



Stratégies 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.

- [Analyse du réseau, à la page 1](#)
- [Gérer les politiques d'analyse du réseau, à la page 2](#)
- [Définitions et terminologies pour les politiques d'analyse de réseau Snort 3, à la page 3](#)
- [Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 6](#)
- [Paramètres de politique d'analyse de réseau et modifications en cache, à la page 35](#)
- [Générer des recommandations Snort 3, à la page 36](#)

Analyse du réseau

Une *politique d'analyse de réseau* est une configuration de prétraitement du trafic qui

- régit de nombreuses options de prétraitement du trafic et est appelée par les paramètres avancés de votre stratégie de contrôle d'accès,
- effectue le prétraitement après la correspondance Security Intelligence et le déchiffrement SSL, et
- termine le traitement avant que ne commence l'inspection des intrusions ou des fichiers.

Politiques d'analyse du réseau par défaut et personnalisées

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 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

Cette tâche vous permet d'effectuer diverses opérations de gestion sur les politiques d'analyse de réseau, notamment la création, la modification, la suppression, la comparaison et la génération de rapports.

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.

**Remarque**

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour plus de renseignements sur les fonctionnalités de Snort 2 prises en charge dans les versions antérieures à la version 7.7, consultez le [guide du centre de gestion](#) correspondant à votre version de Threat Defense.

Procédure

Étape 1

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

- **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Access Control (Contrôle d'accès)**, puis cliquez sur **Politique d'analyse de réseau**
- **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**, puis cliquez sur **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

- **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 **version Snort 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 les politiques 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 en tenir compte. Lorsque le trafic correspond aux conditions définies dans l'inspecteur Binder, alors seulement les valeurs et configurations de cet inspecteur entrent en vigueur. Pour en savoir plus, consultez la section <i>Inspecteur de classeur</i> 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 <i>Inspecteurs Singleton</i> 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 <i>Inspecteurs Multiton</i> 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 14.

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 14.
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 14.
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 14.

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 14](#)

[Mappage de la stratégie d'analyse du réseau, à la page 11](#)

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

La création d'une politique d'analyse de réseau personnalisée pour Snort 3 est un processus de configuration basé sur les données qui

- permet aux utilisateurs avancés de personnaliser la politique d'analyse de réseau par défaut pour des exigences de réseau spécifiques ou d'optimiser les performances, et
- utilise JSON et le schéma JSON en fonction de la spécification OpenAPI pour configurer les inspecteurs et les paramètres.

Aperçu de la personnalisation de la politique d'analyse du réseau

La politique d'analyse de réseau par défaut est réglée pour les exigences de réseau typiques et des performances optimales. Dans la plupart des situations, vous n'avez pas besoin de personnaliser la politique. 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.

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. Le nombre d'inspecteurs et de paramètres disponibles dans Firewall Management Center est un sous-ensemble de ceux 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 Firewall Management Center.



Remarque

- Lors de la mise à niveau de Firewall Management Center 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 **Inspectors** (Inspecteurs) dans la version **Snort 3** de votre politique d'analyse de réseau.

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 Binder, alors seulement les valeurs et 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.

a

Si ces conditions sont remplies, utilisez le type imap.

```

▼ binder
185 {
186     "when": {
187         "service": "imap",
188         "role": "any"
189     },
190     "use": {
191         "type": "imap"
192     }
193 },

```

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. Assurez-vous d'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 sécurisé des périphériques,
- fournit une communication à sécurité intégrée entre différents nœuds sur un réseau CIP, et
- comprend deux composants principaux pour l'échange des paramètres de sécurité et la transmission des informations de sécurité.

Composants du protocole de sécurité 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

Cette tâche permet la détection et le blocage des segments de sécurité CIP tout en permettant le passage d'autres paquets CIP.

Utilisez cette procédure 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 stratégie de contrôle d'accès.

Procédure

- | | |
|----------------|--|
| Étape 1 | Accédez à Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau) . |
| Étape 2 | Cliquez sur la version Snort 3 de la politique d'analyse de réseau cip_safety que vous avez créée. |
| Étape 3 | Sous Inspectors (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 Sous Inspectors (Inspecteurs) , cliquez sur CIP pour le développer . de false (par défaut) à true. |
| Étape 5 | Cliquez sur OK , puis sur Save (Enregistrer). |
| Étape 6 | Pour affecter l'inspecteur CIP à la stratégie de contrôle d'accès, choisissez Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Access Control (Contrôle d'accès) , cliquez sur Edit (Modifier) et sélectionnez l'option Advanced Settings (Paramètres avancés) dans la liste déroulante More (Plus) à la fin de la ligne de flux de paquets. |

- Étape 7** Cliquez sur **Modifier** (✎) à côté de **Politiques d'analyse du réseau et de prévention des intrusions**.
- Étape 8** 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 9** Après avoir envoyé le trafic en direct contenant les flux de paquets CIP Safety, accédez à **Connection Events** (Incidents 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

Le mappage des politiques d'analyse du réseau est un mécanisme de corrélation qui

- fournit des informations de cartographie pour les politiques d'analyse du réseau,
- recherche la version des politiques Snort 2 correspondante pour la version Snort 3, et
- garantit que les politiques de la version Snort 3 ont leur équivalent dans la version Snort 2.

Afficher le mappage de la politique d'analyse des réseaux

Affichez les politiques d'analyse de réseau Snort 3 qui sont automatiquement mappées à leurs politiques équivalentes Snort 2 dans le système.

Le mappage des politiques d'analyse de réseau vous permet de voir la relation entre les politiques Snort 3 et Snort 2 lors de la transition entre les versions ou de la gestion des deux simultanément.

Procédure

- Étape 1** Accédez à **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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

Créez une nouvelle politique d'analyse de réseau qui fournit des versions Snort 2 et Snort 3 pour l'inspection et l'analyse du trafic réseau.

Toutes les politiques d'analyse de réseau existantes sont disponibles dans Firewall Management Center 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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau) . |
| Étape 2 | Cliquez sur Créer une politique . |
| Étape 3 | Remplissez les champs Nom et Description . |
| Étape 4 | Sélectionnez une politique de base et cliquez sur Save (Enregistrer). |
-

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

Cette tâche vous permet de mettre à jour la configuration d'une politique d'analyse de réseau existante en modifiant ses propriétés telles que le nom, la description ou les paramètres de la politique de base.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau) . |
| Étape 2 | Cliquez sur Edit (Modifier) pour changer le nom, la description, le mode d'inspection ou la politique de base. |

**Attention**

Obsolescence du mode de détection : à partir de la version 7.1.0 du centre de gestion, pour une politique d'analyse de réseau (NAP), le mode d'inspection de **détection** est obsolète et sera supprimé dans une prochaine version.

Le mode de **détection** était destiné à être utilisé comme mode de test afin que vous puissiez activer les inspections et voir comment elles se comportent dans votre réseau avant de le configurer pour abandonner le trafic, c'est-à-dire pour afficher le trafic qui serait abandonné.

Ce comportement est amélioré lorsque tous les abandons de l'inspecteur sont contrôlés par l'état de la règle et que vous pouvez définir chacun d'eux pour générer des événements. Ceci est fait pour les tester avant de configurer l'état de la règle pour abandonner le trafic. Comme nous avons maintenant un contrôle fin des pertes de trafic dans Snort 3, le mode de **détection** ne fait qu'ajouter plus de complexité au produit et n'est pas nécessaire, le mode de détection est donc obsolète.

Si vous modifiez une Politique d'analyse de réseau (NAP) de **détection** à **Prévention**, la Politique d'analyse de réseau (NAP) qui traite le trafic des incidents d'intrusion qui « sera abandonnée » est « abandonnée », et le trafic correspondant abandonnera le trafic de ces événements. Cela s'applique aux règles dont les GID ne sont pas 1 ou 3. Les GID 1 et 3 sont des règles de texte ou compilées (généralement fournies par Talos ou à partir de vos règles personnalisées ou importées), et tous les autres GID sont des inspections pour détecter des anomalies. Il s'agit de règles moins courantes à déclencher dans un réseau. Il est peu probable que le passage en mode de **prévention** ait un impact sur le trafic. Il vous suffit de désactiver la règle de prévention des intrusions qui s'applique au trafic abandonné et de la régler sur généré ou désactivé.

Nous vous recommandons de choisir **Prévention** comme mode d'inspection, mais si vous choisissez **Prévention**, vous ne pouvez pas revenir au mode **Détection**.

**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).

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

Cette tâche vous permet de localiser rapidement des inspecteurs dans l'interface de politique d'analyse de réseau en utilisant la fonctionnalité de recherche.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.

- 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 **Search** (Rechercher).
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.
-

Copier la configuration de l'inspecteur

Cette tâche décrit comment copier les configurations 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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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 **Copy to clipboard** (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 14

Personnaliser la politique d'analyse de réseau

Personnalisez la politique d'analyse de réseau pour adapter les configurations Snort 3 en fonction de vos exigences de sécurité.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.

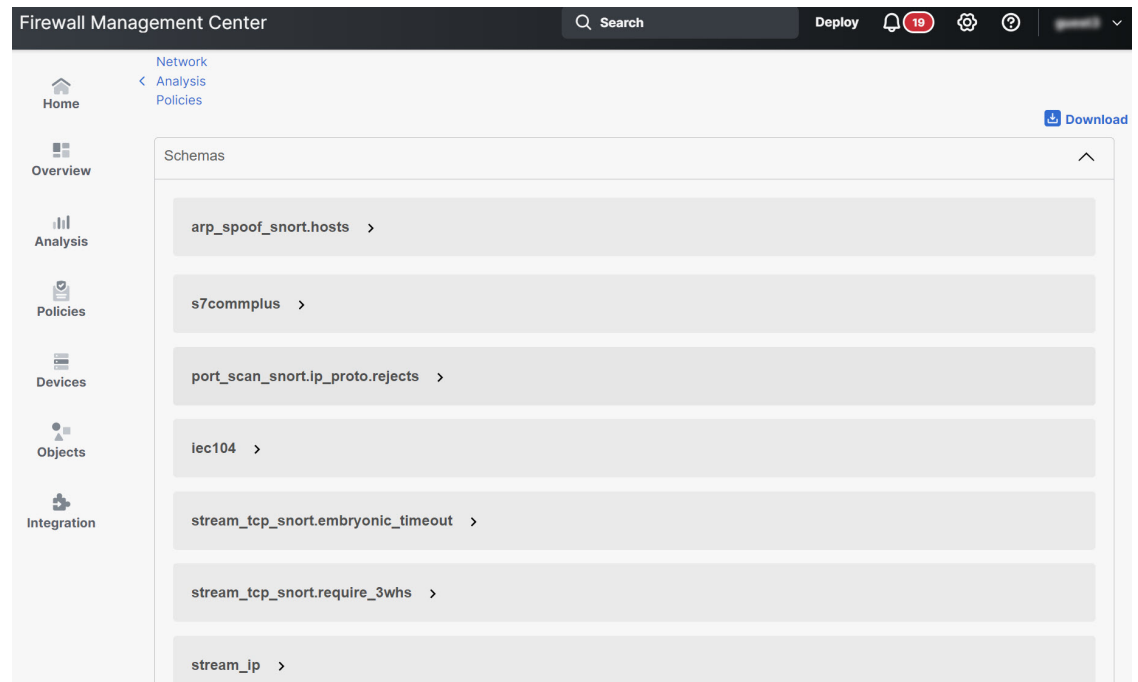
Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

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.

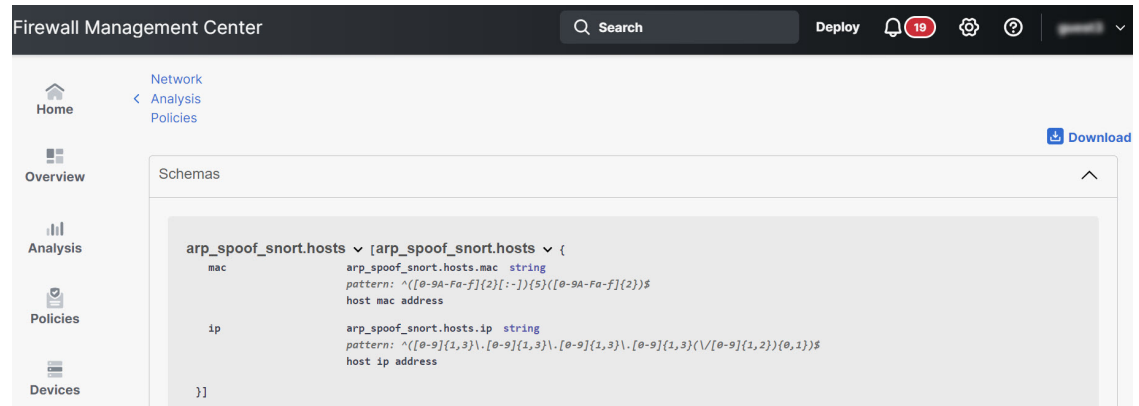
a) Cliquez sur **Télécharger le schéma** pour télécharger le fichier de schéma.

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. Ce fichier contient tous les renseignements sur la configuration de l'inspecteur.

- 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 Firewall Management Center. 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 charger le fichier de configuration remplacé.

Si vous avez choisi d'effectuer les modifications en ligne directement dans Firewall Management Center, 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 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 charger 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. Passez attentivement votre choix en revue avant d'utiliser cette option pour remplacer la configuration.

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 une sauvegarde de temps à autre lorsque vous remplacez la configuration de l'inspecteur.

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.

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 14](#) pour obtenir de plus amples renseignements.

Procédure

- Étape 1** Accédez à **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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, Firewall Management Center 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 14](#)
- [Annuler les modifications non enregistrées lors des modifications en ligne, à la page 20](#)
- [Rétablir la configuration remplacée à la configuration par défaut, à la page 21](#)
- [Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 24](#)

Annuler les modifications non enregistrées lors des modifications en ligne

Cette tâche vous permet de revenir sur toutes les modifications non enregistrées effectuées lors des modifications en ligne afin de remplacer la configuration d'un inspecteur, en revenant à la dernière valeur enregistrée.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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 remplacée à la configuration par défaut](#), à la page 21

[Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration](#), à la page 18

Afficher la liste des inspecteurs avec remplacements

Cette tâche vous permet d'identifier et de passer en revue tous les inspecteurs qui ont été remplacés dans la configuration de votre politique d'analyse de réseau.

Vous pouvez afficher une liste de tous les inspecteurs remplacés.

Procédure

-
- Étape 1** Accédez à **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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

[Rechercher un inspecteur dans la page des politiques d'analyse de réseau.](#), à la page 13

[Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration](#), à la page 18

[Personnaliser la politique d'analyse de réseau](#), à la page 14

Rétablir la configuration remplacée à la configuration par défaut

Annulez les modifications que vous avez apportées pour remplacer la configuration par défaut d'un inspecteur, en restaurant les paramètres par défaut d'origine.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau) . |
| Étape 2 | Accédez à la version Snort 3 de la politique d'analyse de réseau. |
| Étape 3 | <p>Sous Inspecteurs, développez l'inspecteur requis pour lequel vous souhaitez rétablir la configuration remplacée.</p> <p>Les inspecteurs remplacés sont signalés par une icône jaune à côté de leur nom.</p> <p>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.</p> <p>Si vous n'avez apporté aucune modification à la configuration par défaut de l'inspecteur, cette option est désactivée.</p> |
| 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 20

[Personnaliser la politique d'analyse de réseau](#), à la page 14

[Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration](#), à la page 18

[Exemples de configuration de politique d'analyse de réseau personnalisée](#), à la page 24

Valider les politiques Snort 3

Cette tâche valide les politiques Snort 3 pour s'assurer qu'elles fonctionnent correctement avec les versions de périphérique actuelles et précédentes, en gérant les configurations spécifiques à la version et les paramètres d'inspection.

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

- La version actuelle de Firewall Management Center peut gérer plusieurs versions de Firewall Threat Defense.
- La version actuelle de Firewall Management Center prend en charge les configurations de politique d'analyse de réseau (NAP) qui ne sont pas applicables aux versions précédentes de Firewall Threat Defense.
- 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 Firewall Threat Defense.
- Les modifications de configuration de la politique sont acceptées si elles sont valides pour la version actuelle et effectuées à l'aide du binaire Snort 3 et du schéma NAP actuels.
- Pour les versions précédentes de Firewall Threat Defense, 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 la configuration non prise en charge sur la version donnée ne sera pas déployée, tandis 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.

- a) 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`. Cliquez sur **OK**.

- b) Cliquez sur **Enregistrer** pour enregistrer vos modifications.

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

- Étape 2** Cliquez sur le menu déroulant **Actions** dans la section **Snort 3 Version** (Version Snort 3) de la politique d'analyse de réseau.
- Étape 3** Sous **Upload** (Charger), vous pouvez cliquer sur **Overridden Configuration** (Configuration remplacée) pour charger le fichier JSON qui contient la configuration remplacée.

**Mise en garde**

Chargez uniquement les modifications dont vous avez besoin. Vous ne devez pas charger 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.

- **Merge inspector overrides (Fusionner les remplacements de l'inspecteur)** : le contenu du fichier chargé 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.
- **Replace inspector overrides (Remplacer les remplacements de l'inspecteur)** : supprime tous les remplacements précédents et les remplace par le nouveau contenu du fichier chargé.

**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 4** **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).
- 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.
 - Cliquez sur **OK** puis sur **Save** (Enregistrer) pour enregistrer la politique.
- Étape 5** 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).
- Cliquez sur **Add Rule** (ajouter une règle).
 - Configurez les conditions de la règle en cliquant sur les options que vous souhaitez ajouter.
 - 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.
 - Cliquez sur **Add** (ajouter).

Étape 6 **Déploiement :** Dans la barre de menu Firewall Management Center, cliquez sur **Déployer**, puis sélectionnez **Déploiement**.

Étape 7 Définissez et choisissez les appareils sur lesquels vous souhaitez déployer les modifications de configuration.

- Recherche : Recherchez 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 cochant la case du périphérique, toutes les modifications pour ce périphérique qui y sont répertoriées sont transmises. Vous pouvez également utiliser **Policy Selection** (Sélection de politique) pour sélectionner des politiques ou des configurations individuelles à déployer tout en excluant les autres.

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

Étape 8 Cliquez sur **Deploy** (déployer).

Étape 9 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 de réseau Snort 3 contient des inspecteurs ou des attributs non valides pour cette version Firewall Threat Defense. 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 Firewall Management Center. Consultez [Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration](#), à la page 18.
- Utilisez le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé. Consultez [Personnaliser la politique d'analyse de réseau](#), à la page 14.

Avant de choisir l'une de ces options, consultez tous les détails et exemples pour vous aider à définir les remplacements de politique d'analyse de réseau avec succès. Pour éviter les risques et les erreurs, lisez et comprenez les scénarios fournis ici.

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": []
  },
  "iecl04": {
    "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 Firewall Threat Defense, 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**.

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.

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.

Générer des recommandations Snort 3

Recommandations de règles Snort 3

Les recommandations de règles Snort 3 sont une fonctionnalité de réglage de sécurité qui

- ajuste automatiquement votre politique de prévention des intrusions avec des règles spécifiques à l'environnement hôte,
- active des règles supplémentaires ou ajustent l'ensemble de règles actuel en désactivant les règles pour les vulnérabilités non présentes dans votre réseau, et
- utilise la base de données de l'hôte pour déterminer les règles qui s'appliquent à votre environnement.

Fonctionnement des recommandations de règles

Le centre de gestion crée une base de données d'hôtes sur votre réseau avec des détails tels que l'adresse IP, le nom de domaine, le système d'exploitation, les services, les utilisateurs et les applications client par découverte passive. En fonction de ces informations, le système fait correspondre les vulnérabilités à chaque hôte détecté. La fonctionnalité de recommandations utilise cette base de données d'hôte pour déterminer les règles qui s'appliquent à votre environnement.

Dans Snort 3, il existe quatre niveaux de sécurité, chacun correspondant à une politique Talos spécifique :

- Niveau 1 : connectivité sur la sécurité
- Niveau de sécurité 2 : équilibre entre sécurité et connectivité
- Niveau de sécurité 3 : la sécurité prime sur la connectivité
- Niveau de sécurité 4 : détection maximale

Cochez la case **Accept Recommendation to Disable Rules** (Accepter la recommandation pour désactiver les règles) pour désactiver les règles pour les vulnérabilités introuvables sur les hôtes de votre réseau. Utilisez cette option, uniquement si vous devez supprimer votre ensemble de règles en raison d'un nombre élevé d'alertes ou pour améliorer les performances de l'inspection.

Pour en savoir plus, consultez [Règles conseillées pour Secure Firewall](#).

Avantages

- En configurant les recommandations, vous pouvez adapter votre politique de prévention des intrusions pour détecter des types de menaces spécifiques à l'aide de règles spécifiques à l'environnement d'hôte.
- Les recommandations contribuent à un processus d'intervention plus efficace en réduisant les faux positifs et les fausses négations.

Exemple de scénario d'entreprise

Un exemple de scénario d'entreprise est une implémentation de la sécurité réseau qui montre comment un grand réseau d'entreprise utilise Snort 3 comme système principal de détection et de prévention des intrusions

pour améliorer les capacités de réponse aux incidents par le biais de la génération de règles basées sur les vulnérabilités et de l'optimisation des politiques de prévention des intrusions.

Détails du scénario d'exploitation

Dans ce scénario, un grand réseau d'entreprise adopte des mesures de sécurité réseau robustes dans un paysage des menaces en pleine évolution. L'équipe de sécurité souhaite améliorer ses capacités de réponse aux incidents en générant des recommandations ou des ensembles de règles en fonction des vulnérabilités détectées dans le réseau d'hôte. Cela les aide à optimiser leurs politiques de prévention des intrusions, veillant ainsi au réseau plus efficacement.

Bonnes pratiques

- Vous devez avoir des données d'hôte précises et de haute qualité.
En raison de la nature passive de la découverte du réseau, vos appareils de défense contre les menaces doivent être placés aussi près que possible de vos hôtes protégés. Cela permet aux appareils de défense contre les menaces de surveiller le trafic réseau à destination et en provenance de ces hôtes, ce qui vous fournit des données précises sur les applications, les services et les vulnérabilités de votre réseau.
- Les périphériques doivent avoir une visibilité sur les flux de trafic est-ouest ainsi que sur les flux de trafic nord-sud pour créer un profil d'hôte précis.
- Vous pouvez créer une tâche planifiée pour mettre à jour automatiquement les recommandations.

Conditions préalables à la génération de recommandations

- Assurez-vous que des hôtes sont présents dans le système pour générer des recommandations.
- Les réseaux protégés configurés pour les recommandations doivent être mappés aux hôtes présents dans le système

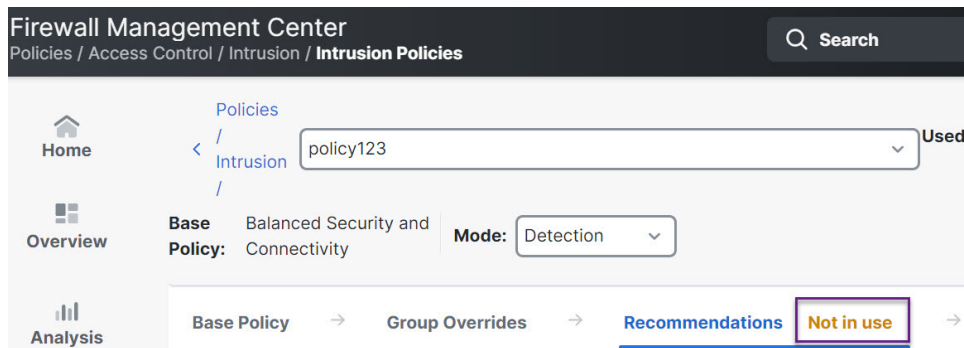
Générer des recommandations Snort 3

Générez et appliquez des recommandations de règles Snort 3 pour optimiser votre politique de prévention des intrusions en fonction de la configuration de votre réseau et des exigences de sécurité.

Les recommandations Snort 3 vous aident à configurer des politiques de prévention des intrusions avec des règles adaptées à votre environnement réseau. Le système analyse vos réseaux protégés et suggère les niveaux de sécurité et les configurations de règles appropriés.

Procédure

- | | |
|----------------|--|
| Étape 1 | Choisissez Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion. |
| Étape 2 | Cliquer sur le bouton Snort 3 Version (Version Snort 3) de la politique de prévention des intrusions. |
| Étape 3 | Cliquez sur la couche Recommendations (Not in Use) pour configurer les recommandations de règles. |



Dans la fenêtre **Cisco Recommended Rules** (Règles conseillées par Cisco), vous pouvez définir le niveau de sécurité.

Cisco Recommended Rules

Security Level (Click to select)



☐ Accept Recommendation to Disable Rules ⓘ

No Impact— No new rules will be enabled and no existing rules will be disabled.
To increase protections, please select a higher Security Level.

Protected Networks ⓘ

 Add +

Cancel

Generate

Generate and Apply

Étape 4 Cliquez pour sélectionner le niveau de sécurité.

Étape 5 (Facultatif) Cochez la case **Accept Recommendation to Disable Rules** (Accepter la recommandation pour désactiver les règles) pour désactiver les règles écrites pour les vulnérabilités introuvables sur les hôtes de votre réseau.

Utilisez cette option, uniquement si vous devez supprimer votre ensemble de règles en raison d'un nombre élevé d'alertes ou pour améliorer les performances de l'inspection.

Étape 6 Dans la liste déroulante **Protected Networks** (Réseaux protégés), choisissez les objets réseau qui doivent être inspectés par les recommandations. Par défaut, tous les réseaux IPv4 ou IPv6 sont sélectionnés si vous ne faites aucune sélection.

Cliquez sur **Add +** (Ajouter) pour créer un nouvel objet réseau de type **Host** (Hôte) ou **Network** (Réseau) et cliquez sur **Save** (Enregistrer).

Étape 7 Générer et appliquer les recommandations :

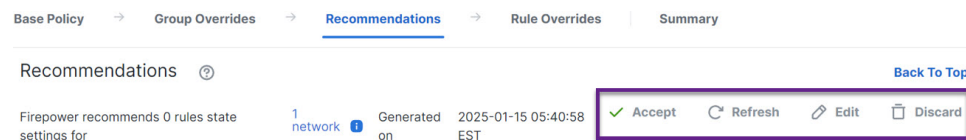
- **Generate** (Générer) : génère les recommandations pour une politique de prévention des intrusions. Cette action répertorie les règles sous **Recommended Rules (Not in use)** (Règles recommandées [non utilisées]).
- **Generate and Apply** (Générer et appliquer) : génère et applique les recommandations pour une politique de prévention des intrusions. Cette action répertorie les règles sous **Recommended Rules (Not in use)** (Règles recommandées [non utilisées]).

Les recommandations ont été générées avec succès. Un nouvel onglet de recommandation apparaît avec toutes les règles recommandées avec leurs actions recommandées correspondantes. Des filtres d'action de règle prédéfinis sont également disponibles pour cet onglet, en plus de nouvelles recommandations.

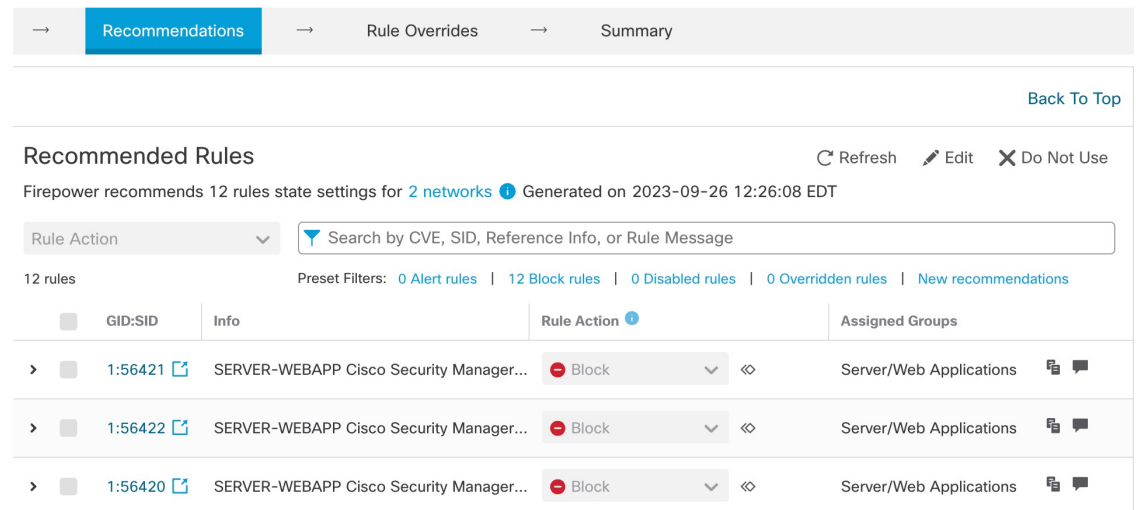
Étape 8

Vérifiez les recommandations, puis appliquez-les en conséquence :

- **Accept** (Accepter) : applique les recommandations générées précédemment pour une politique de prévention des intrusions.
- **Refresh** (Actualiser) : régénère et met à jour les recommandations de règles pour une politique de prévention des intrusions.
- **Edit** (Modifier) : ouvre la boîte de dialogue **Recommendations** (Recommandations), qui vous permet de fournir les valeurs d'entrée de recommandation, puis de générer les recommandations.
- **Discard** (Supprimer) : rétablit ou supprime les règles recommandées appliquées de la politique et supprime également l'onglet **Recommendations** (Recommandations).



Sous **All Rules** (Toutes les règles), la section Recommended Rules (Règles recommandées) affiche les règles recommandées.



Étape 9

Pour utiliser efficacement les recommandations, elles doivent être mises à jour périodiquement. Suivez ces étapes :

1. Choisissez **Système** (🔍) > **Tools (Outils)** > **Scheduling (Planification)**.
2. Cliquez sur **Add Task** (Ajouter une tâche).
3. Choisissez **Cisco Recommended Rules** (Règles conseillées par Cisco) dans la liste déroulante **Job Type** (Type de tâche).
4. Veuillez mettre à jour les champs obligatoires, au besoin.

New Task

Job Type Cisco Recommended Rules ▾

(Cisco Recommended Rules must first be configured in the selected [policies](#))Schedule task to run ☐ Once ☒ Recurring

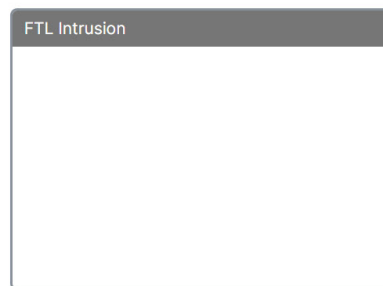
Start On January ▾ 15 ▾ 2025 ▾ America/New York

Repeat Every 1 ▾ ☐ Hours ☐ Days ☒ Weeks ☐ Months

Run At 10:00 ▾ Pm ▾

Repeat On ☒ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Job Name Update recommendations

Policies ☒ All Policies

5. Cliquez sur **Save** (Enregistrer).

Prochaine étape

Déployer les modifications de configuration Reportez-vous à [Déploiement des modifications de configuration](#)

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.