Réglage du rendement de la prévention des intrusions

Les rubriques suivantes décrivent comment affiner les performances de prévention des intrusions :

À propos du réglage des performances de la prévention des intrusions

Cisco fournit plusieurs fonctionnalités pour améliorer les performances de votre système lors de l'analyse du trafic à la recherche de tentatives d'intrusions. Vous pouvez réaliser les actions suivantes :

- Spécifiez le nombre de paquets à autoriser dans la file d'attente des événements. Vous pouvez également, avant et après le réassemblage des flux, activer ou désactiver l'inspection des paquets qui seront recréés en flux plus importants.
- Remplacez les limites de correspondance et de récursivité par défaut sur PCRE qui sont utilisées dans les règles de prévention des intrusions pour examiner le contenu de la charge utile des paquets.
- Choisissez que le moteur de règles journalise plus d'un événement par paquet ou flux de paquets lorsque plusieurs événements sont générés, ce qui vous permet de recueillir des informations au-delà de l'événement signalé.

- Trouvez un équilibre entre la sécurité et le besoin de maintenir la latence des périphériques à un niveau acceptable grâce à un seuil de latence des paquets et des règles.
- Configurez les paramètres de base sur la façon dont les périphériques surveillent et communiquent leurs propres performances. Cela vous permet de préciser les intervalles auxquels le système met à jour les statistiques de performance sur vos périphériques.

Vous configurez ces paramètres de performance pour chaque politique de contrôle d'accès et ils s'appliquent à toutes les politiques de prévention des intrusions invoquées par cette politique de contrôle d'accès parente.

Licence requise pour le réglage du rendement de la prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour le réglage du rendement de la prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Administrateur d’accès
- Administrateur de réseau

Limitation de la correspondance entre les schémas des intrusions

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancées** (**Politiques** > **Contrôle d'accès** > **Modifier** > **Plus** > **Paramètres avancés**).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** ( ) à côté de **Performance Settings** (Paramètres de performance).

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Cliquez sur **Limites de correspondance de modèles** dans la fenêtre contextuelle **Paramètres de performance**.

Étape 4 Saisissez une valeur pour le nombre maximal d'événements à mettre en file d'attente dans le champ **Nombre maximal d'états de signatures à analyser par paquet**.

Étape 5 Pour désactiver l'inspection des paquets qui seront recréés en flux de données plus volumineux avant et après le réassemblage des flux dans Snort 2, cochez la case **Disable Content Checks on Traffic Subject to future Reassembly** (Désactiver les vérifications de contenu sur le trafic sujet à un réassemblage futur). L'inspection avant et après le assemblage nécessite une surcharge de traitement plus importante et peut réduire les performances.

Important Dans Snort 3, les paramètres de la case à cocher **Désactiver les vérifications de contenu sur le trafic sujet à un réassemblage futur** sont :

- Cochée : indique la détection de la charge utile TCP avant le réassemblage. Cela comprend l'inspection des paquets avant et après le réassemblage du flux. Ce processus nécessite plus de trafic de traitement et peut réduire les performances.
- Non cochée : indique la détection de la charge utile TCP après le réassemblage.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Remplacements des limites de l'expression régulière pour les règles d'intrusion

Les limites de l'expression régulière par défaut assurent un niveau de performance minimal. Le dépassement de ces limites peut accroître la sécurité, mais peut également avoir un impact considérable sur les performances en autorisant l'évaluation des paquets par rapport à des expressions régulières inefficaces.

Mise en garde N'outrepassez pas les limites PCRE par défaut à moins d'être un rédacteur de règles de prévention des intrusions expérimenté et de connaître les incidences des modèles dégradés.

Tableau 1 : Options de contrainte d'expression régulière

Option	Description
Faire correspondre à l'état limite	Spécifie s'il faut remplacer la **limite** de correspondance . Vous avez les options suivantes : • sélectionnez **Default** (par défaut) pour utiliser la valeur configurée pour la **limite** de correspondance. • sélectionnez **Illimité** pour autoriser un nombre illimité de tentatives. • sélectionnez **Personnalisé** pour spécifier une limite de 1 ou plus pour la **Limite de correspondance** ou spécifiez 0 pour désactiver complètement les évaluations de correspondance PCRE
Faire correspondre à la limite	Spécifie le nombre de tentatives de correspondre à un modèle défini dans une expression régulière PCRE.
Faire correspondre à l'état limite de récursivité	Spécifie s'il faut remplacer la **limite de récursivité** de la correspondance . Vous avez les options suivantes : • sélectionnez **Default** (par défaut) pour utiliser la valeur configurée pour la **limite de récursivité** de correspondance. • sélectionnez **Illimité** pour autoriser un nombre illimité de récursivités. • sélectionnez **Personnalisé** pour spécifier une limite égale ou supérieure à 1 pour la **limite de récursivité de correspondance** ou spécifiez 0 pour désactiver complètement les récursions PCRE Notez que pour que la **limite de récursivité de correspondance** soit significative, elle doit être inférieure à la **limite de correspondance**.
Faire correspondre à la limite de récursivité	Spécifie le nombre de récursions lors de l'évaluation d'une expression régulière PCRE par rapport à la charge utile du paquet.

Sujets connexes

Présentation : le mot-clé pcre

Remplacement des limites de l'expression régulière pour les règles d'intrusion

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** ( ) à côté de **Performance Settings** (Paramètres de performance).

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Cliquez sur **Normal Expression Limits** (Limites d'expression normale) dans la fenêtre contextuelle **Performance Settings** (Paramètres de performance).

Étape 4 Vous pouvez modifier n'importe quelle option, comme décrit dans Remplacements des limites de l'expression régulière pour les règles d'intrusion, à la page 4.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Limites de génération d'événements d'intrusion par paquet

Lorsque le moteur de règles de prévention des intrusions évalue le trafic en fonction des règles, il place les événements générés pour un paquet ou flux de paquets donné dans une file d'attente des événements, puis signale les principaux événements de la file d'attente à l'interface utilisateur. Lors de la configuration des limites de journalisation des incidents d'intrusion, vous pouvez préciser le nombre d'événements qui peuvent être placés dans la file d'attente et combien sont journalisés, et sélectionner les critères pour déterminer l'ordre des événements dans la file d'attente.

Tableau 2 : Options de limites de journalisation des incidents d'intrusion

Option	Description
Nombre maximal d'événements stockés par paquet	Le nombre maximal d'événements qui peuvent être stockés pour un paquet ou flux de paquets donné.

Option	Description
Nombre maximal d'événements journalisés par paquet	Le nombre d'événements enregistrés pour un paquet ou flux de paquets donné. Le nombre ne peut pas dépasser la valeur **Nombre maximal d'événements stockés par paquet**.
Prioriser la journalisation des événements par	Valeur utilisée pour déterminer l'ordre des événements dans la file d'attente des événements. L'événement ordonné le plus élevé est signalé par l'intermédiaire de l'interface utilisateur. Vous avez le choix entre : • `priority` (priorité), qui classe les événements dans la file d'attente en fonction de leur priorité. • `content_length` (longueur du contenu), qui classe les événements en fonction de la correspondance de contenu identifié la plus longue. Lorsque les événements sont classés en fonction de la longueur du contenu, les événements liés aux règles ont toujours la priorité sur les événements liés au décodeur et au préprocesseur.

Limitation des incidents d'intrusion générés par paquet

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** (✎) à côté de **Performance Settings** (Paramètres de performance).

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Cliquez sur **Intrusion Event Logging Limits** (Limites d'enregistrement des incidents d'intrusion) dans la fenêtre contextuelle **Performance Settings** (Paramètres de rendement).

Étape 4 Vous pouvez modifier n'importe quelle option dans Limites de génération d'événements d'intrusion par paquet, à la page 5.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configuration du seuil de latence des règles de paquets et d'intrusion

Chaque politique de contrôle d'accès comporte des paramètres basés sur la latence qui utilisent un seuil pour gérer les performances de traitement des paquets et des règles.

Le seuil de latence des paquets mesure le temps total écoulé depuis le traitement d'un paquet par les décodeurs, les préprocesseurs et les règles applicables, et interrompt l'inspection du paquet si le temps de traitement dépasse un seuil configurable.

Le seuil de latence des règles mesure le temps écoulé nécessaire à chaque règle pour traiter un paquet individuel, suspend la règle en question ainsi qu'un groupe de règles connexes pendant un temps donné si le temps de traitement dépasse le seuil de latence de la règle un nombre de fois consécutives configurables et restaure le à l'expiration de la suspension.

Paramètres de performance en fonction de la latence

Par défaut, le système utilise les paramètres de performance basés sur la latence de la dernière mise à jour des règles de prévention des intrusions déployées sur votre système.

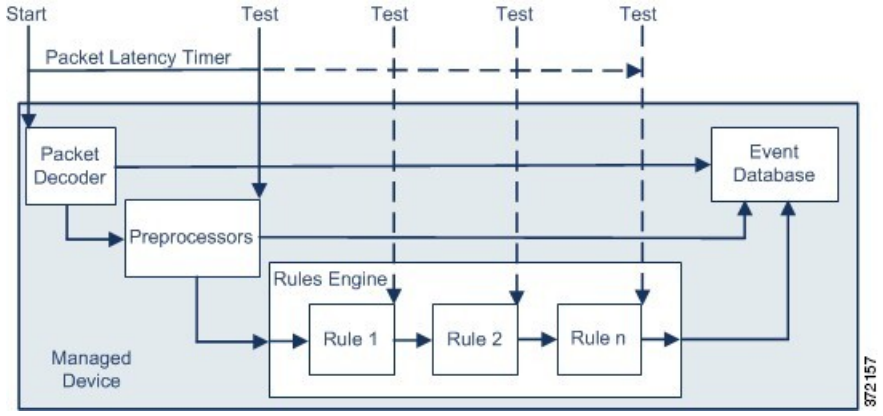
Les paramètres de latence qui sont réellement appliqués dépendent du niveau de sécurité de la politique d'analyse de réseau (NAP) associée à la politique de contrôle d'accès. En général, il s'agit de la politique Politique d'analyse de réseau (NAP) par défaut. Toutefois, si des règles d'analyse de réseau personnalisées sont configurées et si l'une d'entre elles spécifie une politique d'analyse de réseau (NAP) plus sécurisée que la politique d'analyse de réseau (NAP) par défaut, les paramètres de latence sont basés sur la politique d'analyse de réseau (NAP) la plus sécurisée parmi les règles personnalisées. Si la politique d'analyse de réseau (NAP) par défaut ou des règles personnalisées font appel à une politique d'analyse de réseau (NAP) personnalisée, le niveau de sécurité utilisé dans l'évaluation est celui de la politique de base fournie par le système sur lequel chaque politique d'analyse de réseau (NAP) personnalisée est basée.

Ce qui précède est vrai, que le seuil effectif et/ou les configurations d'analyse de réseau soient hérités ou configurés directement dans la politique.

Seuil de latence des paquets

Le seuil de latence des paquets mesure le temps écoulé, pas seulement le temps de traitement, afin de refléter avec plus de précision le temps réel nécessaire à la règle pour traiter un paquet. Cependant, le seuil de latence est une implémentation logicielle de la latence qui n'applique pas un calendrier strict.

Le compromis pour les avantages en matière de performance et de latence dérivés du seuil de latence est que les paquets non inspectés pourraient contenir des attaques. Une minuterie démarre pour chaque paquet au début du traitement du décodeur. La synchronisation se poursuit jusqu'à la fin du traitement du paquet ou jusqu'à ce que la durée de traitement dépasse le seuil à un point de test de synchronisation.



Comme l'illustre la figure ci-dessus, la synchronisation de la latence des paquets est testée aux points de test suivants :

- après l'achèvement de tous les traitements du décodeur et du préprocesseur et avant le début du traitement des règles
- après le traitement par chaque règle

Si le temps de traitement dépasse le seuil à un point de test, l'inspection des paquets s'arrête.

Astuces Le temps total de traitement des paquets ne comprend pas les heures de réassemblage des flux TCP de routine ou des fragments IP.

Le seuil de latence des paquets n'a aucun effet sur les événements déclenchés par un décodeur, un préprocesseur ou une règle qui traite le paquet. Tout décodeur, préprocesseur ou règle applicable se déclenche normalement jusqu'à ce qu'un paquet soit entièrement traité ou jusqu'à la fin du traitement des paquets parce que le seuil de latence est dépassé, selon la première de ces éventualités. Si une règle de suppression détecte une intrusion dans un déploiement en ligne, elle déclenche un événement et le paquet est abandonné.

Remarque Aucun paquet n'est évalué par rapport aux règles une fois que le traitement de ce paquet a cessé en raison d'une violation du seuil de latence des paquets. Une règle qui aurait déclenché un événement ne peut pas déclencher cet événement et, pour les règles de suppression, ne peut pas abandonner le paquet.

Le seuil de latence des paquets peut améliorer les performances du système dans les déploiements passifs et en ligne et peut réduire la latence dans les déploiements en ligne, en arrêtant l'inspection des paquets qui nécessitent un temps de traitement excessif. Ces gains de performance peuvent se produire lorsque, par exemple :

- Pour les déploiements passifs et en ligne, l'inspection successive d'un paquet par plusieurs règles nécessite beaucoup de temps
- Pour les déploiements en ligne, une période de faible performance du réseau, par exemple lorsqu'un utilisateur télécharge un fichier extrêmement volumineux, ralentit le traitement des paquets

Dans un déploiement passif, l'arrêt du traitement des paquets peut ne pas contribuer à restaurer les performances du réseau, car le traitement passe simplement au paquet suivant.

Remarques sur le seuil de latence des paquets

Par défaut, les paramètres de performance basés sur la latence pour la gestion des paquets sont désactivés. Vous pouvez choisir de l'activer. Cependant, Cisco vous recommande de ne pas modifier la valeur par défaut du paramètre de seuil.

Les informations de cette rubrique s'appliquent uniquement si vous choisissez de spécifier des valeurs personnalisées.

Tableau 3 : Option de seuil de latence des paquets

Option	Description
Seuil (microsecondes)	Spécifie l'heure, en microsecondes, à laquelle l'inspection d'un paquet prend fin.

Activation du seuil de latence des paquets

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** ( ) à côté de **Latency-Based Performance Settings** (Paramètres de performance basés sur la latence).

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Packet Management** (gestion des paquets) dans la fenêtre contextuelle **Latency-Based Performance Settings** (paramètres de performance basés sur la latence).

Étape 4 Cochez la case **Enabled** (activer).

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configuration du seuil de latence des paquets

Par défaut, les paramètres de performance basés sur la latence pour la gestion des paquets sont désactivés. Vous pouvez choisir de l'activer. Cependant, Cisco vous recommande de ne pas modifier la valeur par défaut du paramètre de seuil.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** (✎) à côté de **Latency-Based Performance Settings** (Paramètres de performance basés sur la latence).

System (⚙) > **Monitoring (surveillance)** > **Statistics (statistiques)**

Étape 3 Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 4 Cliquez sur **Packet Management** (gestion des paquets) dans la fenêtre contextuelle **Latency-Based Performance Settings** (paramètres de performance basés sur la latence).

Par défaut, l'option **Installed Rule Update** (mise à jour des règles installée) est sélectionnée. Il est conseillé d'utiliser cette valeur par défaut.

Les valeurs affichées ne reflètent pas les paramètres automatisés.

Étape 5 Si vous choisissez d'indiquer des valeurs personnalisées :

- Cochez la case **Enabled** (activé) et consultez Remarques sur le seuil de latence des paquets, à la page 9 pour connaître les paramètres de **seuil** minimaux recommandés.
- Vous devez préciser des valeurs personnalisées dans les onglets de gestion des paquets et des règles.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Seuil de latence des règles

Le seuil de latence des règles mesure le temps écoulé, pas seulement le temps de traitement, afin de refléter plus précisément le temps réel nécessaire à la règle pour traiter un paquet. Cependant, le seuil de latence est une implémentation logicielle de la latence qui n'applique pas un calendrier strict.

Le compromis pour les avantages en matière de performance et de latence dérivés du seuil de latence est que les paquets non inspectés pourraient contenir des attaques. Une minuterie mesure le temps de traitement chaque fois qu'un paquet est traité selon un groupe de règles. Chaque fois que le temps de traitement de la règle dépasse un seuil de latence de règle spécifié, le système incrémente un compteur. Si le nombre de dépassements de seuil consécutifs atteint un nombre déterminé, le système effectue les actions suivantes :

- suspend les règles pendant la période spécifiée
- déclenche un événement indiquant que les règles ont été suspendues

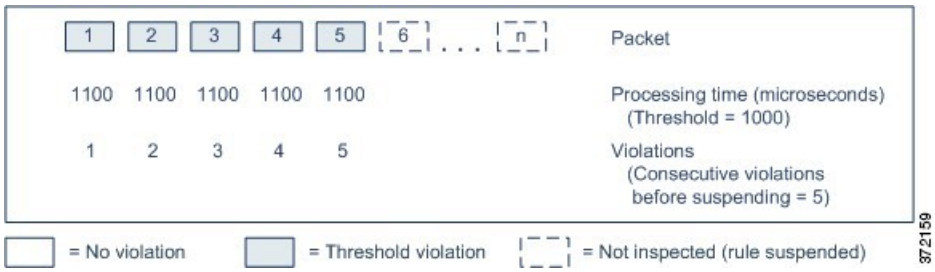
- réactive les règles à l'expiration de la suspension.
- déclenche un événement indiquant que les règles ont été réactivées

Le système remet le compteur à zéro lorsque le groupe de règles a été suspendu ou lorsque les violations aux règles ne sont pas consécutives. Autoriser certaines violations consécutives avant de suspendre les règles vous permet d'ignorer des violations occasionnelles de règles qui pourraient avoir un impact négligeable sur les performances et de vous concentrer sur l'impact plus important des règles qui dépassent à plusieurs reprises le seuil de latence des règles.

L'exemple suivant montre cinq temps de traitement de règle consécutifs qui n'entraînent pas la suspension de règle.

Dans l'exemple ci-dessus, le temps requis pour traiter chacun des trois premiers paquets dépasse le seuil de latence de la règle de 1000 microsecondes, et le compteur de violations augmente à chaque violation. Le traitement du quatrième paquet ne dépasse pas le seuil et le compteur des violations est réinitialisé à zéro. Le sixième paquet viole le seuil et le compteur de violations redémarre à un.

L'exemple suivant montre cinq temps de traitement de règle consécutifs qui entraînent une suspension de règle.



Dans le deuxième exemple, le temps nécessaire pour traiter chacun des cinq paquets enfreint le seuil de latence de la règle de 1 000 microsecondes. Le groupe de règles est suspendu, car le temps de traitement de la règle de 1100 microsecondes pour chaque paquet dépasse le seuil de 1000 microsecondes pour les cinq violations consécutives spécifiées. Les paquets suivants, représentés dans la figure par les paquets 6 à n, ne sont pas examinés en fonction des règles de suspension avant l'expiration de la suspension. Si plus de paquets se produisent après la réactivation des règles, le compteur de violations recommence à zéro.

Le seuil de latence des règles n'a aucun effet sur les incidents d'intrusion déclenchés par les règles qui traitent le paquet. Une règle déclenche un événement pour toute intrusion détectée dans le paquet, que le temps de traitement de la règle dépasse ou non le seuil. Si la règle qui détecte l'intrusion est une règle de suppression dans un déploiement en ligne, le paquet est abandonné. Lorsqu'une règle de suppression détecte une intrusion dans un paquet qui entraîne la suspension de la règle, la règle de suppression déclenche un incident d'intrusion, le paquet est abandonné et cette règle ainsi que toutes les règles connexes sont suspendues.

Remarque Les paquets ne sont pas évalués par rapport aux règles suspendues. Une règle suspendue qui aurait déclenché un événement ne peut pas déclencher cet événement et, pour les règles de suppression, ne peut pas abandonner le paquet.

Le seuil de latence des règles peut améliorer les performances du système dans les déploiements passifs et en ligne, et peut réduire la latence dans les déploiements en ligne, en suspendant les règles qui prennent le plus de temps à traiter les paquets. Les paquets ne sont pas évalués à nouveau par rapport aux règles suspendues avant l'expiration d'un délai configurable, ce qui donne au périphérique surchargé le temps de récupérer. Ces gains de performance peuvent se produire lorsque, par exemple :

- des règles écrites à la hâte et en grande partie non testées nécessitent un temps de traitement excessif
- une période de piètre performance du réseau, quand quelqu'un télécharge un fichier extrêmement volumineux, retarde l'inspection des paquets

Remarques sur le seuil de latence des règles

Par défaut, les paramètres de rendement basés sur la latence pour le traitement des paquets et des règles sont automatiquement remplis par la dernière mise à niveau des règles d'intrusion déployées, et il est conseillé de ne pas modifier la valeur par défaut.

Les informations de cette rubrique s'appliquent uniquement si vous choisissez de spécifier des valeurs personnalisées.

Le seuil de latence des règles suspend les règles pendant la durée spécifiée par l'attribut **Suspension Time** (Temps de suspension) lorsque la durée nécessaire aux règles pour traiter un paquet dépasse le **Threshold** (Seuil) le nombre de fois consécutives précisé par **Consécutive Threshold Violations Before Suspending Rule** (Violations consécutives du seuil avant la suspension de la règle).

Vous pouvez activer la règle 134:1 pour générer un événement lorsque des règles sont suspendues et la règle 134:2 pour générer un événement lorsque des règles suspendues sont activées. Consultez Options d'état de règle de prévention des intrusions.

Tableau 4 : Options de seuil de latence de la règle

Option	Description
Seuil	Spécifie la durée en microsecondes que les règles ne doivent pas dépasser lors de l'examen d'un paquet.
Quantité de violations consécutives du seuil avant la suspension de la règle	Spécifie le nombre de fois consécutives où les règles peuvent prendre plus de temps que le temps défini pour le **Threshold** (Seuil) pour inspecter les paquets avant que les règles ne soient suspendues.
Temps de la suspension	Spécifie la durée en secondes de suspension d'un groupe de règles.

Configuration du seuil de latence des règles

Par défaut, les paramètres de rendement basés sur la latence pour le traitement des paquets et des règles sont automatiquement remplis par la dernière mise à niveau des règles d'intrusion déployées, et il est conseillé de ne pas modifier la valeur par défaut.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** (✎) à côté de **Latency-Based Performance Settings** (Paramètres de performance basés sur la latence).

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Cliquez sur **Rule Management** (gestion des règles) dans la fenêtre contextuelle **Latency-Based Performance Settings** (paramètres de performance basés sur la latence).

Par défaut, l'option **Installed Rule Update** (mise à jour des règles installée) est sélectionnée. Il est conseillé d'utiliser cette valeur par défaut.

Les valeurs affichées ne reflètent pas les paramètres automatisés.

Étape 4 Si vous choisissez d'indiquer des valeurs personnalisées :

- Vous pouvez configurer n'importe quelle option dans Remarques sur le seuil de latence des règles, à la page 12.
- Vous devez préciser des valeurs personnalisées dans les onglets de gestion des paquets et des règles.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Si vous souhaitez générer des événements, activez les règles de latence 134:1 et 134:2. Pour en savoir plus, consultez Options d'état de règle de prévention des intrusions.
- Déployer les changements de configuration.

Configuration de la journalisation des statistiques de rendement en cas d'intrusion

Durée d'échantillonnage (secondes) et Nombre minimal de paquets

Lorsque le nombre de secondes spécifié s'écoule entre les mises à jour des statistiques de performance, le système vérifie qu'il a analysé le nombre de paquets spécifié. Si tel est le cas, le système met à jour les statistiques de performance. Sinon, le système attend d'analyser le nombre de paquets spécifié.

⚠

Mise en garde La configuration d'une valeur très faible (par exemple 1 seconde) pour la durée d'échantillonnage peut avoir un impact considérable sur le périphérique; les statistiques de performance enregistrées sur ce dernier peuvent entraîner des problèmes d'espace disque et affecter le fonctionnement du périphérique. Par conséquent, nous vous recommandons de ne pas configurer de valeur très faible.

Options de dépannage : journaliser la session/la distribution du protocole

Le service d'assistance peut vous demander lors d'un appel de dépannage de journaliser la distribution du protocole, la longueur des paquets et les statistiques de port.

⚠

Mise en garde N'activez pas la **journalisation de session/de la distribution du protocole,** sauf si le service d'assistance vous le demande.

Options de dépannage : récapitulatif

Lors d'un appel de dépannage, l'assistance peut vous demander de configurer le système pour qu'il calcule les statistiques de performance uniquement lorsque le processus Snort est arrêté ou redémarré. Pour activer cette option, vous devez également activer l'option de dépannage **session de journalisation/la distribution du protocole**.

⚠

Mise en garde N'activez pas le **récapitulatif**, sauf si le service d'assistance vous le demande.

Configuration de la journalisation des statistiques de rendement de la prévention des intrusions

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancé**, puis sur **Edit** (✎) à côté de **Performance Settings** (paramètres de rendement).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 2 Cliquez sur **PerformanceStatistics** dans la fenêtre contextuelle qui apparaît.

Étape 3 Modifiez la **durée d'échantillonnage** ou le **nombre minimal de paquets** comme décrit dans Configuration de la journalisation des statistiques de rendement en cas d'intrusion, à la page 14.

Mise en garde La configuration d'une valeur très faible (par exemple 1 seconde) pour la **durée d'échantillonnage** peut avoir une incidence considérable sur le périphérique; les statistiques de performance enregistrées sur le périphérique peuvent entraîner des problèmes d'espace disque et affecter le fonctionnement du périphérique. Par conséquent, nous vous recommandons de ne pas configurer de valeur très faible.

Étape 4 Vous pouvez également développer la section des **options de dépannage** et modifier ces options uniquement si le service d'assistance vous le demande.

Étape 5 Cliquez sur **OK**.

Prochaine étape

- Déployer les changements 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.