Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion

Les rubriques suivantes décrivent comment configurer les paramètres avancés pour les politiques d'analyse de réseau et de prévention des intrusions :

À propos des paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion

De nombreux paramètres avancés d'une politique de contrôle d'accès régissent les configurations de détection et de prévention des intrusions qui nécessitent une expertise particulière. Les paramètres avancés nécessitent généralement peu ou pas de modification et ne sont pas communs à tous les déploiements.

Exigences et conditions préalables pour les paramètres de contrôle d'accès avancé, pour l'analyse de réseau et les politiques de prévention d'intrusion

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Inspection des paquets qui passent avant que le trafic ne soit identifié

Pour certaines fonctions, notamment le filtrage d'URL, la détection d'applications, la limitation de débit et le contournement intelligent des applications, quelques paquets doivent passer pour que la connexion soit établie et pour permettre au système d'identifier le trafic et de déterminer quelle règle de contrôle d'accès (le cas échéant) gérera ce trafic.

Vous devez configurer explicitement votre politique de contrôle d'accès pour inspecter ces paquets, les empêcher d'atteindre leur destination et générer des événements. Consultez Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic, à la page 3.

Dès que le système identifie la règle de contrôle d'accès ou l'action par défaut qui doit gérer la connexion, les paquets restants de la connexion sont gérés et inspectés en conséquence.

Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic

- L'action par défaut spécifiée pour une politique de contrôle d'accès N'EST PAS appliquée à ces paquets.
- Utilisez plutôt les directives suivantes pour choisir une valeur pour la **politique de prévention des intrusions utilisée avant la détermination de la règle de contrôle d'accès** dans les paramètres avancés de la politique de contrôle d'accès.
  - Vous pouvez choisir une politique de prévention des intrusions créée par le système ou personnalisée. Par exemple, vous pouvez sélectionner **Sécurité et connectivité équilibrées**.
  - Pour des raisons de performance, sauf si vous avez une bonne raison de procéder autrement, ce paramètre doit correspondre aux actions par défaut définies pour votre politique de contrôle d'accès.
  - Si votre système n'effectue pas d'inspection des intrusions (par exemple, dans un déploiement de découverte uniquement), sélectionnez **No Rules Active** (Pas de règles actives). Le système n'inspectera pas ces paquets initiaux et ils seront autorisés à passer.
  - Par défaut, ce paramètre utilise l'ensemble de variables par défaut. Assurez-vous qu'il convient à vos besoins. Pour en savoir plus, consultez Ensemble de variables.
  - La politique d'analyse de réseau associée à la première règle d'analyse de réseau correspondante prétraite le trafic pour la politique que vous sélectionnez. S'il n'y a aucune règle d'analyse de réseau ou qu'aucune règle ne correspond, la politique d'analyse de réseau par défaut est utilisée.

Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic

Remarque Ce paramètre est parfois appelé *politique de prévention des intrusions par défaut*. (à ne pas confondre avec l'action par défaut pour une politique de contrôle d'accès.)

Avant de commencer

Passez en revue les bonnes pratiques pour ces paramètres. Consultez Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic, à la page 2.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé), puis sur **Edit** (✎) à côté de la section **Network Analysis** (Analyse du réseau) et **Intrusion Policies** (Politiques de prévention des intrusions).

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 Sélectionnez une politique de prévention des intrusions dans la liste déroulante **Politique de prévention des intrusions utilisée avant la détermination de la règle de contrôle d'accès**.

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

Étape 3 Vous pouvez également sélectionner un autre ensemble de variables dans la liste déroulante **Intrusion Policy Variable Set** (ensemble de variables de politique de prévention des intrusions). Vous pouvez également sélectionner **Edit** (✎) à côté de l'ensemble de variables pour créer et modifier des ensembles de variables. Si vous ne modifiez pas l'ensemble de variables, le système utilise un ensemble par défaut.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Ensemble de variables

Paramètres avancés pour les politiques d'analyse de réseau

Les politiques d'analyse de réseau régissent la façon dont le trafic est décodé et prétraité afin de pouvoir être évalué, en particulier pour le trafic anormal qui pourrait signaler une tentative de prévention des intrusions. Ce prétraitement de trafic a lieu après la mise en correspondance Security Intelligence et le déchiffrement du trafic, mais avant que les politiques de prévention des intrusions n'inspectent les paquets en détail. Par défaut, la politique d'analyse de réseau Sécurité et connectivité équilibrées fournie par le système est la politique d'analyse de réseau par défaut.

Astuces La politique d'analyse du réseau de sécurité et de connectivité équilibrée fournie par le système et la politique d'intrusion de sécurité et de connectivité équilibrée fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles d'intrusion. Cependant, la politique d'analyse de réseau régit principalement les options de prétraitement, alors que la politique de prévention de prévention des intrusions régit principalement les règles de prévention des intrusions.

Un moyen simple de régler le prétraitement consiste à créer et à utiliser une politique d'analyse de réseau personnalisée par défaut. Pour les utilisateurs avancés ayant des déploiements complexes, vous pouvez créer plusieurs politiques d'analyse du réseau, chacune étant conçue pour prétraiter le trafic différemment. Ensuite, vous pouvez configurer le système pour utiliser ces politiques et régir le prétraitement du trafic en utilisant différentes zones de sécurité, réseaux ou VLAN.

Pour ce faire, ajoutez des *règles d'analyse de réseau* personnalisées à votre politique de contrôle d'accès. Une règle d'analyse de réseau est simplement un ensemble de configurations et de conditions qui spécifient la manière dont vous traitez le trafic qui correspond à ces conditions. Vous pouvez créer et modifier les règles d'analyse de réseau dans les options avancées d'une politique de contrôle d'accès existante. Chaque règle n'appartient qu'à une seule politique.

Chaque règle comporte :

- un ensemble de conditions de règles qui identifient le trafic spécifique que vous souhaitez prétraiter
- une politique d'analyse de réseau associée que vous souhaitez utiliser pour prétraiter le trafic qui répond à toutes les conditions des règles

Lorsque vient le temps pour le système de prétraiter le trafic, il fait correspondre les paquets aux règles d'analyse de réseau en ordre descendant par numéro de règle. Le trafic qui ne correspond à aucune règle d'analyse de réseau est prétraité par la politique d'analyse de réseau par défaut.

Définition de la politique d'analyse du réseau par défaut

Vous pouvez choisir une politique créée par le système ou par l'utilisateur.

Remarque Si vous désactivez un préprocesseur, mais que le système doit évaluer les paquets prétraités par rapport à une règle de prévention des intrusions ou de préprocesseur activée, le système active et utilise automatiquement le préprocesseur, bien qu'il reste désactivé dans l'interface Web de la politique d'analyse de réseau. La personnalisation du prétraitement, en particulier de l'utilisation de plusieurs politiques d'analyse de réseau personnalisées, est une tâche **avancée**. Le prétraitement et l'inspection de prévention des intrusions étant si étroitement liés, vous **devez** faire attention et autoriser les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet à se compléter.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancé**, puis sur **Edit** (✎) à côté de la section Network Analysis and Intrusion Policies (Analyse de réseau et politiques d'intrusion).

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 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** (✎) pour modifier la politique dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Limites des politiques personnalisées

Règles d'analyse du réseau

Dans les paramètres avancés de votre politique de contrôle d'accès, vous pouvez utiliser des règles d'analyse de réseau pour adapter les configurations de prétraitement au trafic réseau.

Les règles d'analyse de réseau sont numérotées, en commençant par 1. Lorsque vient le temps pour le système de prétraiter le trafic, il fait correspondre les paquets aux règles d'analyse de réseau dans l'ordre ascendant par numéro de règle ascendant, et prétraite le trafic selon la première règle où toutes les conditions des règles correspondent.

Vous pouvez ajouter des conditions de zone, de réseau et de balise VLAN à une règle. Si vous ne configurez pas de condition particulière pour une règle, le système ne correspond pas au trafic en fonction de ce critère. Par exemple, une règle avec une condition de réseau, mais aucune condition de zone évalue le trafic en fonction

de son adresse IP de source ou de destination, quelle que soit son interface d'entrée ou de sortie. Le trafic qui ne correspond à aucune règle d'analyse de réseau est prétraité par la politique d'analyse de réseau par défaut.

Conditions des règles de politique d'analyse de réseau

Les conditions de règles vous permettent d'affiner votre politique d'analyse de réseau pour cibler les utilisateurs et les réseaux que vous souhaitez contrôler. Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Conditions des règles de zone de sécurité
Conditions des règles de réseau
Conditions de règle des balises VLAN

Conditions des règles de zone de sécurité

Les zones de sécurité segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques.

Les conditions de règles de zone contrôlent le trafic en fonction de ses zones de sécurité de source et de destination. Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle.

Tout comme toutes les interfaces d'une zone doivent être du même type (en ligne, passives, commutées ou routées), toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Astuces Restreindre les règles par zone est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle ne s'applique pas au trafic via l'une des interfaces de périphérique, cette règle n'affecte pas les performances de ce périphérique.

Conditions des zones de sécurité et de la multilocalisation de détention

Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :
  - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
  - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Configuration des règles d'analyse du réseau

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancé**, puis sur **Edit** (✎) à côté de la section Network Analysis and Intrusion Policies (Analyse de réseau et politiques d'intrusion).

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.

Astuces Cliquez sur **Network Analysis Policy List** (Liste des politiques d'analyse de réseau) pour afficher et modifier les politiques d'analyse de réseau personnalisées existantes.

Étape 2 À côté de **Network Analysis Rules** (règles d'analyse de réseau), cliquez sur l'énoncé qui indique combien de règles personnalisées vous avez.

Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

Étape 4 Configurez les conditions de la règle en cliquant sur les conditions que vous souhaitez ajouter; voir Configuration des règles d'analyse du réseau, à la page 8.

Étape 5 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 **Edit** (✎) pour modifier une politique personnalisée dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.

Étape 6 Cliquez sur **Add** (Ajouter).

Prochaine étape

- Déployer les changements de configuration.

Gestion des règles d'analyse du réseau

Une règle d'analyse de réseau est simplement un ensemble de configurations et de conditions qui spécifient la manière dont vous traitez le trafic qui correspond à ces conditions. Vous pouvez créer et modifier les règles d'analyse de réseau dans les options avancées d'une politique de contrôle d'accès existante. Chaque règle n'appartient qu'à une seule politique.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé), puis sur **Edit** (✎) à côté de la section Politiques de prévention des intrusions et d'analyse de réseau.

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 À côté de **Network Analysis Rules** (règles d'analyse de réseau), cliquez sur l'énoncé qui indique combien de règles personnalisées vous avez.

Étape 3 Modifier vos règles personnalisées Vous avez les options suivantes :

- Pour modifier les conditions d'une règle ou la politique d'analyse de réseau appelée par la règle, cliquez sur **Edit** ( ) à côté de la règle.
- Pour modifier l'ordre d'évaluation d'une règle, cliquez sur la règle et faites-la glisser jusqu'à l'emplacement approprié. Pour sélectionner plusieurs règles, utilisez la touche Maj + Ctrl.
- Pour supprimer une règle, cliquez sur **Supprimer** ( ) à côté de la règle.

Astuces Cliquez avec le bouton droit sur une règle pour afficher un menu contextuel qui vous permet de couper, de copier, de coller, de modifier, de supprimer et d'ajouter de nouvelles règles d'analyse de réseau.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

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.