *Guide de configuration de Cisco Secure Firewall Management Center*.
- Pour la version Snort 3, consultez Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 6.

- Delete (supprimer) : Si vous souhaitez supprimer une politique d'analyse de réseau, cliquez sur l'icône **Delete** (supprimer), puis confirmez que vous souhaitez supprimer la politique. Vous ne pouvez pas supprimer une politique d'analyse de réseau si une politique de contrôle d'accès y fait référence.

  Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

- Edit (modifier) : Si vous souhaitez modifier une politique d'analyse de réseau existante, cliquez sur l'icône **Edit** (modifier).

  Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

- Report (rapport) : Cliquez sur l'icône **Report** (rapport); Consultez la section *Génération des rapports sur les politiques actuelles* dans le *Guide de configuration de Cisco Secure Firewall Management Center*.

Définitions et terminologies pour la politique d'analyse de réseau Snort 3

Le tableau suivant dresse la liste des concepts et termes de Snort 3 utilisés dans la politique d'analyse de réseau.

Tableau 1 : Définitions et terminologies pour la politique d'analyse de réseau Snort 3

Terme	Description
Inspecteurs	Les inspecteurs sont des modules d'extension qui traitent les paquets (semblables au préprocesseur Snort 2).

Terme	Description
Inspecteur de classeur	L'inspecteur Binder définit le flux lorsqu'il faut accéder à un inspecteur particulier et prendre en compte. Lorsque le trafic correspond aux conditions définies dans l'inspecteur de classeur, ce n'est qu'alors que les valeurs/configurations de cet inspecteur prennent effet. Pour en savoir plus, consultez la section *Inspecteur de classeur* dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 6.
Inspecteurs Singleton	Les inspecteurs Singleton contiennent une instance. Ces inspecteurs ne prennent pas en charge l'ajout d'instances, comme les inspecteurs Multiton. Les paramètres de l'inspecteur Singleton sont appliqués à l'ensemble du trafic correspondant à cet inspecteur et non à un segment de trafic spécifique. Pour en savoir plus, consultez la section *Inspecteurs Singleton* dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 6.
Inspecteurs Multiton	Les inspecteurs Multiton contiennent plusieurs instances que vous pouvez configurer selon vos besoins. Ces inspecteurs prennent en charge la configuration de paramètres en fonction de conditions spécifiques, telles que le réseau, le port et le VLAN. Un ensemble de paramètres pris en charge s'appelle une instance. Pour en savoir plus, consultez *Inspecteurs Multiton* dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 6.
Schéma	Le fichier de schéma est basé sur la spécification OpenAPI JSON et valide le contenu que vous chargez ou téléchargez. Vous pouvez télécharger le fichier de schéma et l'ouvrir à l'aide de n'importe quel éditeur JSON tiers, tel que l'éditeur Swagger. Le fichier de schéma vous aide à identifier les paramètres pouvant être configurés pour les inspecteurs ainsi que les valeurs autorisées, la plage et les modèles acceptés correspondants. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 13.

Terme	Description
Exemple de fichier	Il s'agit d'un modèle préexistant qui contient des exemples de configuration pour vous aider à configurer les inspecteurs. Vous pouvez consulter les exemples de configuration inclus dans le fichier exemple et apporter les modifications nécessaires. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 13.
Configuration complète	Vous pouvez télécharger la configuration complète de l'inspecteur dans un seul fichier. Tous les renseignements concernant la configuration de l'inspecteur sont disponibles dans ce fichier. La configuration complète est une configuration fusionnée de la configuration par défaut (déployée dans le cadre des mises à jour des LSP par Cisco Talos) et des configurations de l'inspecteur Politique d'analyse de réseau (NAP) personnalisé. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 13.
Configuration remplacée	Dans la **version Snort 3** de la page de politiques d'analyse de réseau : • Sous **Actions** > **Upload** (Actions > Téléverser), vous pouvez cliquer sur **Overridden Configuration** (configuration remplacée) pour téléverser le fichier JSON qui contient la configuration remplacée. • Sous **Actions** > **Télécharger**, vous pouvez cliquer sur **Overridden Configuration** (configuration remplacée) pour télécharger la configuration de l'inspecteur qui a été remplacée. Si vous n'avez remplacé aucune configuration d'inspecteur, cette option est désactivée. Lorsque vous remplacez la configuration de l'inspecteur, cette option est activée automatiquement pour vous permettre d'effectuer le téléchargement. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 13.

Sujets connexes

Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 6
Personnaliser la politique d'analyse de réseau, à la page 13
Mappage de la stratégie d'analyse du réseau, à la page 11

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Défense contre les menaces.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

Création d'une politique d'analyse de réseau personnalisée pour Snort 3

La politique d'analyse de réseau par défaut est réglée pour les exigences de réseau typiques et des performances optimales. Généralement, la politique d'analyse de réseau par défaut répond à la plupart des exigences du réseau et vous n'aurez peut-être pas besoin de la personnaliser. Toutefois, lorsque vous avez des besoins particuliers en matière de réseau ou lorsque vous faites face à des problèmes de rendement, la politique d'analyse de réseau par défaut peut être personnalisée. Notez que la personnalisation de la politique d'analyse de réseau est une configuration avancée qui ne doit être effectuée que par des utilisateurs avancés ou par le service d'assistance Cisco.

La configuration de la politique d'analyse de réseau pour Snort 3 est un modèle basé sur les données, qui repose sur JSON et le schéma JSON. Le schéma est basé sur la spécification OpenAPI et vous aide à obtenir un aperçu des inspecteurs, des paramètres, des types de paramètres et des valeurs valides pris en charge. Les inspecteurs Snort 3 sont des modules d'extension qui traitent les paquets (comme le préprocesseur Snort 2). La configuration de la politique d'analyse de réseau est disponible pour téléchargement au format JSON.

Dans Snort 3, la liste des inspecteurs et des paramètres ne correspond pas exactement à la liste des préprocesseurs et des paramètres de Snort 2. De plus, le nombre d'inspecteurs et de paramètres disponibles dans centre de gestion est un sous-ensemble des inspecteurs et des paramètres pris en charge par Snort 3. Consultez https://snort.org/snort3 pour de plus amples renseignements sur Snort 3. Consultez https://www.cisco.com/go/snort3-inspectors pour en savoir plus sur les inspecteurs disponibles dans centre de gestion.

Remarque

- Lors de la mise à niveau de centre de gestion à la version 7.0, les modifications effectuées dans la version Snort 2 de la politique d'analyse de réseau ne sont pas migrées vers Snort 3 après la mise à niveau.
- Contrairement à la politique de prévention des intrusions, il n'y a pas d'option pour synchroniser les paramètres de politique d'analyse de réseau Snort 2 avec Snort 3.

Mises à jour de l'inspecteur par défaut

Les mises à jour du progiciel de sécurité allégé (LSP) peuvent contenir de nouveaux inspecteurs ou des modifications de plages d'entiers pour les configurations d'inspecteurs existantes. À la suite de l'installation d'un LSP, de nouveaux inspecteurs ou des plages mises à jour seront disponibles sous la section **Inspecteurs** dans la **version Snort 3** de votre politique d'analyse de réseau.

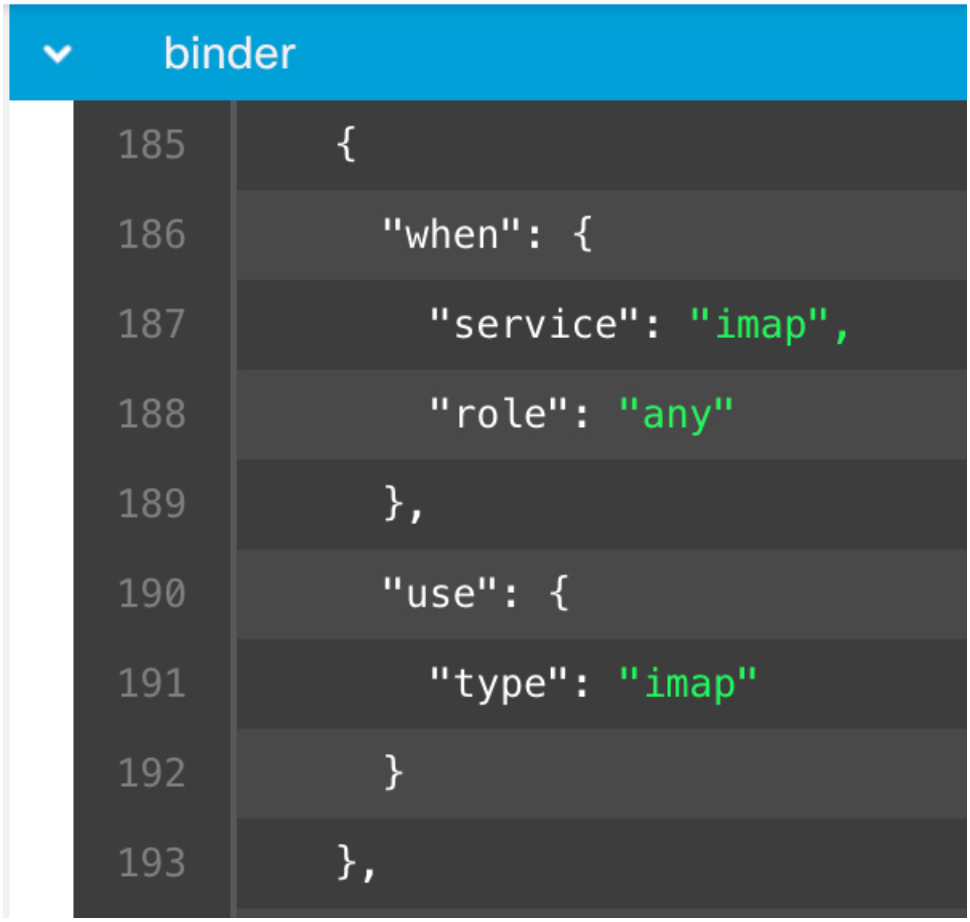
Inspecteur Binder

L'inspecteur Binder définit le flux lorsqu'il faut accéder à un inspecteur particulier et prendre en compte. Lorsque le trafic correspond aux conditions définies dans l'inspecteur Binder, alors seulement les valeurs ou configurations de cet inspecteur entrent en vigueur. Par exemple :

Pour l'inspecteur *imap*, le binder définit la condition suivante lorsqu'il doit être accédé. C'est lorsque :

- Le service est égal à imap.
- Le rôle est égal à Tout.

Si ces conditions sont remplies, utilisez le type imap.



Inspecteurs Singleton

Les inspecteurs Singleton ne contiennent qu'une seule instance. Ces inspecteurs ne prennent pas en charge l'ajout d'instances, comme les inspecteurs Multiton. Les paramètres de l'inspecteur Singleton sont appliqués à l'ensemble du trafic et non à un segment de trafic en particulier.

Par exemple :

```
{
   "normalizer":{
      "enabled":true,
```

```
      "type":"singleton",
      "data":{
         "ip4":{
            "df":true
         }
      }
   }
}
```

Inspecteurs Multiton

Les inspecteurs Multiton contiennent plusieurs instances que vous pouvez configurer selon vos besoins. Ces inspecteurs prennent en charge la configuration de paramètres en fonction de conditions spécifiques, telles que le réseau, le port et le VLAN. Un ensemble de paramètres pris en charge s'appelle une instance. Il existe une instance par défaut, et vous pouvez également ajouter des instances supplémentaires en fonction de conditions spécifiques. Si le trafic correspond à cette condition, les paramètres de cette instance sont appliqués. Sinon, les paramètres de l'instance par défaut sont appliqués. En outre, le nom de l'instance par défaut est le même que le nom de l'inspecteur.

Pour un inspecteur Multiton, lorsque vous téléversez la configuration de l'inspecteur remplacée, vous devez également inclure ou définir une condition binder correspondante (conditions dans lesquelles l'accès à l'inspecteur ou l'utilisation de celui-ci doit être effectué) pour chaque instance du fichier JSON, sinon le téléversement produira une erreur. Vous pouvez également créer de nouvelles instances, mais veillez à inclure une condition binder pour chaque nouvelle instance que vous créez pour éviter les erreurs.

Par exemple :

- L'inspecteur Multiton, où l'instance par défaut est modifiée.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- L'inspecteur Multiton où l'instance par défaut et le binder par défaut sont modifiés.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
```

```
        "enabled":true,
        "rules":[
           {
              "use":{
                 "type":"http_inspect"
              },
              "when":{
                 "role":"any",
                 "ports":"8080",
                 "proto":"tcp",
                 "service":"http"
              }
           }
        ]
     }
}
```

- Un inspecteur Multiton où une instance personnalisée et un binder personnalisés sont ajoutés.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect1",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect",
               "name":"http_inspect1"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

Sécurité du Protocole industriel commun (CIP)

La sécurité CIP (Common Industrial Protocol) est un ensemble d'extensions du protocole CIP qui permet le fonctionnement sûr des périphériques. Il fournit également une communication à sécurité intégrée entre différents nœuds sur un réseau CIP.

Le protocole sécurité CIP comprend deux composants principaux :

- Segments CIP Safety : utilisés dans les messages Forward Open pour échanger des paramètres de sécurité pour la session de sécurité suivante.

- Messages CIP Safety : utilisés pour échanger des informations de sécurité réelles.

L'inspecteur CIP détecte et identifie :

- CIP en tant que service et client
- Charges utiles, telles que la lecture CIP, l'administration CIP, l'infrastructure CIP et l'écriture CIP

  L'inspecteur CIP peut analyser les segments CIP et détecter les segments CIP Safety dans les demandes Forward Open.

Pour tester la fonction CIP Safety, vous devez activer l'inspecteur CIP. Consultez Détection et blocage des segments de sécurité dans les paquets CIP, à la page 10.

Détection et blocage des segments de sécurité dans les paquets CIP

Scénario : pour détecter et bloquer les segments CIP Safety tout en autorisant d'autres paquets CIP :

- Créez une politique d'analyse de réseau personnalisée appelée **cip_safety**.
- Créez des règles de contrôle d'accès dans votre politique de contrôle d'accès pour bloquer la fonction CIP Safety et autoriser tous les autres paquets.

Pour tester la fonction CIP Safety, activez l'inspecteur CIP dans le centre de gestion et affectez-le à une politique de contrôle d'accès.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur la **version Snort 3** de la politique d'analyse de réseau **cip_safety** que vous avez créée.

Étape 3 Sous **Inspecteurs**, cliquez sur **cip** pour le développer.

La configuration par défaut s'affiche dans la colonne de gauche et la configuration remplacée s'affiche dans la colonne de droite sous l'inspecteur.

Étape 4 sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône **Edit Inspector** (modifier l'inspecteur) et modifiez le champ « enabled » dans le champ **cip** de false (par défaut) à true.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Pour affecter l'inspecteur **cip** à la politique de contrôle d'accès, choisissez **Policies** > **Access Control** > **Edit** (modifier le contrôle d'accès des politiques), puis l'option **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 8 Cliquez sur **Modifier** ( )à côté de **Politiques d'analyse du réseau et de prévention des intrusions**.

Étape 9 Dans la fenêtre **Network Analysis and Intrusion Policies** (Politiques d'analyse du réseau et de prévention des intrusions), choisissez la politique de contrôle d'accès **cip_safety** que vous avez créée dans la liste déroulante **Default Network Analysis Policy** (Politique d'analyse du réseau par défaut).

L'inspecteur CIP est maintenant activé dans le centre de gestion. Vous pouvez créer les règles de contrôle d'accès personnalisées pour bloquer les paquets CIP Safety et autoriser tous les autres paquets CIP.

Étape 10 Après avoir envoyé le trafic en direct contenant les flux de paquets CIP Safety, accédez à **Connection Events** (Événements de connexion) pour vérifier que la charge utile est la charge utile attendue qui contient les journaux de paquets CIP Safety pour le scénario de détection et de blocage comme mentionné dans cette procédure. **CIP** est détecté en tant que protocole d'application et client (consultez les champs **Application Protocol** (Protocole d'application) et **Client** (client) et **CIP Safety** (CIP Safety) est affiché sous le champ **Web Application** (Application Web).

Mappage de la stratégie d'analyse du réseau

Pour les politiques d'analyse de réseau, Cisco Talos fournit des informations de mappage, qui sont utilisées pour trouver la version Snort 2 correspondante des politiques pour la version Snort 3.

Ce mappage garantit que les politiques de la version Snort 3 contiennent les politiques équivalentes de la version Snort 2.

Afficher le mappage de la politique d'analyse des réseaux

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur**Mappage NAP**.

Étape 3 Développez la flèche **Afficher les mappages**.

Les politiques d'analyse de réseau Snort 3 qui sont automatiquement mappées à une politique équivalente Snort 2 s'affichent.

Étape 4 Cliquez sur **OK**.

Créer une politique d'analyse de réseau

Toutes les politiques d'analyse de réseau existantes sont disponibles dans centre de gestion avec leurs versions Snort 2 et Snort 3 correspondantes. Lorsque vous créez une nouvelle politique d'analyse de réseau, elle est créée avec la version 2 et la version Snort 3.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur **Créer une politique**.

Étape 3 Remplissez les champs **Nom** et **Description**.

Étape 4 Choisir le **mode d'inspection** parmi les choix disponibles.

- **Détection**
- **Prévention**

Étape 5 Sélectionnez une **politique de base** et cliquez sur **Save**(Enregistrer).

Remarque Configurez la politique d'analyse de réseau (NAP) en mode **prévention** si vous utilisez Snort 3 et le déchiffrement SSL ou l'identité du serveur TLS.

La nouvelle politique d'analyse de réseau est créée avec ses **versions Snort 2** et **Snort 3**correspondantes.

Modifier la politique d'analyse de réseau

Vous pouvez modifier la politique d'analyse de réseau pour changer son nom, sa description ou sa politique de base.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur **Edit** (Modifier) pour changer le nom, la description, le mode d'inspection ou la politique de base.

Remarque Si vous modifiez le nom, la description, la politique de base et le mode d'inspection de la politique d'analyse de réseau, les modifications sont appliquées aux versions Snort 2 et Snort 3. Si vous souhaitez modifier le mode d'inspection pour une version spécifique, vous pouvez le faire à partir de la page de politique d'analyse de réseau pour cette version respective.

Étape 3 Cliquez sur **Save** (enregistrer).

Recherchez un inspecteur dans la page des politiques d'analyse de réseau.

Dans la version Snort 3 de la page de politique d'analyse de réseau, vous devrez peut-être rechercher un inspecteur en saisissant tout texte pertinent dans la barre de recherche.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Saisissez le nom d'un inspecteur ou tout autre texte pertinent à rechercher dans la barre de **recherche**.

Tous les inspecteurs correspondant au texte que vous recherchez s'affichent.

Par exemple, si vous saisissez `pop`, l'inspecteur pop et l'inspecteur de classeurs s'affichent comme des résultats correspondants à l'écran.

Sujets connexes

Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 22
Afficher la liste des inspecteurs avec remplacements, à la page 19

Définitions et terminologies pour la politique d'analyse de réseau Snort 3 , à la page 3
Personnaliser la politique d'analyse de réseau, à la page 13
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 17

Copier la configuration de l'inspecteur

Vous pouvez copier la configuration de l'inspecteur pour la version Snort 3 de la politique d'analyse de réseau en fonction de vos besoins.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis dont vous souhaitez copier la configuration.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 4 Cliquez sur l'icône **Copier dans le presse-papier** pour copier la configuration de l'inspecteur dans le presse-papier de l'un des éléments suivants ou des deux.

- **Configuration par défaut** dans la colonne de gauche
- **Configuration remplacée** dans la colonne de droite

Étape 5 Collez la configuration de l'inspecteur copiée dans un éditeur JSON pour apporter les modifications nécessaires.

Sujets connexes

Personnaliser la politique d'analyse de réseau, à la page 13

Personnaliser la politique d'analyse de réseau

Vous pouvez personnaliser la version Snort 3 de la politique d'analyse de réseau en fonction de vos besoins.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

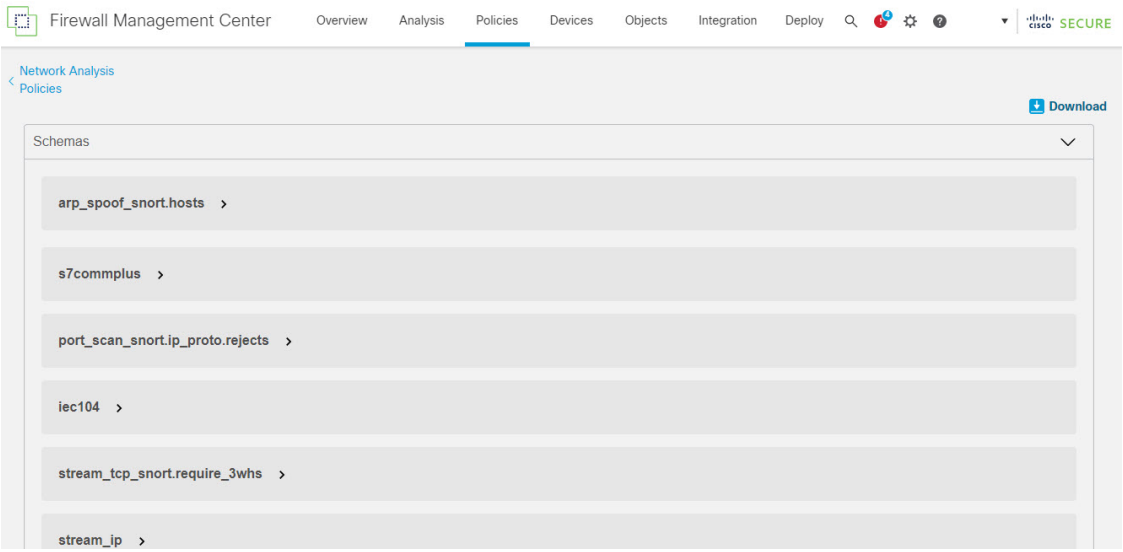
Étape 3 Cliquez sur le menu déroulant **Actions** .

Les options suivantes s'affichent.

- Afficher le schéma
- Télécharger un schéma, télécharger un exemple de fichier ou de modèle
- Télécharger la configuration complète
- Télécharger la configuration remplacée

- Téléverser la configuration remplacée

Étape 4 Cliquez sur **Afficher le schéma** pour ouvrir le fichier de schéma directement dans un navigateur.



Étape 5 Vous pouvez télécharger le fichier de schéma, un exemple de fichier/modèle, la configuration complète ou la configuration remplacée au besoin.

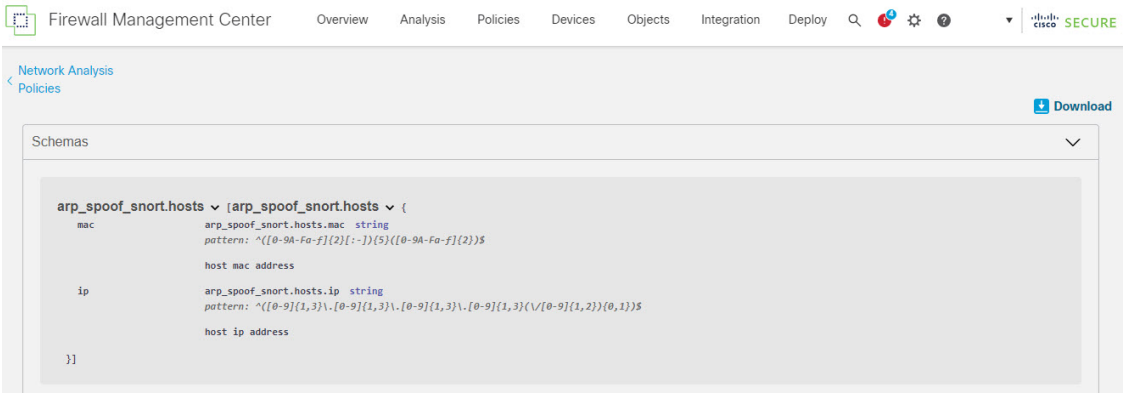
Ces options vous donnent un aperçu des valeurs autorisées, de la plage et des modèles, des configurations de l'inspecteur existantes et par défaut et des configurations de l'inspecteur remplacées.

a) Cliquez sur **Télécharger le schéma** pour télécharger le fichier de schéma.

Le fichier de schéma valide le contenu que vous chargez ou téléchargez. Vous pouvez télécharger le fichier de schéma et l'ouvrir à l'aide de n'importe quel éditeur JSON tiers. Le fichier de schéma vous aide à identifier les paramètres pouvant être configurés pour les inspecteurs ainsi que les valeurs autorisées, la plage et les modèles acceptés correspondants.

Par exemple, pour l'inspecteur *arp_spoof_snort*, vous pouvez configurer les hôtes. Les hôtes comprennent les valeurs d'adresses *mac* et *ip*. Le fichier de schéma présente le modèle accepté suivant pour ces valeurs.

- **mac** – `pattern: ^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **IP** – `modèle : ^([0-9] {1,3}.[0-9] {1,3}.[0-9] {1,3}.[0-9] {1,3}( /[0-9] {1,2}) {0,1})$`



Vous devez fournir les valeurs, la plage et les modèles conformément à ceux acceptés dans le fichier de schéma pour pouvoir remplacer la configuration de l'inspecteur avec succès, sinon, vous obtenez un message d'erreur.

b) Cliquez sur **télécharger un exemple de fichier / modèle** pour utiliser un modèle préexistant qui contient des exemples de configuration pour vous aider à configurer les inspecteurs.

Vous pouvez consulter les exemples de configuration inclus dans le fichier exemple et apporter les modifications nécessaires.

c) Cliquez sur **Télécharger la configuration complète** pour télécharger les configurations complètes de l'inspecteur dans un seul fichier JSON.

Au lieu de développer les inspecteurs séparément, vous pouvez télécharger la configuration complète pour rechercher les informations dont vous avez besoin. Tous les renseignements concernant la configuration de l'inspecteur sont disponibles dans ce fichier.

d) Cliquez sur **Chargement de la configuration remplacée** pour télécharger la configuration de l'inspecteur qui a été remplacée.

Étape 6 Pour remplacer la configuration existante, suivez les étapes.

Vous pouvez choisir de remplacer une configuration de l'inspecteur des manières suivantes.

- Apportez des modifications en ligne pour un inspecteur directement dans centre de gestion. Consultez la section **Modifier en ligne un inspecteur pour remplacer la configuration** dans le chapitre **Premiers pas avec les politiques d'analyse de réseau** du *Guide de configuration Snort 3 de Cisco Secure Firewall Management Center*.
- Continuez à suivre la procédure actuelle qui consiste à utiliser le menu déroulant**Actions**pour téléverser le fichier de configuration remplacé.

Si vous avez choisi d'effectuer les modifications en ligne directement dans centre de gestion, vous n'avez pas besoin de suivre plus avant la procédure actuelle. Sinon, vous devez suivre cette procédure entièrement.

a) Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez remplacer la configuration par défaut.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Vous devrez peut-être rechercher un inspecteur en saisissant tout texte pertinent dans dans la barre de recherche.

b) Cliquez sur l'icône **Copier dans le presse-papier** pour copier la configuration de l'inspecteur par défaut dans le presse-papier.
c) Créez un fichier JSON et collez-y la configuration par défaut.
d) Conservez la configuration de l'inspecteur que vous souhaitez remplacer et supprimez toutes les autres configurations et instances du fichier JSON.

   Vous pouvez également utiliser le **fichier ou le modèle exemple** pour comprendre comment remplacer la configuration par défaut. Il s'agit d'un exemple de fichier qui comprend des extraits de code JSON expliquant comment personnaliser la politique d'analyse de réseau pour Snort 3.

e) Apporter des modifications à la configuration de l'inspecteur au besoin.

   Validez les modifications et assurez-vous qu'elles sont conformes au fichier de schéma. Pour les inspecteurs multiton, assurez-vous que les conditions de classeur pour toutes les instances sont incluses dans le fichier JSON. Pour obtenir de plus amples renseignements, consultez *Inspecteurs Multiton* dans la rubrique **Création de politique d'analyse de réseau personnalisée pour Snort 3** dans le *Guide de configuration de Snort 3 de Cisco Secure Firewall Management Center*.

f) Si vous copiez d'autres configurations de l'inspecteur par défaut, ajoutez cette configuration de l'inspecteur au fichier existant qui contient la configuration remplacée.

   Remarque La configuration de l'inspecteur copiée doit être conforme aux normes JSON.

g) Enregistrez le fichier de configuration remplacé sur votre système.

Étape 7 dans le menu déroulant **Actions**, choisissez Upload Overridden Configuration pour téléverser le fichier JSON qui contient la configuration remplacée.

Mise en garde Chargez uniquement les modifications dont vous avez besoin. Vous ne devez pas télécharger la configuration complète, car cela rend les remplacements persistants et, par conséquent, toute modification ultérieure à la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée.

Vous pouvez faire glisser et déposer un fichier ou cliquer pour naviguer jusqu'au fichier JSON enregistré dans votre système qui contient la configuration de l'inspecteur remplacée.

- **Fusionner les remplacements de l'inspecteur** : Le contenu du fichier téléversé est fusionné avec la configuration existante en l'absence d'inspecteur commun. S'il y a présence d'inspecteurs communs, le contenu du fichier téléversé (pour les inspecteurs communs) prévaut sur le contenu précédent et remplace la configuration pour ces inspecteurs.
- **Remplacer les remplacements de l'inspecteur** : supprime tous les remplacements précédents et les remplace par le nouveau contenu du fichier téléversé.

  Attention Choisir cette option supprime tous les remplacements précédents. Faites un choix avisé avant de remplacer la configuration à l'aide de cette option.

Si une erreur se produit lors du chargement des inspecteurs remplacés, elle est visible dans la fenêtre contextuelle **Upload Overridden Configuration File** (téléverser le fichier de configuration remplacé). Vous pouvez également télécharger le fichier avec l'erreur, corriger l'erreur et téléverser de nouveau le fichier.

Étape 8 Dans la fenêtre contextuelle **Upload Overridden Configuration File** (téléverser le fichier de configuration remplacé), cliquez sur **Importer** pour téléverser la configuration de l'inspecteur remplacée.

Après avoir téléversé la configuration de l'inspecteur remplacée, vous verrez une icône jaune à côté de l'inspecteur qui signifie qu'il s'agit d'un inspecteur remplacé.

En outre, la colonne **Overridden Configuration** (Configuration remplacée) sous l'inspecteur affiche la valeur remplacée.

Vous pouvez également afficher tous les inspecteurs remplacés en cochant la case **Afficher les remplacements uniquement** à côté de la barre de recherche.

Remarque Assurez-vous de toujours télécharger la configuration remplacée, d'ouvrir le fichier JSON et d'ajouter les nouvelles modifications ou remplacements aux configurations de l'inspecteur à ce fichier. Cette action est nécessaire pour ne pas perdre les anciennes configurations remplacées.

Étape 9 (Facultatif) Effectuez une sauvegarde du fichier de configuration remplacé sur votre système avant d'apporter de nouvelles modifications à la configuration de l'inspecteur.

Astuces Nous vous recommandons d'utiliser la sauvegarde de temps à autre lorsque vous remplacez la configuration de l'inspecteur.

Sujets connexes

Rétablir la configuration par défaut de la configuration remplacée, à la page 19
Afficher la liste des inspecteurs avec remplacements, à la page 19
Recherchez un inspecteur dans la page des politiques d'analyse de réseau., à la page 12
Copier la configuration de l'inspecteur , à la page 13

Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration

Pour la version Snort 3 de la politique d'analyse de réseau, vous pouvez apporter une modification en ligne à la configuration de l'inspecteur afin de remplacer la configuration selon vos besoins.

Vous pouvez également utiliser le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé. Consultez Personnaliser la politique d'analyse de réseau, à la page 13 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez remplacer le paramètre par défaut.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 4 Sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône **Edit Inspector** (Modifier l'inspecteur) (en forme de crayon) pour apporter des modifications à la configuration de l'inspecteur.

La fenêtre contextuelle Override Configuration (remplacer la configuration) s'affiche dans laquelle vous pouvez apporter les modifications nécessaires.

Remarque
- Conserver seulement les paramètres à remplacer. Si vous conservez la même valeur dans un paramètre, ce champ devient rémanent. Cela signifie que, si Talos modifie ultérieurement ce paramètre, la valeur actuelle est conservée.
- Si vous ajoutez ou supprimez toute instance personnalisée, assurez-vous d'ajouter ou supprimer une règle de classeur pour cette instance dans le classeur inspecteur.

Étape 5 Cliquez sur **OK**.

S'il y a des erreurs selon les normes JSON, un message d'erreur s'affiche.

Étape 6 Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Si les modifications sont conformes à la spécification de schéma OpenAPI, centre de gestion vous permet d'enregistrer la configuration, sinon, la fenêtre contextuelle **d'erreur lors de l'enregistrement de la configuration remplacée** apparaît pour afficher les erreurs. Vous pouvez également télécharger le fichier avec les erreurs.

Sujets connexes

Personnaliser la politique d'analyse de réseau, à la page 13
Annuler les modifications non enregistrées lors des modifications en ligne , à la page 18
Rétablir la configuration par défaut de la configuration remplacée, à la page 19
Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 22

Annuler les modifications non enregistrées lors des modifications en ligne

Lorsque vous apportez des modifications en ligne pour remplacer la configuration pour un inspecteur, , vous pouvez annuler des modifications non enregistrées. Notez que cette action rétablit toutes les modifications non enregistrées aux dernières valeurs enregistrées, mais ne rétablit pas la configuration à la configuration par défaut pour un inspecteur.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez annuler les modifications non enregistrées.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 4 Sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône en forme de **croix** (X) pour annuler les modifications non enregistrées pour l'inspecteur.

Vous pouvez également cliquer sur **Cancel** (Annuler) pour annuler l'opération.

Si aucune modification non enregistrée a été apportée à la configuration de l'inspecteur, cette option n'est pas visible.

Sujets connexes

Rétablir la configuration par défaut de la configuration remplacée, à la page 19
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 17

Afficher la liste des inspecteurs avec remplacements

Vous pouvez afficher une liste de tous les inspecteurs remplacés.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Cochez la case **Show Overrides Only** (afficher les remplacements uniquement) à côté de la barre de recherche pour afficher la liste des inspecteurs remplacés.

Tous les inspecteurs remplacés sont affichés avec une icône orange à côté de leur nom pour vous aider à les identifier.

Sujets connexes

Recherchez un inspecteur dans la page des politiques d'analyse de réseau., à la page 12
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 17
Personnaliser la politique d'analyse de réseau, à la page 13

Rétablir la configuration par défaut de la configuration remplacée

Vous pouvez annuler les modifications que vous avez apportées pour remplacer la configuration par défaut d'un inspecteur. Cette action rétablit la configuration remplacée à la configuration par défaut pour un inspecteur.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez rétablir la configuration remplacée.

Les inspecteurs remplacés sont signalés par une icône jaune à côté de leur nom.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur. Sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône **Revenir à la configuration par défaut** (flèche de retour) pour rétablir la configuration remplacée pour l'inspecteur à la configuration par défaut.

Si vous n'avez apporté aucune modification à la configuration par défaut de l'inspecteur, cette option est désactivée.

Étape 4 Cliquez sur **Revert** (Rétablir) pour confirmer la décision.

Étape 5 Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Si vous ne souhaitez pas enregistrer les modifications, vous pouvez cliquer sur **Annuler** ou sur l'icône **(X)**.

Sujets connexes

Annuler les modifications non enregistrées lors des modifications en ligne , à la page 18
Personnaliser la politique d'analyse de réseau, à la page 13
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 17
Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 22

Valider les politiques Snort 3

Pour valider les politiques Snort 3, voici une liste d'informations de base que l'utilisateur peut prendre en note :

- La version actuelle de centre de gestion peut gérer plusieurs versions de Défense contre les menaces.
- La version actuelle de centre de gestion prend en charge les configurations Politique d'analyse de réseau (NAP) qui ne sont pas applicables aux versions précédentes de Défense contre les menaces.
- La politique Politique d'analyse de réseau (NAP) et les validations actuelles fonctionneront selon la version actuelle prise en charge.
- Les modifications peuvent inclure du contenu qui n'est pas valide pour les versions précédentes des Défense contre les menaces.
- Les modifications de configuration de la politique sont acceptées s'il s'agit d'une configuration valide pour la version actuelle et si elle est effectuée à l'aide du binaire Snort 3 et du schéma Politique d'analyse de réseau (NAP) actuels.
- Pour les versions précédentes de Défense contre les menaces, la validation est effectuée lors du déploiement à l'aide du schéma Politique d'analyse de réseau (NAP) et du binaire Snort 3 pour cette version spécifique. S'il y a une configuration qui n'est pas applicable à la version donnée, l'utilisateur est informé ou averti que nous ne déploierons pas la configuration qui n'est pas prise en charge sur la version donnée et que la configuration restante sera déployée.

Dans cette procédure, lorsque nous associons la politique Politique d'analyse de réseau (NAP) à une politique de contrôle d'accès et la déployons sur un périphérique, par exemple, une configuration de filtre de débit comme celle d'un inspecteur est appliquée pour valider les politiques Snort 3.

Procédure

Étape 1 **Étapes pour remplacer la configuration de la politique Politique d'analyse de réseau (NAP) :** sous **Inspecteurs** dans la **version Snort 3** de la politique d'analyse de réseau, développez l'inspecteur requis pour lequel vous souhaitez remplacer le paramètre par défaut.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 2 Sous la section **Overridden Configuration (configuration remplacée)** dans la colonne de droite, cliquez sur l'icône **Edit Inspecteur** (Modifier l'inspecteur, en forme de crayon) pour apporter des modifications à un inspecteur comme rate_filter.

La fenêtre contextuelle Override Configuration (Remplacer la configuration) s'affiche dans laquelle vous pouvez apporter les modifications nécessaires à l'inspecteur rate_filter.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Vous pouvez également utiliser le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé.

Étape 5 Cliquez sur le menu déroulant **Actions** dans la section **Version 3 de Snort** de la politique d'analyse de réseau.

Étape 6 Sous **Téléverser**, vous pouvez cliquer sur **Overridden Configuration** (configuration remplacée) pour téléverser le fichier JSON qui contient la configuration remplacée.

Mise en garde Chargez uniquement les modifications dont vous avez besoin. Vous ne devez pas télécharger la configuration complète, car cela rend les remplacements persistants et, par conséquent, toute modification ultérieure de la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée.

Vous pouvez faire glisser et déposer un fichier ou cliquer pour naviguer jusqu'au fichier JSON enregistré dans votre système qui contient la configuration de l'inspecteur remplacée.

- **Fusionner les remplacements de l'inspecteur** : Le contenu du fichier téléversé est fusionné avec la configuration existante en l'absence d'inspecteur commun. S'il y a présence d'inspecteurs communs, le contenu du fichier téléversé (pour les inspecteurs communs) prévaut sur le contenu précédent et remplace la configuration pour ces inspecteurs.
- **Remplacer les remplacements de l'inspecteur** : supprime tous les remplacements précédents et les remplace par le nouveau contenu du fichier téléversé.

  Attention Comme le choix de cette option supprime tous les remplacements précédents, prenez une décision éclairée avant de remplacer la configuration à l'aide de cette option.

Si une erreur se produit lors du chargement des inspecteurs remplacés, elle est visible dans la fenêtre contextuelle **Upload Overridden Configuration File** (téléverser le fichier de configuration remplacé). Vous pouvez également télécharger le fichier avec l'erreur, puis corriger l'erreur et télécharger à nouveau le fichier.

Étape 7 **Étapes pour associer la Politique d'analyse de réseau (NAP) à la politique de contrôle d'accès :** dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced**(Avancé), puis sur **Edit** (modifier) à côté de la section Network Analysis and Intrusion Policies (Politiques d'analyse des réseaux et de prévention des intrusions).

Étape 8 Dans la liste déroulante **Default Network Analysis Policy** (politique d'analyse de réseau par défaut), sélectionnez une politique d'analyse de réseau par défaut.

Si vous choisissez une politique créée par l'utilisateur, vous pouvez cliquer sur **Edit** (modifier) pour modifier la politique dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Étape 11 Sinon, dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced**(Avancé), puis sur **Edit** (modifier) à côté de la section Network Analysis and Intrusion Policies (Politiques d'analyse des réseaux et de prévention des intrusions).

Étape 12 Cliquez sur **Add Rule** (ajouter une règle).

Étape 13 Configurez les conditions de la règle en cliquant sur les conditions que vous souhaitez ajouter.

Étape 14 Cliquez sur **Network Analysis** (analyse de réseau) et choisissez la **politique d'analyse de réseau** que vous souhaitez utiliser pour prétraiter le trafic correspondant à cette règle.

Étape 15 Cliquez sur **Add** (ajouter).

Étape 16 **Déploiement :** Dans la barre de menu centre de gestion, cliquez sur **Déployer**, puis sélectionnez **Déploiement**.

Étape 17 Définissez et choisissez les appareils sur lesquels vous souhaitez déployer les modifications de configuration.

- Search (rechercher) : Faites une recherche par nom, type, domaine, groupe ou état du périphérique dans le champ de recherche.
- Développer : Cliquez sur **Expand Arrow** (développer la flèche) pour afficher les modifications de configuration propres au périphérique à déployer.

  En sélectionnant la case à cocher du périphérique, toutes les modifications à apporter au périphérique, qui sont répertoriées sous le périphérique, sont poussées pour le déploiement. Cependant, vous pouvez utiliser **sélection de politique** pour sélectionner des politiques ou des configurations à déployer tout en conservant les modifications restantes sans les déployer.

  Facultativement, utilisez **Afficher ou masquer la politique** pour afficher ou masquer sélectivement les politiques non modifiées connexes.

Étape 18 Cliquez sur **Deploy** (déployer).

Étape 19 Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs.

Remarque Il affiche un avertissement indiquant que la politique d'analyse réseau de Snort 3 contient des inspecteurs ou des attributs qui ne sont pas valides pour cette version Défense contre les menaces, et que les paramètres non valides seront ignorés lors du déploiement : les inspecteurs non valides sont : ["rate_filter"] uniquement pour les périphériques inférieurs à la version 7.1.

Exemples de configuration de politique d'analyse de réseau personnalisée

Il s'agit d'un exemple de fichier qui comprend des extraits de code JSON expliquant comment personnaliser la politique d'analyse de réseau pour Snort 3. Vous pouvez choisir de remplacer une configuration de l'inspecteur des manières suivantes :

- Apportez des modifications en ligne pour un inspecteur directement dans centre de gestion. Consultez Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 17.
- Utilisez le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé. Consultez Personnaliser la politique d'analyse de réseau, à la page 13.

Avant de choisir l'une de ces options, consultez tous les détails et exemples suivants qui vous aideront à définir les remplacements de politique d'analyse de réseau avec succès. Vous devez lire et comprendre les exemples des différents scénarios expliqués ici afin d'éviter tout risque et toute erreur.

Si vous choisissez de remplacer une configuration de l'inspecteur dans le menu déroulant **Actions**, vous devez créer un fichier JSON pour les remplacements de politique d'analyse de réseau, puis téléverser le fichier.

Pour remplacer une configuration d'inspecteur dans la politique d'analyse de réseau, vous devez téléverser uniquement les modifications dont vous avez besoin. Vous ne devez pas télécharger la configuration complète,

car cela rend les remplacements persistants par nature et, par conséquent, toute modification ultérieure des valeurs ou de la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée.

Voici des exemples pour différents scénarios :

Activation d'un inspecteur Singleton lorsque l'état par défaut dans la politique de base est désactivé

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

Désactivation d'un inspecteur Singleton lorsque l'état par défaut dans la politique de base est activé

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

Activation d'un inspecteur Multiton lorsque l'état par défaut dans la politique de base est désactivé

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
  }
}
```

Désactivation d'un inspecteur Multiton lorsque l'état par défaut dans la politique de base est activé

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iec104": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

Remplacement de la valeur par défaut de paramètres spécifiques pour l'inspecteur Singleton

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
```

```
    }
}
```

Remplacement des paramètres spécifiques d'une instance par défaut (lorsque le nom de l'instance correspond au type d'inspecteur) dans l'inspecteur Multiton

```
{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false
        },
        "name": "http_inspect"
      }
    ]
  }
}
```

Ajout d'une règle de classeur pour une instance par défaut avec les modifications requises

Remarque Les règles du classeur par défaut ne peuvent pas être modifiées, elles sont toujours ajoutées à la fin.

```
{
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

Ajout d'une nouvelle instance personnalisée

Remarque L'entrée de règle de classeur correspondante doit être définie dans l'inspecteur de classeur.

```
{
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
```

```
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

Remplacement d'une instance Singleton, d'une instance par défaut de Multiton et de la création d'une nouvelle instance Multiton dans un remplacement JSON unique

Exemple pour afficher les éléments suivants dans un seul remplacement JSON :

- Remplacement d'une instance Singleton (inspecteur **`du normalisateur`**)
- Remplacement d'une instance par défaut de Multiton (inspecteur **`http_inspect`**)
- Création d'une nouvelle instance Multiton (inspecteur **`Telnet`**)

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false,
          "xff_headers": "x-forwarded-for true-client-ip x-another-forwarding-header"
        },
        "name": "http_inspect"
      }
    ]
  },
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
```

```
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      },
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

Remarque Vous n'avez pas besoin de fournir l'attribut de **nom** pour l'instance par défaut dans les règles de classeur.

Configuration de arp_spoof

Exemple de configuration de **arp_spoof** :

L'inspecteur **arp_spoof** n'a aucune configuration par défaut pour aucun attribut. Cela montre un cas où vous pouvez fournir les remplacements.

```
{
  "arp_spoof": {
    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
```

```
  }
}
```

Configuration de rate_filter

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

Configuration des règles de classeur lors de l'utilisation de la politique d'analyse de réseau à plusieurs hiérarchies

Cet exemple illustre l'ajout d'une nouvelle instance personnalisée dans la politique enfant et la façon dont les règles de classeur doivent être écrites. Les règles du classeur sont définies sous forme de liste et, par conséquent, il est important de reprendre les règles définies dans la politique parente et de construire les nouvelles règles par-dessus, car les règles ne seront pas fusionnées automatiquement. Les règles de classeur disponibles dans la politique enfant sont une source de réalité en entier.

Dans Défense contre les menaces, les règles de politique par défaut de Cisco Talos sont ajoutées pour ces remplacements définis par l'utilisateur.

Politique parente :

Nous avons défini une instance personnalisée sous le nom **`telnet_parent_instance`** et la règle de classeur correspondante.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
```

```
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Politique enfant :

Cette politique d'analyse de réseau a la politique susmentionnée comme politique de base. Nous avons défini une instance personnalisée sous le nom **`telnet_child_instance`** et avons également défini les règles de classeur pour cette instance. Les règles de classeur de la politique parente doivent être copiées ici, puis les règles de classeur de la politique enfant peuvent être ajoutées au début ou par-dessus en fonction de la nature de la règle.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Configuration de l'attribut de l'inspecteur de listes en général

Lors de la modification des remplacements pour un attribut de type liste, il est important de transmettre le contenu complet plutôt que le remplacement partiel. Cela signifie que si les attributs de politique de base sont définis comme :

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

Si vous souhaitez modifier **`value1`** en **`value1-new`**, la charge utile de remplacement doit ressembler à ce qui suit :

Méthode correcte :

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

Méthode incorrecte :

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
  ]
}
```

Vous pouvez comprendre cette configuration en prenant les valeurs diminuées de l'attribut **`alt_max_command_line_len`** dans l'inspecteur **`smtp`**. Supposons que la configuration de politique par défaut (de base) pour l'inspecteur **`smtp`** soit la suivante :

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "decompress_zip": false,
```

```
            "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
             EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
             NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
             TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
             ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
             XSTA XTRN XUSR",
            "ignore_data": false,
            "max_command_line_len": 512,
            "max_header_line_len": 1000,
            "log_rcptto": false,
            "decompress_swf": false,
            "max_response_line_len": 512,
            "b64_decode_depth": -1,
            "max_auth_command_line_len": 1000,
            "log_email_hdrs": false,
            "xlink2state": "alert",
            "binary_data_cmds": "BDAT XEXCH50",
            "auth_cmds": "AUTH XAUTH X-EXPS",
            "log_filename": false,
            "uu_decode_depth": -1,
            "ignore_tls_data": false,
            "data_cmds": "DATA",
            "bitenc_decode_depth": -1,
            "alt_max_command_line_len": [
              {
                "length": 255,
                "command": "ATRN"
              },
              {
                "command": "AUTH",
                "length": 246
              },
              {
                "length": 255,
                "command": "BDAT"
              },
              {
                "length": 246,
                "command": "DATA"
              }
            ],
            "log_mailfrom": false,
            "decompress_pdf": false,
            "normalize": "none",
            "email_hdrs_log_depth": 1464,
            "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
             EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
             NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
             TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
             ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
             XSTA XTRN XUSR",
            "qp_decode_depth": -1
          }
        }
    ],
    "enabled": true
  }
}
```

Maintenant, si vous souhaitez ajouter deux autres objets à la liste **`alt_max_command_line_len`** :

```
{
    "length": 246,
    "command": "XEXCH50"
},
```

```
{
    "length": 246,
    "command": "X-EXPS"
}
```

Le JSON de la politique d'analyse personnalisée du réseau ressemblerait alors à ce qui suit :

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

Configuration des remplacements lorsque la politique d'analyse de réseau multi-hiérarchisation est utilisée dans l'inspecteur Multiton

Cet exemple illustre le remplacement des attributs dans la politique enfant et la façon dont la configuration fusionnée sera utilisée dans la politique enfant pour toute instance. Tous les remplacements définis dans la politique enfant seront fusionnés avec la politique parent. Par conséquent, si attribut1 et attribut2 sont remplacés dans la politique parente et que les attribut2 et attribut3 sont remplacés dans la politique enfant, les configurations fusionnées sont pour la politique enfant. Cela signifie que l'attribut1 (défini dans la politique parente), l'attribut2 (défini dans la politique enfant) et l'attribut3 (défini dans la politique enfant) seront configurés sur le périphérique.

Politique parente :

Ici, nous avons défini une instance personnalisée sous le nom **`telnet_parent_instance`** et remplacé deux attributs, à savoir **`normalize`** et **`encrypted_traffic`** dans l'instance personnalisée.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Politique enfant :

Cette politique d'analyse de réseau a la politique susmentionnée comme politique de base. Nous avons remplacé l'attribut **`encrypted_traffic`** de la politique parente et remplacé le nouvel attribut **`ayt_attack_thresh`**.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}
```

Avec le JSON de politique ci-dessus, lorsque vous déployez la politique d'analyse de réseau, le JSON fusionné suivant sera configuré sur le périphérique.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
```

```
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Cet exemple illustre les détails de la politique d'analyse de réseau personnalisée. Le même comportement se produit dans l'instance par défaut. En outre, une fusion similaire serait effectuée pour les inspecteurs Singleton.

Suppression de tous les remplacements de l'inspecteur pour la politique d'analyse de réseau :

Chaque fois que vous souhaitez supprimer tous les remplacements pour une politique d'analyse de réseau spécifique, vous pouvez téléverser un fichier JSON vide. Lors du chargement des remplacements, choisissez l'option **Remplacer les remplacements de l'inspecteur**.

```
{
}
```

Sujets connexes

Définitions et terminologies pour la politique d'analyse de réseau Snort 3 , à la page 3
Mappage de la stratégie d'analyse du réseau, à la page 11
Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 6
Recherchez un inspecteur dans la page des politiques d'analyse de réseau., à la page 12
Copier la configuration de l'inspecteur , à la page 13
Personnaliser la politique d'analyse de réseau, à la page 13
Afficher la liste des inspecteurs avec remplacements, à la page 19

Paramètres de politique d'analyse de réseau et modifications en cache

Lorsque vous créez une politique d'analyse de réseau, elle utilise les mêmes paramètres que sa politique de base.

Lorsque vous adaptez une politique d'analyse de réseau, en particulier lorsque vous désactivez les inspecteurs, gardez à l'esprit que certains inspecteurs et certaines règles de prévention des intrusions exigent que le trafic soit d'abord décodé ou prétraité d'une certaine manière. Si vous désactivez un inspecteur obligatoire, le

système l'utilise automatiquement avec ses paramètres actuels, bien que l'inspecteur reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Remarque Le prétraitement et l'inspection de prévention des intrusions sont si étroitement liés que les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet **doivent** se compléter mutuellement. La personnalisation du prétraitement, en particulier de l'utilisation de plusieurs politiques d'analyse de réseau personnalisées, est une tâche **avancée**.

Le système met en cache une politique d'analyse de réseau par utilisateur. Lors de la modification d'une politique d'analyse de réseau, si vous sélectionnez un menu ou un autre chemin vers une autre page, vos modifications restent dans le cache système même si vous quittez la page.

Règles personnalisées dans Snort 3

Vous pouvez créer une règle de prévention des intrusions personnalisée en important un fichier de règle local. Le fichier de règles peut avoir une extension `.txt` ou `.rules`. Le système enregistre la règle personnalisée dans la catégorie de règle locale, quelle que soit la méthode que vous avez utilisée pour la créer. Une règle personnalisée doit appartenir à un groupe de règles. Cependant, une règle personnalisée peut également faire partie de deux groupes ou plus.

Lorsque vous créez une règle de prévention des intrusions personnalisée, le système lui attribue un numéro de règle unique, qui a le format `GID:SID:Rev`. Les éléments composant ce numéro sont les suivants :

- **GID** : ID de générateur. Pour les règles personnalisées, il n'est pas nécessaire de préciser le GID. Le système génère automatiquement le GID lors du chargement des règles selon que vous vous trouvez dans le domaine global ou dans un sous-domaine. Pour toutes les règles de texte standard, cette valeur est de 2 000 pour un domaine global.
- **SID** : ID Snort. Indique s'il s'agit d'une règle locale d'une règle système. Lorsque vous créez une règle, attribuez-lui un SID unique.

  Les numéros SID des règles locales commencent à 1000000 et le SID de chaque nouvelle règle locale est incrémenté de un.
- **Rev** : le numéro de la révision. Pour une nouvelle règle, le numéro de révision est de 1. Chaque fois que vous modifiez une règle personnalisée, le numéro de révision doit être incrémenté de un.

Dans une règle de texte standard personnalisée, vous définissez les paramètres d'en-tête de règle ainsi que les mots-clés et les arguments de la règle. Vous pouvez utiliser les paramètres d'en-tête de règle pour axer la règle de manière à ce qu'elle ne corresponde qu'au trafic utilisant un protocole spécifique et circulant vers ou à partir d'adresses IP ou de ports spécifiques.

Remarque Les règles personnalisées Snort 3 ne peuvent pas être modifiées. Assurez-vous que les règles personnalisées comportent un message de classification valide pour le type de `classe` dans le texte de la règle. Si vous importez une règle sans classification ou avec une mauvaise classification, supprimez et recréez la règle.

Présentation du moteur de visibilité chiffrée

Le moteur de visibilité chiffrée (EVE, Encrypted Visibility Engine) est utilisé pour offrir plus de visibilité sur les sessions chiffrées sans qu'il soit nécessaire de les déchiffrer. Ces informations sur les sessions chiffrées sont obtenues par la bibliothèque de logiciels libres de Cisco, qui est présente dans la base de données de vulnérabilités (VDB) de Cisco. La bibliothèque prend et analyse les empreintes des sessions chiffrées entrantes et les compare à un ensemble d'empreintes connues. Cette base de données d'empreintes digitales connues est également disponible dans la base de données de Cisco VDB.

Remarque La fonctionnalité de moteur de visibilité chiffrée n'est prise en charge que sur les périphériques gérés par centre de gestion exécutant Snort 3. Cette fonctionnalité n'est pas prise en charge sur les périphériques Snort 2, les périphériques gérés par gestionnaire d'appareil, ou CDO.

Certaines des caractéristiques importantes d'EVE sont les suivantes :

- Vous pouvez appliquer des actions de politique de contrôle d'accès sur le trafic en utilisant les informations dérivées d'EVE.
- La VDB incluse dans Cisco Secure Firewall a la capacité d'affecter des applications à certains processus détectés par EVE avec une valeur de confiance élevée. Vous pouvez également créer des détecteurs d'application personnalisés pour :
  - Mettre en correspondance des processus détectés par EVE pour les nouvelles applications définies par l'utilisateur.
  - Remplacer la valeur intégrée de niveau de confiance de processus qui est utilisée pour affecter des applications aux processus détectés par EVE.

    Reportez-vous aux sections **Configuration des détecteurs d'application personnalisés** et **Spécification des affectations de processus EVE** dans le chapitre sur la **détection d'applications** du Guide de configuration des périphériques de Cisco Secure Firewall Management Center.
- EVE peut détecter le type et la version du système d'exploitation du client qui a créé un paquet Client Hello dans le trafic chiffré.
- EVE prend également en charge l'empreinte et l'analyse du trafic QUIC (Quick UDP Internet Connections). Le nom du serveur du paquet Client Hello s'affiche dans le champ URL de la page des **événements de connexion**.

Attention Pour utiliser la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) sur centre de gestion, vous devez avoir une licence IPS valide sur votre périphérique. En l'absence de licence IPS , la politique affiche un avertissement et le déploiement n'est pas autorisé.

Remarque La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut détecter le type et la version des sessions SSL du système d'exploitation. L'utilisation normale du système d'exploitation, comme l'exécution d'applications et d'un logiciel de gestion des paquets, peut déclencher la détection du système d'exploitation. Pour afficher la détection du système d'exploitation client, en plus d'activer le bouton à bascule EVE, vous devez activer les **hôtes** sous les **politiques** > **de découverte de réseau**. Pour afficher une liste des systèmes d'exploitation possibles sur l'adresse IP de l'hôte, cliquez sur **Analysis** > **Hosts** > **Network Map**(Analyse > Hôtes > Carte du réseau), puis choisissez l'hôte requis.

Liens connexes

Configurer la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée), à la page 37

Comment fonctionne EVE

Le moteur de visibilité chiffrée (EVE) inspecte la partie Client Hello de l'établissement de liaison TLS pour identifier les processus clients. Le Client Hello est le paquet de données initial qui est envoyé au serveur. Cela donne une bonne indication du processus client sur l'hôte. Cette empreinte, combinée à d'autres données telles que l'adresse IP de destination, fournit la base pour l'identification de l'application d'EVE. En identifiant des empreintes d'applications précises lors de l'établissement de session TLS, le système peut identifier le processus client et prendre les mesures appropriées (autoriser/bloquer).

La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut identifier plus de 5 000 processus clients. Le système mappe un certain nombre de ces processus aux applications clientes afin de les utiliser comme critères dans les règles de contrôle d'accès. Cela donne au système la capacité d'identifier et de contrôler ces applications sans activer le déchiffrement TLS. En utilisant les empreintes de processus malveillants connus, la technologie EVE peut également être utilisée pour identifier et bloquer le trafic malveillant chiffré sans déchiffrement sortant.

Grâce à la technologie d'apprentissage automatique, Cisco traite plus d'un milliards d'empreintes TLS et plus de 10 000 échantillons de programmes malveillants par jour pour créer et mettre à jour des empreintes EVE. Ces mises à jour sont ensuite fournies aux clients au moyen des offres groupées de la base de données de vulnérabilités (VDB) de Cisco.

Événements d'indications de compromission

Les événements d'indication de compromission (IoC) de l'hôte pour la détection du moteur de visibilité chiffrée vous permettent de vérifier les événements de connexion avec un niveau de confiance très élevé des programmes malveillants, comme indiqué par EVE. Les événements d'IoC sont déclenchés pour les sessions chiffrées générées à partir d'un hôte à l'aide d'un client malveillant. Vous pouvez afficher des informations telles que l'adresse IP, l'adresse MAC et les informations sur le système d'exploitation de l'hôte malveillant, ainsi que l'horodatage de l'activité suspecte.

Une session avec un niveau de confiance des menaces pour la visibilité chiffrée « très élevé », comme indiqué dans les événements de connexion, génère un événement IoC. Vous devez activer les **hôtes** à partir des **politiques** > **découverte de réseau**. Dans la centre de gestion, vous pouvez afficher l'existence de l'événement d'IoC à partir de :

- **Analyse** > **Indications de compromission**.

- **Analyse** > **Carte du réseau** > **Indications de compromission** : choisissez l'hôte qui doit être vérifié.

  Vous pouvez afficher les informations de processus de la session qui a généré l'IoC à partir de :

  Analyse > **Événements de connexion** > **Vue en tableau des événements de connexion, colonne** > **IoC**. Notez que vous devez sélectionner manuellement les champs Encrypted Visibility (Visibilité chiffrée) et le champ IoC.

Empreinte QUIC dans EVE

Snort peut identifier les applications clientes dans les connexions Internet UDP rapides (sessions QUIC) basées sur la fonctionnalité EVE. La détection d'empreintes QUIC peut :

- Détecter les applications sur QUIC sans activer le déchiffrement.
- Déterminer les programmes malveillants sans activer le déchiffrement.
- Détection des applications de service. Vous pouvez affecter des règles de contrôle d'accès en fonction du service détecté sur le protocole QUIC.

Configurer la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée)

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Cliquez sur **Edit** (Modifier) ( ) à côté de la politique de contrôle d'accès que vous souhaitez modifier.

Étape 3 Choisissez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 4 Cliquez sur **Edit** (Modifier) ( ) à côté de **Encrypted Visibility Engine**(Moteur de visibilité chiffrée) (EVE).

Étape 5 Dans la page **Encrypted Visibility Engine** (moteur de visibilité chiffrée), activez le bouton à bascule **Encrypted Visibility Engine** (moteur de visibilité chiffrée).

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployer les modifications de configuration

Afficher les événements EVE

Après avoir activé l'**Encrypted Visibility Engine** (moteur de visibilité chiffrée) et déployé votre politique de contrôle d'accès, vous pouvez commencer à envoyer du trafic en direct par votre système. Vous pouvez

afficher les événements de connexion enregistrés dans la page **Connection Events** (événements de connexion). Pour accéder aux événements de connexion, dans centre de gestion :

Procédure

Étape 1 Cliquez sur **Analysis (Analyse)** > **Connections (Connexions)** > **Events** (Événements).

Étape 2 Cliquez sur l'onglet **Table View of Connection Events** (Vue de tableau des événements de connexion).

Vous pouvez également afficher les champs d'événements de connexion dans la visionneuse des **événements unifiés**, qui se trouve dans le menu **Analysis** (Analyse).

Le moteur de chiffrée peut identifier le processus client qui a lancé une connexion, le système d'exploitation du client et si le processus contient ou non des programmes malveillants.

Étape 3 Dans la page **Connection Events** (événements de connexion), affichez les colonnes suivantes, qui sont ajoutées pour la prise d' ,Encrypted Visibility Engine (Moteur de visibilité chiffrée) . Notez que vous devez activer explicitement les colonnes mentionnées.

- Nom du processus de visibilité chiffrée
- Note de confiance du processus de visibilité chiffrée
- Niveau de confiance des menaces pour la visibilité chiffrée
- Note de confiance des menaces pour la visibilité chiffrée
- Type de détection

Pour en savoir plus sur ces champs, consultez la section **Champs d'événements de connexion et de renseignement de sécurité** dans le chapitre **Événements liés à la connexion et à la sécurité** du Guide d'administration de Cisco Secure Firewall Management Center.

Remarque Dans la page **Connection Events** (événements de connexion), si les processus sont affectés à des applications, la colonne **Detection Type** (type de détection) affiche **Encrypted Visibility Engine** (moteur de visibilité chiffrée), indiquant que l'application client a été identifiée par EVE. Sans affectations d'applications aux noms de processus, la colonne **Detection Type** affiche **AppID** indiquant que le moteur qui a identifié l'application client était AppID.

Afficher le tableau de bord EVE

Vous pouvez afficher les informations de l'analyse EVE dans deux tableaux de bord. Pour accéder aux tableaux de bord :

Procédure

Étape 1 Sous **Présentation** > **Tableaux de bord**, cliquez sur **Tableau de bord**.

Étape 2 Dans la fenêtre **Summary Dashboard** (tableau de bord résumé), cliquez sur le lien **Switch Dashboard** (Changer de tableau de bord) et choisissez **Application Statistics** (Statistiques de l'application) dans la liste déroulante.

Étape 3 Choisissez l'onglet **Digital Visibility Engine** (moteur de visibilité chiffrée par empreintes) pour afficher les deux tableaux de bord suivants :

- **Principaux processus découverts par le moteur de visibilité chiffrée** : affiche les principaux noms de processus TLS utilisés dans votre réseau et le nombre de connexions. Vous pouvez cliquer sur le nom du processus dans le tableau pour voir la vue filtrée de la page des **événements de connexion**, qui est filtrée par nom de processus.
- **Connexions par moteur de visibilité chiffrée de confiance dans la menace** : affiche les connexions en fonction des niveaux de confiance (très élevé, très faible, etc.). Vous pouvez cliquer sur le niveau de confiance des menaces dans le tableau pour afficher la vue filtrée de la page des **événements de connexion**, qui est filtrée par niveau de confiance.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.