Couches des politiques d'analyse des réseaux et de prévention des intrusions

Les rubriques suivantes expliquent comment utiliser les couches dans les politiques de prévention des intrusions et d'analyse de réseau :

Principes de base des couches

Les grandes entreprises qui utilisent de nombreux périphériques gérés peuvent avoir de nombreuses politiques de prévention des intrusions et d'analyses de réseau pour répondre aux besoins uniques de différents services, de différentes unités commerciales ou, dans certains cas, de différentes entreprises. Les configurations des deux types de politiques sont contenues dans des blocs de construction appelés *couches,* que vous pouvez utiliser pour gérer efficacement plusieurs politiques.

Les couches des politiques d'analyse de réseau et de prévention des intrusions fonctionnent essentiellement de la même manière. Vous pouvez créer et modifier l'un ou l'autre des types de politique sans utiliser délibérément les couches. Vous pouvez modifier vos configurations de politiques et, si vous n'avez pas ajouté de couches d'utilisateurs à votre politique, le système inclut automatiquement vos modifications dans une seule couche configurable qui est initialement nommée *My Changes* (Mes modifications). Vous pouvez également ajouter jusqu'à 200 couches auxquelles vous pouvez configurer n'importe quelle combinaison de paramètres. Vous pouvez copier, fusionner, déplacer et supprimer des couches d'utilisateurs et, plus important encore, partager des couches d'utilisateurs individuelles avec d'autres politiques du même type.

Exigences de licence pour les couches des politiques d'analyse de réseau et de prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les couches des politiques d'analyse de réseau et de prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

La pile des couches

Les piles de couches sont composées des éléments suivants :

Couches d'utilisateur

les couches configurables par l'utilisateur; Vous pouvez copier, fusionner, déplacer ou supprimer n'importe quelle couche configurable par l'utilisateur et faire en sorte qu'elle soit partagée par d'autres politiques du même type. Cette couche comprend la couche générée automatiquement nommée initialement My Changes.

Couches intégrées

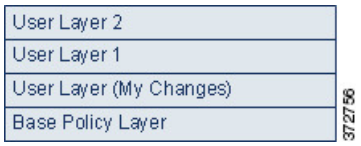
La couche de politiques de base en lecture seule. La politique de cette couche peut être une politique fournie par le système ou une politique personnalisée que vous avez créée.

Par défaut, une politique d'analyse de réseau ou de prévention des intrusions comprend une couche de politique de base et une couche Mes modifications. Vous pouvez ajouter des couches d'utilisateurs au besoin.

Chaque couche de politique contient des configurations complètes pour tous les préprocesseurs dans une politique d'analyse de réseau ou pour l'ensemble des règles de prévention des intrusions et des paramètres avancés dans une politique de prévention des intrusions. La couche de politiques de base la plus basse comprend tous les paramètres de la politique de base que vous avez sélectionnée lors de sa création. Un paramètre d'un niveau de niveau supérieur prévaut sur le même paramètre d'un niveau inférieur. Les fonctionnalités qui ne sont pas explicitement définies dans une couche *héritent* de leurs paramètres de la couche immédiatement supérieure où elles sont explicitement définies. Le système *aplatit* les couches, c'est-à-dire qu'il applique uniquement l'effet cumulatif de tous les paramètres, lorsqu'il gère le trafic réseau.

Astuces Vous pouvez créer une politique de prévention des intrusions ou d'analyse de réseau uniquement en fonction des paramètres par défaut de la politique de base. Dans le cas d'une politique de prévention des intrusions, vous pouvez également utiliser les recommandations d'état des règles Firepower si vous souhaitez adapter votre politique de prévention des intrusions aux besoins spécifiques de votre réseau surveillé.

La figure suivante montre un exemple de pile de couches qui, en plus de la couche de politique de base et de la couche initiale Mes modifications, comprend également deux couches supplémentaires configurables par *l'utilisateur, la couche d'utilisateur 1* et *la couche d'utilisateur 2*. Notez dans la figure que chaque couche configurable par l'utilisateur que vous ajoutez est initialement placée comme la couche la plus élevée de la pile. par conséquent, la couche d'utilisateur 2 dans la figure a été ajoutée en dernier et est la plus élevée dans la pile.



Que vous autorisiez ou non les mises à jour de règles à modifier votre politique, les modifications dans une mise à jour de règles ne remplacent jamais les modifications que vous apportez à une couche. En effet, les modifications dans une mise à jour de règle sont apportées à la politique de base, qui détermine les paramètres par défaut dans votre couche de politique de base; vos modifications sont toujours apportées à une couche supérieure, de sorte qu'elles remplacent toutes les modifications apportées à votre politique de base par la mise à jour d'une règle.

La couche de base

La couche de base, également appelée politique de base, d'une politique de prévention des intrusions ou d'analyse de réseau définit les paramètres par défaut pour toutes les configurations de la politique et constitue la couche la plus basse de la politique. Lorsque vous créez une nouvelle politique et modifiez un paramètre sans ajouter de nouvelles couches, la modification est stockée dans la couche Mes Modifications et remplace le paramètre de la politique de base, mais ne le modifie pas.

Politiques de base fournies par le système

Le système Firepower fournit plusieurs paires de politiques d'analyse de réseau et de politiques de prévention des intrusions. En utilisant les politiques d'analyse de réseau et de prévention des intrusions fournies par le système, vous pouvez profiter de l'expérience de Talos Intelligence Group. Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de préprocesseur, et fournit les configurations initiales pour les préprocesseurs et d'autres paramètres avancés. Vous pouvez utiliser ces politiques fournies par le système telles quelles ou vous pouvez les utiliser comme base pour des politiques personnalisées.

Si vous utilisez une politique fournie par le système comme politique de base, l'importation de mises à jour de règles peut modifier les paramètres de votre politique de base. Cependant, vous pouvez configurer une politique personnalisée pour que le système n'apporte pas automatiquement ces modifications à la politique de base fournie par le système. Cela vous permet de mettre à jour les politiques de base fournies par le système manuellement, selon un calendrier indépendant des mises à jour des règles. Dans les deux cas, les modifications apportées à votre politique de base par la mise à jour d'une règle ne modifient pas ou ne remplacent pas les paramètres de Mes modifications ou de toute autre couche.

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.

Politiques de base personnalisées

Vous pouvez utiliser une politique personnalisée comme base. Vous pouvez ajuster les paramètres de vos politiques personnalisées pour inspecter le trafic aux fins qui vous intéressent le plus. Ainsi, vous pouvez améliorer les performances de vos périphériques gérés et votre capacité à répondre efficacement aux événements qu'ils génèrent.

Si vous remplacez la politique personnalisée que vous utilisez comme base par une autre politique, ces modifications sont automatiquement utilisées comme paramètres par défaut de la politique qui utilise la base.

En outre, une mise à jour d'une règle peut avoir une incidence sur votre politique même si vous utilisez une politique de base personnalisée, car toutes les politiques ont une politique fournie par le système comme base éventuelle dans une chaîne de politiques. Si la première politique personnalisée d'une chaîne (celui qui utilise la politique fournie par le système comme base) permet aux mises à jour de règles de modifier sa politique de base, votre politique peut en être affectée.

Quelle que soit la façon dont les modifications sont apportées à votre politique de base, que ce soit par la mise à jour d'une règle ou lorsque vous modifiez une politique personnalisée que vous utilisez comme politique de base, elles ne changent pas et ne remplacent pas les paramètres de vos modifications ou de toute autre couche.

L'incidence des mises à jour des règles sur les politiques de base

Lorsque vous importez des mises à jour de règles, le système modifie les politiques d'analyse de réseau, de contrôle d'accès et de prévention des intrusions fournies par le système. Les mises à jour de règles peuvent inclure :

- paramètres modifiés du préprocesseur d'analyse de réseau
- modification des paramètres avancés dans les politiques de contrôle d'accès et de prévention des intrusions
- règles de prévention des intrusions nouvelles et mises à jour
- états modifiés pour des règles existantes
- nouvelles catégories de règles et variables par défaut

Les mises à jour de règles peuvent également supprimer des règles existantes des politiques fournies par le système.

Les modifications apportées aux variables par défaut et aux catégories de règles sont gérées au niveau du système.

Lorsque vous utilisez une politique fournie par le système comme politique de base d'analyse de réseau ou de prévention des intrusions, vous pouvez permettre aux mises à jour de règles de modifier votre politique de base qui, dans ce cas, est une copie de la politique fournie par le système. Si vous autorisez les mises à jour de règles à mettre à jour votre politique de base, une nouvelle mise à jour de règles apporte les mêmes modifications dans votre politique de base qu'elle apporte à la politique fournie par le système que vous utilisez comme politique de base. Si vous n'avez pas modifié le paramètre correspondant, un paramètre de votre politique de base détermine le paramètre de votre politique. Cependant, les mises à jour de règles ne remplacent pas les modifications que vous apportez à votre politique.

Si vous n'autorisez pas les mises à jour de règles à modifier votre politique de base, vous pouvez mettre à jour manuellement votre politique de base après avoir importé une ou plusieurs mises à jour de règles.

Les mises à jour de règles suppriment toujours les règles de prévention des intrusions que Talos supprime, quel que soit l'état des règles dans votre politique de prévention des intrusions ou si vous autorisez les mises à jour de règles à modifier votre politique de base en matière de prévention des intrusions.

Jusqu'à ce que vous redéployiez vos modifications sur le trafic réseau, les règles de vos politiques de prévention des intrusions actuellement déployées se comportent comme suit :

- Les règles de prévention des intrusions désactivées restent désactivées.
- Les règles définies sur **Générer des événements** continuent de générer des événements lorsqu'elles sont déclenchées.
- Les règles définies sur **Abandon et Générer des événements** continuent de générer des événements et d'abandonner les paquets fautifs lorsqu'elles sont déclenchées.

Les mises à jour de règles ne modifient pas une politique de base personnalisée, sauf si les deux conditions suivantes sont remplies :

- Vous permettez aux mises à jour de règles de modifier la politique de base fournie par le système de la politique parente, c'est-à-dire la politique à l'origine de la politique de base personnalisée.
- Vous n'avez pas apporté de modifications à la politique parente qui remplace les paramètres correspondants de la politique de base du parent.

Lorsque les deux conditions sont remplies, les modifications apportées à la mise à jour de la règle sont transmises à la politique enfant, c'est-à-dire à la politique qui utilise la politique de base personnalisée, lorsque vous enregistrez la politique parent.

Par exemple, si la mise à jour d'une règle active une règle de prévention des intrusions précédemment désactivée et que vous n'avez pas modifié l'état de la règle dans la politique parente en matière de prévention des intrusions, l'état modifié de la règle est transmis à la politique de base lorsque vous enregistrez la politique parente.

De même, si une mise à jour de règle modifie un paramètre de préprocesseur par défaut et que vous n'avez pas modifié le paramètre dans la politique d'analyse de réseau parent, le paramètre modifié est transmis à la politique de base lorsque vous enregistrez la politique parente.

Modification de la politique de base en cours

Vous pouvez choisir une autre politique personnalisée ou fournie par le système comme politique de base.

Vous pouvez enchaîner jusqu'à cinq politiques personnalisées, quatre d'entre elles utilisant comme politique de base l'une des quatre autres politiques créées précédemment; la cinquième doit utiliser comme base une politique fournie par le système.

Procédure

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

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

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

Étape 3 Cliquez sur **Edit** ( ) à la ligne requise de la politique de prévention des intrusions.

Étape 4 Choisir une politique de base : choisissez dans la liste déroulante **Base Policy** (Politique de base).

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Couche de recommandations Cisco

Lorsque vous générez des recommandations d'état de règles dans une politique de prévention des intrusions, vous pouvez choisir de modifier automatiquement les états de règles en fonction des recommandations.

Comme le montre la figure suivante, l'utilisation des états de règles recommandés insère une couche de recommandations Cisco intégrée en lecture seule immédiatement au-dessus de la couche de base.

Notez que cette couche est unique aux politiques de prévention des intrusions.

Si vous choisissez par la suite de ne pas utiliser les états de règles recommandés, le système supprime la couche de recommandations Cisco. Vous ne pouvez pas supprimer manuellement cette couche, mais vous pouvez l'ajouter et la supprimer en choisissant d'utiliser ou de ne pas utiliser les états de règles recommandés.

L'ajout de la couche de recommandations Cisco ajoute un lien aux recommandations Cisco sous Policy Layers (Couches des politiques) dans le panneau de navigation. Ce lien vous mène à une vue en lecture seule de la page de la couche de recommandations Cisco où vous pouvez accéder à une vue filtrée par les recommandations de la page Rules (Règles) en mode lecture seule.

L'utilisation des états de règles recommandés ajoute également un sous-lien Rules (Règles) sous le lien de recommandations Cisco dans le panneau de navigation. Le sous-lien Rules permet d'accéder en lecture seule à la page Rules (Règles) dans la couche de recommandations Cisco. Notez les éléments suivants dans cette vue :

- Lorsqu'il n'y a aucune icône d'état de règle dans la colonne d'état, l'état est hérité de la politique de base.
- Lorsqu'il n'y a pas d'icône d'état de règle dans la colonne Recommandation Cisco de cet affichage ou d'autres affichages de la page de règles, il n'y a aucune recommandation pour cette règle.

Sujets connexes

Adaptation de la prévention des intrusions à vos ressources réseau

Gestion des couches

La page Policy Layers (couches de politiques) fournit un résumé d'une page de l'ensemble de la pile de couches de votre politique d'analyse de réseau ou de prévention des intrusions. Sur cette page, vous pouvez ajouter des couches partagées et non partagées, copier, fusionner, déplacer et supprimer des couches, accéder à la page de résumé de chaque couche et accéder aux pages de configuration des configurations activées, désactivées et remplacées dans chaque couche.

Pour chaque couche, vous pouvez afficher les informations suivantes :

- si la couche est une couche d'utilisateur intégrée, partagée ou non partagée
- quelles couches contiennent les configurations les plus élevées, c'est-à-dire les configurations effectives de préprocesseur ou de paramètres avancés, par nom de fonctionnalité
- dans une politique de prévention des intrusions, le nombre de règles de prévention des intrusions dont les états sont définis dans la couche et le nombre de règles définies pour chaque état de règle.

La page Policy Layers (couches de politiques) fournit également un résumé de l'effet net de tous les préprocesseurs activés (analyse de réseau) ou des paramètres avancés (intrusion) et, pour les politiques de prévention des intrusions, les règles de prévention des intrusions.

Le nom de la fonctionnalité dans le résumé de chaque couche indique quelles configurations sont activées, désactivées, remplacées ou héritées dans la couche, comme suit :

Lorsque la fonctionnalité est...	Le nom de la fonctionnalité est...
activé dans la couche	écrit en texte brut
désactivé dans la couche	biffé
remplacée par la configuration dans une couche supérieure	écrit en italique
hérité d'une couche inférieure	absent

Vous pouvez ajouter jusqu'à 200 couches à une analyse de réseau ou à une politique de prévention des intrusions. Lorsque vous ajoutez une couche, elle apparaît comme la couche la plus élevée dans votre politique. L'état initial est Hériter pour toutes les fonctions et, dans une politique de prévention des intrusions, aucun filtrage des événements, état dynamique ou action de règle d'alerte n'est défini.

Vous donnez un nom unique à une couche configurable par l'utilisateur lorsque vous l'ajoutez à votre politique. Plus tard, vous pouvez changer le nom et, éventuellement, ajouter ou modifier une description qui est visible lorsque vous modifiez la couche.

Vous pouvez copier, déplacer un calque vers le haut ou le bas dans la zone de page des calques d'utilisateurs ou supprimer un calque d'utilisateur, y compris le calque initial My Changes. Tenez compte des considérations suivantes :

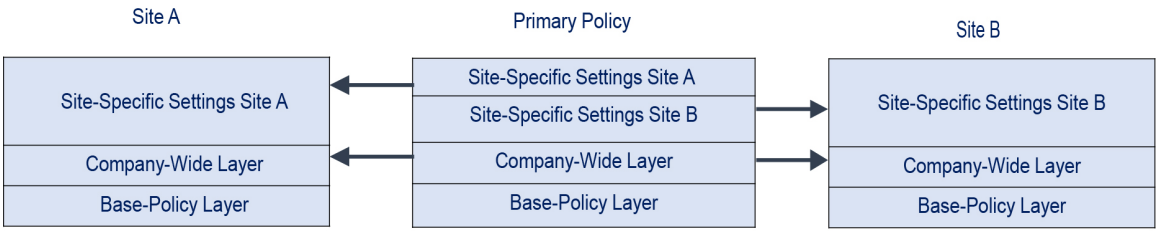
- Lorsque vous copiez une couche, la copie s'affiche comme la couche la plus élevée.
- La copie de la couche partagée crée une couche qui est initialement non partagée et que vous pouvez ensuite partager si vous le souhaitez.
- Vous ne pouvez pas supprimer une couche partagée; une couche dont le partage est activé et que vous n'avez pas partagée avec une autre politique n'est pas une couche partagée.

Vous pouvez fusionner une couche configurable par l'utilisateur avec une autre couche configurable par l'utilisateur immédiatement sous elle. Une couche fusionnée conserve tous les paramètres qui étaient propres à l'une ou l'autre des couches et accepte les paramètres de la couche supérieure si les deux couches comprennent des paramètres pour le même préprocesseur, la même règle de prévention des intrusions ou le paramètre avancé. La couche fusionnée conserve le nom de la couche inférieure. Dans la politique où vous créez une couche partageable que vous pouvez ajouter à d'autres politiques, vous pouvez fusionner une couche non partagée immédiatement au-dessus de la couche partageable avec la couche partageable, mais vous ne pouvez pas fusionner la couche partageable avec une couche non partagée en dessous. Dans une politique où vous ajoutez une couche partagée que vous avez créée dans une autre politique, vous pouvez fusionner la couche partagée avec une couche non partagée située immédiatement en dessous, et la couche résultante n'est plus partagée ; vous ne pouvez pas fusionner une couche non partagée avec une couche partagée située en dessous.

Couche partagées

Une *couche partagée* est une couche que vous ajoutez à votre politique après l'avoir créée dans une autre politique où vous autorisez son partage. Une *couche partageable* est une couche que vous autorisez à partager.

La figure suivante montre un exemple de politique principale dans laquelle vous créez la couche pour l'ensemble de l'entreprise et des couches spécifiques au site pour les sites A et B, et autorisez leur partage. Vous les ajoutez ensuite en tant que couches partagées aux politiques des sites A et B.



La couche à l'échelle de l'entreprise dans la politique principale comprend les paramètres applicables aux sites A et B. Les couches propres au site comprennent les paramètres propres à chaque site. Par exemple, dans le cas d'une politique d'analyse de réseau, le site A pourrait ne pas avoir de serveur Web sur le réseau surveillé et ne nécessiterait pas la protection ou le surdébit de traitement du préprocesseur HTTP Inspect, mais les deux sites nécessiteraient probablement un prétraitement des flux TCP. Vous pourriez activer le traitement des flux TCP dans la couche de l'entreprise que vous partagez avec les deux sites, désactiver le préprocesseur HTTP Inspect dans la couche spécifique au site que vous partagez avec le site A, et activer le préprocesseur HTTP Inspect dans la couche spécifique au site que vous partagez avec le site B. En modifiant les configurations dans une couche supérieure des politiques spécifiques au site, vous pourriez également affiner la politique pour chaque site, si nécessaire, avec des ajustements de configuration.

Il est peu probable que les paramètres de réseau simplifiés dans l'exemple de politique principale soient utiles pour surveiller le trafic, mais le temps économisé dans la configuration et la mise à jour des politiques spécifiques au site en fait une application utile des couches de politiques.

De nombreuses autres configurations de couche sont possibles. Par exemple, vous pouvez définir des niveaux de politiques par entreprise, par service, par réseau ou même par utilisateur. Dans le cas d'une politique de prévention des intrusions, vous pouvez également inclure des paramètres avancés dans une couche et les paramètres de règles dans un autre.

Vous pouvez autoriser le partage d'une couche configurable par l'utilisateur avec d'autres politiques du même type (analyse de prévention des intrusions ou de réseau). Lorsque vous modifiez une configuration dans une couche partageable et que vous validez vos modifications, le système met à jour toutes les politiques qui partagent la couche et vous fournit une liste de toutes les politiques concernées. Vous pouvez uniquement modifier les configurations des fonctionnalités dans la politique dans laquelle vous avez créé la couche.

Vous ne pouvez pas désactiver le partage pour une couche que vous avez ajoutée à une autre politique; vous devez d'abord supprimer la couche de l'autre politique ou supprimer l'autre politique.

Vous ne pouvez pas ajouter une couche partagée à une politique lorsque votre politique de base est une politique personnalisée dans laquelle la couche que vous souhaitez partager a été créée. Cela confèrerait à la politique une dépendance circulaire.

Dans un déploiement multidomaine, vous pouvez ajouter des couches partagées des politiques ascendantes aux politiques des domaines descendants.

Gestion des couches

Procédure

Étape 1 Lors de la modification de votre politique Snort 2, cliquez sur **Policy Layers** (couches de politiques) dans le panneau de navigation.

Étape 2 Vous pouvez effectuer l'une des actions de gestion suivantes dans la page Policy Layers (couches de politiques) :

- Ajouter une couche partagée d'une autre politique : cliquez sur **Add Shared Layer Ajouter** (+) (ajouter une couche partagée) à côté de User Layers (couches utilisateur), choisissez la couche dans la liste déroulante **Add Shared Layer** (ajouter une couche partagée), puis cliquez sur **OK**.
- Add an un Shared Layer (ajouter une couche non partagée) : cliquez sur Add Layer **Ajouter** (+) à côté de User Layers (couches d'utilisateurs), saisissez un **nom** et cliquez sur **OK**.
- Ajouter ou modifier la description de lacouche : cliquez sur **Edit** (✎) à côté de la couche, puis ajoutez ou modifiez la **description**.
- Autoriser le partage d'une couche avec une autre politique : cliquez sur **Edit** (✎) à côté de la couche, puis décochez la case **Partage**.
- Modifiez le nom de la couche : cliquez sur **Edit** (✎) à côté de la couche, puis modifiez le **nom**.
- Copier une couche : cliquez sur **Copier** (⧉) pour la couche.
- Supprimer une couche : cliquez sur **Supprimer** (🗑) pour la couche, puis cliquez sur **OK**.
- Fusionner deux couches : cliquez sur **Fusionner** (⧉) pour sélectionner la couche supérieure, puis cliquez sur **OK**.

- Déplacer une couche : Cliquez sur n'importe quelle zone vide dans le résumé de la couche et faites glisser jusqu'à ce que la **flèche de positionnement** pointe vers une ligne au-dessus ou en dessous de cette dernière où vous souhaitez la déplacer.

Étape 3 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Navigation dans les couches

Procédure

Étape 1 Lors de la modification de votre politique Snort 2, cliquez sur **Policy Layers** (couches de politiques) dans le panneau de navigation. Pour accéder à votre politique Snort 2, choisissez l'onglet **Policies** > **Intrusion** > **Intrusion Policies (Politiques de prévention des intrusions)**, puis cliquez sur **Snort 2** en regard de la politique que vous souhaitez modifier.

Étape 2 Vous pouvez effectuer l'une des actions suivantes pour naviguer au sein des couches :

- Accéder à la page de préprocesseur ou de paramètres avancés : Si vous souhaitez accéder à une page de configuration de préprocesseur ou de paramètres avancés au niveau de la couche, cliquez sur le nom de la fonctionnalité dans la ligne correspondant à la couche. Les pages de configuration sont en lecture seule dans la politique de base et dans les couches partagées.
- Accéder à une page de règle : Si vous souhaitez accéder à une page de configuration de règles au niveau de la couche filtrée par type d'état de règle, cliquez sur **Drop and Generate Events** (Déposer et créer des événements), **Generate Events** (Générer des événements) ou **Disabled** (Désactivé) dans le résumé de la couche. Aucune règle ne s'affiche si la couche ne contient aucune règle définie sur l'état de règle sélectionné.
- Afficher la page d'informations sur la politique : si vous souhaitez afficher la page d'informations sur la politique, cliquez sur **Policy Summary** (Résumé de la ^politique) dans le panneau de navigation.
- Afficher la page de résumé d'une couche : si vous souhaitez afficher la page de résumé d'une couche, cliquez sur le nom de la couche dans la rangée correspondante ou cliquez sur **Edit** () à côté d'une couche utilisateur. Vous pouvez également cliquer sur **Afficher** () pour accéder à la page de résumé en lecture seule d'une couche partagée.

Étape 3 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Les règles d'intrusion au sein des couches

Vous pouvez afficher les paramètres de couche individuelle dans la page Rules de la couche ou l'effet net de tous les paramètres dans l'affichage de la politique de la page Rules. Lorsque vous modifiez les paramètres de règles dans la vue de politique de la page Rules, vous modifiez la couche configurable par l'utilisateur la plus élevée dans la politique. Vous pouvez passer à une autre couche à l'aide de la liste déroulante des couches sur n'importe quelle page de règles.

Le tableau suivant décrit les effets de la configuration du même type de paramètres dans plusieurs couches.

Tableau 1 : Réglages de la règle des couches

Vous pouvez définir...	De ce type de paramètre...	Pour...
Un	État de la règle	remplacer un ensemble d'états pour la règle dans une couche inférieure et ignorer tous les seuils, les suppressions, les états de règles basés sur le débit et les alertes pour cette règle configurée dans les couches inférieures. Si vous souhaitez qu'une règle hérite de l'état de la politique de base ou d'une couche inférieure, définissez l'état de la règle sur Hériter. Notez que lorsque vous travaillez sur la page des règles de politique de prévention des intrusions, vous ne pouvez pas définir un état de règle sur Hériter, car la page des règles de politique de prévention des intrusions est une vue composée de l'effet net de tous les paramètres de règles.
Un	alerte SNMP de seuil	remplacer un paramètre du même type pour la règle dans une couche inférieure. Notez que la définition d'un seuil remplace tout seuil existant pour la règle dans la couche.
un ou plusieurs	état de règle basée sur le débit de suppression	combiner de manière cumulative des paramètres du même type pour chaque règle sélectionnée jusqu'au premier niveau, où un état de règle est défini pour la règle. Les paramètres situés sous la couche dans laquelle un état de règle est défini sont ignorés.
un ou plusieurs	Commentaire	Ajouter un commentaire à la règle Les commentaires sont propres à une règle et non à une politique ou à une couche. Vous pouvez ajouter un ou plusieurs commentaires à une règle dans n'importe quelle couche.

Par exemple, si vous définissez un état de règle sur Supprimer et Générer des événements dans une couche et sur Désactivé dans une couche supérieure, la page des règles de politique d'intrusion indique que la règle est désactivée.

Dans un autre exemple, si vous définissez une suppression basée sur la source pour une règle à 192.168.1.1 dans une couche et que vous définissez également une suppression basée sur la destination pour la règle à 192.168.1.2 dans une autre couche, la page Rules (Règles) indique que les est de supprimer les événements pour l'adresse source 192.168.1.1 et l'adresse de destination 192.168.1.2. Notez que les paramètres d'état de suppression et de règle basés sur le débit combinent de manière cumulative des paramètres du même type pour chaque règle sélectionnée jusqu'à la première couche où un état de règle est défini pour la règle. Les paramètres situés sous la couche dans laquelle un état de règle est défini sont ignorés.

Un code de couleur sur chaque page de règles pour une couche spécifique indique si l'état effectif est dans la couche supérieure, inférieure ou dans la couche actuelle, comme suit :

- rouge : l'état effectif se trouve dans une couche supérieure
- jaune : l'état effectif se trouve dans une couche inférieure
- non grisé : l'état effectif se trouve dans le calque actuel

Étant donné que la page des règles de la politique de prévention des intrusions est une vue composée de l'effet net de tous les paramètres de règles, les états des règles ne sont pas codés par couleur sur cette page.

Configuration des règles d'intrusion dans les couches

Dans une politique de prévention des intrusions, vous pouvez définir l'état de règle, le filtrage des événements, l'état dynamique, les alertes et les commentaires de règle d'une règle dans n'importe quelle couche configurable par l'utilisateur. Après avoir accédé à la couche où vous souhaitez apporter vos modifications, ajoutez les paramètres sur la page de règles de la couche de la même façon que vous le feriez pour la page de règles de la politique de prévention des intrusions.

Procédure

Étape 1 Lors de la modification de votre politique de prévention des intrusions Snort 2, développez **Policy Layers** (couches de politiques) dans le panneau de navigation.

Étape 2 Développez la couche de politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Rules** (Règles) immédiatement sous la couche de politiques que vous souhaitez modifier.

Étape 4 Modifiez l'un des paramètres décrits en Réglage des politiques de prévention des intrusions à l'aide de règles.

Astuces Pour supprimer un paramètre individuel d'une couche modifiable, double-cliquez sur le message de règle dans la page Rules (règles) pour que la couche affiche les détails de la règle. Cliquez sur le bouton **Delete** (supprimer) à côté du paramètre que vous souhaitez supprimer, puis cliquez deux fois sur **OK**.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Suppression des paramètres de règles de plusieurs couches

Vous pouvez supprimer simultanément un type spécifique de filtre d'événements, d'état dynamique ou d'alerte de plusieurs couches dans votre politique de prévention des intrusions. Le système supprime le paramètre sélectionné et copie les autres paramètres de la règle vers la couche modifiable la plus élevée de la politique.

Le système supprime le type de paramètre vers le bas dans chaque couche où il est défini jusqu'à ce qu'il supprime tous les paramètres ou qu'il rencontre une couche où un état de règle est défini pour la règle. Dans ce dernier cas, il supprime le paramètre de ce calque et arrête de supprimer le type de paramètre.

Lorsque le système rencontre le type de paramètre dans une couche partagée ou dans la politique de base, et si la couche la plus élevée de la politique est modifiable, le système copie les paramètres restants et l'état de la règle dans cette couche modifiable. Sinon, si la couche la plus élevée dans la politique est une couche partagée, le système crée une nouvelle couche modifiable au-dessus de la couche partagée et copie les paramètres restants et l'état de la règle dans cette couche modifiable.

Remarque La suppression des paramètres de règle dérivés d'une couche partagée ou de la politique de base fait en sorte que toutes les modifications apportées à cette règle par les couches inférieures ou la politique de base sont ignorées. Pour cesser d'ignorer les modifications des couches inférieures ou de la politique de base, définissez l'état de la règle sur **Hériter** dans la page de résumé de la couche supérieure.

Procédure

Étape 1 Lors de la modification de votre politique de prévention des intrusions Snort 2, cliquez sur **Rules** immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation. Pour accéder à votre politique Snort 2, choisissez l'onglet **Policies** > **Intrusion** > **Intrusion Policies** (Politiques de prévention des intrusions), puis cliquez sur **Snort 2** en regard de la politique que vous souhaitez modifier.

Astuces Vous pouvez également sélectionner **Policy** dans la liste déroulante des couches sur la page des règles pour n'importe quelle couche ou cliquer sur **Manage Rules** dans la page Policy Information.

Étape 2 Choisissez la ou les règles pour lesquelles vous souhaitez supprimer plusieurs paramètres :

- Choix de règles spécifiques : si vous souhaitez sélectionner des règles spécifiques, cochez la case à côté de chaque règle.
- Tout choisir : si vous souhaitez sélectionner toutes les règles de la liste actuelle, cochez la case en haut de la colonne.

Étape 3 Choisissez une des options suivantes :

- **Filtrage des événements** > **Supprimer les seuils**
- **Filtrage des événements** > **Supprimer les suppressions**
- **État dynamique** > **Supprimer les états des règles basées sur les débits**
- **Alertes** > **Supprimer les alertes SNMP**

Remarque La suppression des paramètres de règle dérivés d'une couche partagée ou de la politique de base fait en sorte que toutes les modifications apportées à cette règle par les couches inférieures ou la politique de base sont ignorées. Pour cesser d'ignorer les modifications des couches inférieures ou de la politique de base, définissez l'état de la règle sur **Hériter** dans la page de résumé de la couche supérieure.

Étape 4 Cliquez sur **OK**.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Acceptation des modifications de règles à partir d'une politique de base personnalisée

Lorsqu'une politique d'analyse de réseau personnalisée ou de prévention des intrusions où vous n'avez pas ajouté de couches utilise une autre politique personnalisée comme politique de base, vous devez définir une règle pour hériter de son état de règle dans les cas suivants :

- vous supprimez un filtre d'événements, un état dynamique ou une alerte SNMP défini pour la règle dans la politique de base, *et*
- vous souhaitez que la règle accepte les modifications ultérieures que vous lui apporterez dans l'autre politique personnalisée que vous utilisez comme politique de base

Procédure

Étape 1 Lors de la modification de votre politique de prévention des intrusions Snort 2, développez **Policy Layers** (couches de politiques) dans le panneau de navigation.

Étape 2 Développez **Mes modifications**.

Étape 3 Cliquez sur le lien **Rules (règles)** immédiatement sous **My Changes** (Mes modifications).

Étape 4 Choisissez la ou les règles dont vous souhaitez accepter les paramètres. Vous avez les choix suivants :

- Choisissez des règles spécifiques – Si vous souhaitez sélectionner des règles spécifiques, cochez la case à côté de chaque règle.
- Choisir toutes les règles : Si vous souhaitez sélectionner toutes les règles de la liste actuelle, cochez la case en haut de la colonne.

Étape 5 Choisissez **Hériter** dans la liste déroulante **Rule State** (état des règles).

Étape 6 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Préprocesseurs et paramètres avancés dans les couches

Vous utilisez des mécanismes similaires pour configurer les préprocesseurs dans une politique d'analyse de réseau et les paramètres avancés dans une politique de prévention des intrusions. Vous pouvez activer et désactiver les préprocesseurs dans la page des paramètres d'analyse de réseau et les paramètres avancés de la politique de prévention des intrusions dans la page des paramètres avancés de la politique de prévention des intrusions. Ces pages fournissent également des résumés des états effectifs pour toutes les fonctionnalités pertinentes. Par exemple, si le préprocesseur SSL de l'analyse de réseau est désactivé dans une couche et activé dans une couche supérieure, la page Settings (paramètres) indique qu'il est activé. Les modifications apportées sur ces pages apparaissent dans la couche supérieure de la politique. Il convient de souligner que le préprocesseur de l'orifice arrière n'a pas d'options configurables par l'utilisateur.

Vous pouvez également activer ou désactiver les préprocesseurs ou les paramètres avancés et accéder à leurs pages de configuration sur la page de résumé d'une couche configurable par l'utilisateur. Sur cette page, vous pouvez modifier le nom et la description de la couche et configurer si vous souhaitez partager la couche avec d'autres politiques du même type. Vous pouvez passer à la page de résumé pour une autre couche en sélectionnant le nom de la couche sous les **couches de politiques** dans le panneau de navigation.

Lorsque vous activez un préprocesseur ou un paramètre avancé, un sous-lien vers la page de configuration de cette fonctionnalité s'affiche sous le nom de la couche dans le panneau de navigation et un **Edit** (✎) s'affiche à côté de la fonctionnalité sur la page de résumé de la couche. ceux-ci disparaîtront lorsque vous désactivez la fonctionnalité dans la couche ou que vous la définissez sur Hériter.

La définition de l'état (activé ou désactivé) pour un préprocesseur ou un paramètre avancé remplace les paramètres d'état et de configuration de cette fonctionnalité dans les couches inférieures. Si vous souhaitez qu'un préprocesseur ou un paramètre avancé hérite de son état et de sa configuration de la politique de base ou d'une couche inférieure, définissez-le sur **Inherit** (hériter). Notez que l'option Hériter de la sélection n'est pas disponible lorsque vous travaillez dans la page Paramètres ou Paramètres avancés. Notez également que si vous héritez d'une fonctionnalité qui est actuellement activée, le sous-lien de la fonctionnalité dans le panneau de navigation et l'icône de modification sur la page de configuration ne s'affichent plus.

Le système utilise la configuration de la couche la plus élevée où la fonctionnalité est activée. À moins que vous ne modifiez explicitement la configuration, le système utilise la configuration par défaut. Par exemple, si vous activez et modifiez le préprocesseur d'analyse de réseau DCE/RPC dans une couche, et que vous l'activez également mais ne modifiez pas dans une couche supérieure, le système utilise la configuration par défaut dans la couche supérieure.

Un code de couleur sur chaque page de résumé de couche indique si la configuration réelle se trouve dans une couche supérieure, inférieure ou actuelle, comme suit :

- rouge : la configuration réelle se trouve dans une couche supérieure
- jaune : la configuration réelle se trouve dans une couche inférieure
- non ombrée : la configuration réelle se trouve dans la couche actuelle

Étant donné que les pages Settings (Paramètres) et Advanced Settings (Paramètres avancés) sont des vues composées de tous les paramètres pertinents, ces pages n'utilisent pas de code de couleur pour indiquer les emplacements des configurations effectives.

Configuration des préprocesseurs et des paramètres avancés dans les couches

Procédure

Étape 1 Lors de la modification de votre politique Snort 2, développez les **Couches de politiques** dans le panneau de navigation, puis cliquez sur le nom de la couche que vous souhaitez modifier.

Étape 2 Vous avez les choix suivants :

- Modifiez le **nom** de la couche.
- Ajoutez ou modifiez la **Description**.
- Cochez ou décochez la case **Sharing** (Partage) pour préciser si une couche peut être partagée avec une autre politique.
- Pour accéder à la page de configuration pour un préprocesseur ou un paramètre avancé activé, cliquez sur **Edit** (✎) ou sur le sous-lien de fonctionnalité.
- Pour désactiver un paramètre de préprocesseur ou avancé de la couche actuelle, cliquez sur **Disabled** (désactivé) à côté de la fonctionnalité.
- Pour activer un paramètre de préprocesseur ou avancé de la couche actuelle, cliquez sur **Enabled** (activé) à côté de la fonctionnalité.
- Pour hériter de l'état et de la configuration du préprocesseur/paramètres avancés des paramètres de la couche la plus élevée, sous la couche actuelle, cliquez sur **Inherit** (Hériter).

Étape 3 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

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.