Aperçu du contrôle d'accès

Introduction au contrôle d'accès

Le contrôle d'accès est une fonctionnalité basée sur des politiques hiérarchiques qui vous permet de spécifier, d'inspecter et de consigner le trafic réseau (non accéléré).

Chaque périphérique géré peut être ciblé par une seule politique de contrôle d'accès. Les données que les *périphériques cibles* de la politique recueillent à propos de votre trafic réseau peuvent être utilisées pour filtrer et contrôler ce trafic en fonction des éléments suivants :

- caractéristiques de transport et de réseau simples et faciles à déterminer : source et destination, port, protocole, etc.
- derniers renseignements contextuels sur le trafic, y compris des caractéristiques telles que la réputation, le risque, la pertinence commerciale, l'application utilisée ou l'URL visitée
- domaine, utilisateur, groupe d'utilisateurs ou attribut ISE
- balise de groupe de sécurité (SGT) personnalisée
- caractéristiques du trafic chiffré; vous pouvez également déchiffrer ce trafic pour conduire une analyse plus approfondie
- si le trafic non chiffré ou déchiffré contient un fichier interdit, un logiciel malveillant détecté ou une tentative de prévention des intrusions
- heure et jour (sur les périphériques pris en charge)

Chaque type d'inspection et de contrôle du trafic est effectué là où cela est le plus logique, pour une flexibilité et une performance maximales. Par exemple, le blocage basé sur la réputation utilise des données de source et de destination simples. Il peut donc bloquer le trafic interdit dès le début du processus. En revanche, la détection et le blocage des intrusions et des exploits sont une défense de dernière ligne.

Introduction aux règles

Les règles de différents types de politiques (contrôle d'accès, SSL, identité, etc.) assurent un contrôle fin sur le trafic réseau. Le système évalue le trafic en fonction des règles dans l'ordre que vous spécifiez, à l'aide d'un algorithme de première correspondance.

Bien que ces règles puissent inclure d'autres configurations qui ne sont pas cohérentes entre les politiques, elles partagent de nombreuses caractéristiques de base et mécanismes de configuration, notamment :

- Conditions : les conditions de règle précisent le trafic géré par chaque règle. Vous pouvez configurer chaque règle avec plusieurs conditions. Le trafic doit correspondre à toutes les conditions pour respecter la règle.
- L'action découlant d'une règle détermine comment le système traite le trafic correspondant. Notez que même si une règle n'est associée à aucune liste d'**actions** dans laquelle vous pouvez choisir, une action est tout de même associée à la règle. Par exemple, une règle d'analyse de réseau personnalisée utilise une politique d'analyse de réseau comme « action ». Par ailleurs, les règles de QoS n'ont pas d'action explicite, car toutes les règles de QoS font la même chose : le trafic de limite de débit.
- Position : la position d'une règle détermine son ordre d'évaluation. Lorsqu'il utilise une politique pour évaluer le trafic, le système fait correspondre le trafic aux règles dans l'ordre que vous spécifiez. Généralement, le système gère le trafic en fonction de la première règle, lorsque toutes les conditions de la règle correspondent au trafic. (Les règles Monitor, qui sont conçues pour le suivi et la journalisation, sont une exception.) Un bon ordre des règles réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles.
- Catégorie : pour organiser certains types de règles, vous pouvez créer des catégories de règles personnalisées dans chaque politique parente.
- Journalisation : pour de nombreuses règles, les paramètres de journalisation régissent si et comment le système consigne les connexions gérées par la règle. Certaines règles (telles que les règles d'analyse d'identité et de réseau) n'incluent pas les paramètres de journalisation, car les règles ne déterminent pas la disposition finale des connexions et ne sont pas spécifiquement conçues pour journaliser les connexions. Par ailleurs, les règles de QoS n'incluent pas les paramètres de journalisation; vous ne pouvez pas enregistrer une connexion simplement parce qu'elle était à débit limité.
- Commentaires : pour certains types de règles, vous pouvez ajouter des commentaires chaque fois que vous enregistrez des modifications. Par exemple, vous pouvez résumer la configuration globale à l'intention des autres utilisateurs, ou indiquer quand vous modifiez une règle et la raison de cette modification.

Astuces Un menu contextuel dans de nombreux Éditeurs de politiques fournit des raccourcis vers de nombreuses options de gestion des règles, y compris la modification, la suppression, le déplacement, l'activation et la désactivation.

Pour en savoir plus, consultez le chapitre qui traite des règles qui vous intéressent (par exemple, les règles de contrôle d'accès).

Sujets connexes

Configuration des conditions d'application et des filtres

Bonnes pratiques de contrôle des applications, à la page 12

Règles de filtrage par périphérique

Certains éditeurs de politiques vous permettent de filtrer l'affichage des règles par périphériques concernés.

Le système utilise les contraintes d'interface d'une règle pour déterminer si la règle affecte un périphérique. Si vous limitez une règle par interface (zone de sécurité ou condition de groupe d'interfaces), le périphérique où se trouve cette interface est affecté par cette règle. Les règles sans contraintes d'interface s'appliquent à n'importe quelle interface et, par conséquent, à chaque périphérique.

Les règles de QoS sont toujours limitées par interface.

Procédure

Étape 1 Dans l'éditeur de politiques, cliquez sur **Rules** (règles), puis sur **Filter by Device** (filtre par périphérique). La liste des périphériques et des groupes de périphériques ciblés s'affiche.

Étape 2 Cochez une ou plusieurs cases pour afficher uniquement les règles qui s'appliquent à ces périphériques ou groupes. Sinon, cochez la case **All** (toutes) pour réinitialiser et afficher toutes les règles.

Astuces Passez votre curseur sur un critère de règle pour voir sa valeur. Si le critère représente un objet avec des remplacements spécifiques au périphérique, le système affiche la valeur de remplacement lorsque vous filtrez la liste de règles uniquement en fonction de ce périphérique. Si le critère représente un objet avec des remplacements spécifiques au domaine, le système affiche la valeur de remplacement lorsque vous filtrez la liste de règles par périphérique dans ce domaine.

Étape 3 Cliquez sur **OK**.

Avertissements relatifs aux règles et autres politiques

Les éditeurs de politiques et de règles utilisent des icônes pour marquer les configurations qui pourraient avoir une incidence négative sur l'analyse et le flux du trafic. Selon le problème, le système peut vous avertir lorsque vous déployez ou vous empêcher de déployer complètement.

Astuces Passez votre pointeur sur une icône pour lire le texte d'avertissement, d'erreur ou d'information.

Tableau 1 : Icônes d'erreur de politique

Icône	Description	Exemple
Erreurs (✖)	Si une règle ou une configuration comporte une erreur, vous ne pouvez pas procéder au déploiement avant d'avoir corrigé le problème, même si vous désactivez les règles touchées.	Une règle qui effectue un filtrage d'URL basé sur la catégorie et la réputation est valide jusqu'à ce que vous cibliez un périphérique qui ne dispose pas de licence de filtrage d'URL. À ce stade, une icône d'erreur s'affiche à côté de la règle et vous ne pouvez pas la déployer avant d'avoir modifié ou supprimé la règle, reciblé la politique ou activé la licence.

Icône	Description	Exemple
Avertissement ()	Vous pouvez déployer une politique qui affiche des règles ou d'autres avertissements. Cependant, les erreurs de configuration signalées par des avertissements n'ont aucun effet. Si vous désactivez une règle avec un avertissement, l'icône d'avertissement disparaît. Elle réapparaît si vous activez la règle sans corriger le problème sous-jacent.	Les règles préemptées ou les règles qui ne peuvent pas correspondre au trafic en raison d'une mauvaise configuration n'ont aucun effet. Cela inclut les conditions utilisant des groupes d'objets vides, les filtres d'application qui ne correspondent à aucune application, les utilisateurs LDAP exclus, les ports non valides, etc. Cependant, si une icône d'avertissement signale une erreur de licence ou une incompatibilité de modèle, vous ne pouvez pas déployer avant d'avoir corrigé le problème.
Information ()	Les icônes d'information transmettent des informations utiles sur les configurations qui peuvent influer sur le flux de trafic. Ces problèmes ne vous empêchent pas de déployer.	Le système peut ignorer la mise en correspondance des premiers paquets d'une connexion avec certaines règles, jusqu'à ce que le système identifie l'application ou le trafic Web dans cette connexion. Cela permet d'établir des connexions pour identifier les applications et les requêtes HTTP.
Conflit de règles ()	Lorsque vous activez l'analyse de conflit de règles, cette icône s'affiche dans le tableau de règles pour les règles en conflit.	Les conflits comprennent les règles redondantes, les objets redondants et les règles observées. Les règles redondantes et observées ne correspondent pas au trafic, car les règles précédentes correspondraient déjà aux critères. Les objets redondants rendent vos règles inutilement complexes.

Action par défaut de la politique de contrôle d'accès

Une politique de contrôle d'accès nouvellement créée ordonne à ses périphériques cibles de gérer tout le trafic à l'aide de son *action par défaut*.

Dans une politique de contrôle d'accès simple, l'action par défaut spécifie comment les périphériques cibles gèrent l'ensemble du trafic. Dans une politique plus complexe, l'action par défaut gère le trafic qui :

- n'a pas la confiance de la fonction de contournement intelligent de l'application
- n'est pas sur une liste de blocage de Security Intelligence
- n'est pas bloqué par l'inspection SSL (trafic chiffré uniquement)
- ne correspond à aucune des règles de la politique (à l'exception des règles Monitor, qui correspondent et consignent le trafic, mais ne gèrent ni ne inspectent)

L'action par défaut de la politique de contrôle d'accès peut bloquer ou faire confiance au trafic sans autre inspection, ou inspecter le trafic pour détecter les intrusions et les données de découverte.

Remarque Vous **ne pouvez pas** inspecter les fichiers ou les programmes malveillants sur le trafic géré par l'action par défaut. La journalisation des connexions gérées par l'action par défaut est initialement désactivée, bien que vous puissiez l'activer.

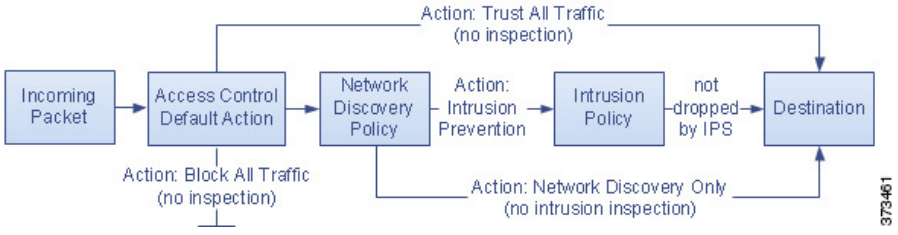
Si vous utilisez l'hérédité des politiques, l'action par défaut pour le descendant du niveau le plus bas détermine le traitement final du trafic. Bien qu'une politique de contrôle d'accès puisse hériter de l'action par défaut de sa politique de base, vous ne pouvez pas appliquer cet apprentissage.

Le tableau suivant décrit les types d'inspections que vous pouvez effectuer sur le trafic géré par chaque action par défaut.

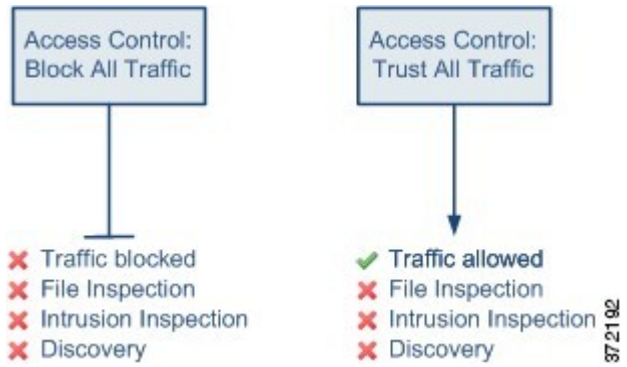
Tableau 2 : Actions par défaut de la politique de contrôle d'accès

Action par défaut	Effet sur le trafic	Type d'inspection et politique
Contrôle d'accès : bloquer tout le trafic	bloquer sans autre inspection	none
Contrôle d'accès : faire confiance à tout le trafic	faire confiance (autoriser l'acheminement vers sa destination finale sans autre inspection)	none
Prévention contre les intrusions	autoriser, à condition qu'il soit transmis par la politique de prévention des intrusions que vous spécifiez	intrusion, à l'aide de la politique de prévention des intrusions et de l'ensemble de variables associé; découverte, utilisation de la politique de découverte de réseau
Découverte du réseau seulement	autoriser	découverte uniquement, à l'aide de la politique de découverte de réseau
Hériter de la stratégie de base	défini dans la politique de base	défini dans la politique de base

Le diagramme suivant illustre le tableau.



Les diagrammes suivants illustrent les actions par défaut de l'option **Bloquer tout le trafic** et **Faire confiance à tout le trafic**.



Les diagrammes suivants illustrent les actions par défaut de la **prévention des intrusions** et **de la découverte de réseau uniquement**.

Astuces L'objectif de **la découverte du réseau uniquement** est d'améliorer les performances dans un déploiement de découverte seule. Différentes configurations peuvent désactiver la découverte si seule la détection et la prévention des intrusions vous intéressent.

Inspection approfondie à l'aide des politiques de fichier et de prévention des intrusions

L'inspection approfondie utilise des politiques de prévention des intrusions et de fichiers comme dernière ligne de défense avant que le trafic ne soit autorisé à atteindre sa destination.

- *Les politiques de prévention des intrusions* régissent les capacités de prévention des intrusions du système.

  Pour obtenir des renseignements complets, consultez Prévention et détection des intrusions.

- *Les politiques de fichiers* régissent le contrôle de fichiers et les capacités de Défense contre les programmes malveillants .

  Pour obtenir des renseignements complets, consultez Protection contre les programmes malveillants de réseau et politiques relatives aux fichiers.

Le contrôle d'accès est effectué avant l'inspection approfondie; les règles de contrôle d'accès et l'action de contrôle d'accès par défaut déterminent quel trafic est inspecté par les politiques de prévention des intrusions et de fichier.

En associant une politique de prévention des intrusions à une règle de contrôle d'accès, vous informez le système qu'avant que ne soit transmis le trafic correspondant aux conditions de la règle de contrôle d'accès, vous souhaitez inspecter le trafic au moyen d'une politique de prévention des intrusions.

Dans une politique de contrôle d'accès, vous pouvez associer une politique de prévention des intrusions à chaque règle d'autorisation et de blocage interactif, ainsi qu'à l'action par défaut. Chaque **paire** de politique de prévention des intrusions et d'ensemble de variables compte pour une politique.

Pour associer les politiques de prévention des intrusions et de fichiers à une règle de contrôle d'accès, consultez :

- Configuration des règles de contrôle d'accès pour effectuer la prévention des intrusions
- Configuration d'une règle de contrôle d'accès pour la protection contre les programmes malveillants

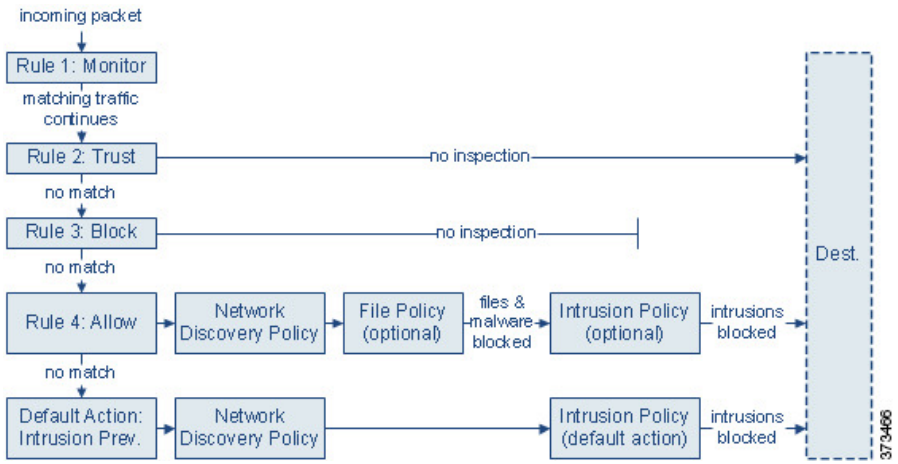
Remarque Par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès qui a configuré l'inspection des intrusions et des fichiers.

Sujets connexes

Comment les politiques examinent le trafic à la recherche d'intrusions
Politique de fichiers

Gestion du trafic de contrôle d'accès avec politiques de prévention des intrusions et de fichiers

Le diagramme suivant montre le flux de trafic dans un périphérique de prévention des intrusions en ligne et de déploiement Défense contre les programmes malveillants , tel que régi par une politique de contrôle d'accès qui contient quatre types différents de règles de contrôle d'accès et une action par défaut.



Dans le scénario ci-dessus, les trois premières règles de contrôle d'accès de la politique (Surveillance, Confiance et Blocage) ne peuvent pas inspecter le trafic correspondant. Les règles de Monitorage suivent et consignent le trafic réseau, mais n'inspectent pas, de sorte que le système continue de faire correspondre le trafic avec des règles supplémentaires pour déterminer s'il faut l'autoriser ou le refuser. (Cependant, consultez une exception et une mise en garde importantes en Action du moniteur des règles de contrôle d'accès.) Les règles de confiance et de blocage gèrent le trafic correspondant sans autre inspection d'aucune sorte, tandis que le trafic qui ne correspond pas passe à la règle de contrôle d'accès suivante.

La quatrième et dernière règle de la politique, une règle Allow (autorisation), fait appel à diverses autres politiques pour inspecter et gérer le trafic correspondant, dans l'ordre suivant :

- **Découverte : Politique de découverte de réseau** : tout d'abord, la politique de découverte de réseau inspecte le trafic à la recherche de données de découverte. La découverte est une analyse passive et n'affecte pas le flux de trafic. Bien que vous n'activiez pas explicitement la découverte, vous pouvez l'améliorer ou la désactiver. Cependant, autoriser le trafic ne garantit pas automatiquement la collecte de données de découverte. Le système effectue la découverte uniquement pour les connexions impliquant des adresses IP explicitement surveillées par votre politique de découverte de réseau.
- **Défense contre les programmes malveillants et Contrôle des fichiers : politique** en matière de fichiers : une fois le trafic inspecté par la découverte, le système peut l'inspecter à la recherche de fichiers interdits et de programmes malveillants. Défense contre les programmes malveillants détecte et bloque les programmes malveillants dans de nombreux types de fichiers, y compris les fichiers PDF, les documents Microsoft Office et autres. Si votre entreprise souhaite bloquer non seulement la transmission de fichiers de programmes malveillants, mais aussi tous les fichiers d'un type précis (qu'ils contiennent ou non des fichiers malveillants), *le contrôle des fichiers* vous permet de surveiller le trafic réseau pour détecter les transmissions de types de fichiers précis, puis bloque ou autorisez le fichier.
- **Prévention des intrusions : politique de prévention des intrusions** – Après l'inspection des fichiers, le système peut inspecter le trafic pour détecter les intrusions et les exploits. Une politique de prévention des intrusions examine les paquets décodés à la recherche d'attaques basées sur des modèles, et peut bloquer ou modifier le trafic malveillant. Les politiques de prévention des intrusions sont associées à *des ensembles de variables*, ce qui vous permet d'utiliser des valeurs nommées pour refléter avec précision votre environnement réseau.
- **Destination** : le trafic qui passe toutes les vérifications décrites ci-dessus vers sa destination.

Une règle Interactive Block (blocage interactif) (non illustrée dans le diagramme) possède les mêmes options d'inspection qu'une règle Allow (autorisation). Cela vous permet d'inspecter le trafic à la recherche de contenu malveillant lorsqu'un utilisateur contourne un site Web bloqué en cliquant dans une page d'avertissement.

Le trafic qui ne correspond à aucune règle de contrôle d'accès de la politique avec une action autre que Surveiller est géré par l'action par défaut. Dans ce scénario, l'action par défaut est une action de prévention des intrusions, qui autorise le trafic vers sa destination finale, à condition qu'elle soit transmise par la politique de prévention des intrusions que vous spécifiez. Dans un autre déploiement, vous pourriez avoir une action par défaut qui approuve ou bloque tout le trafic sans autre inspection. Notez que le système peut inspecter le trafic autorisé par l'action par défaut pour détecter les données de découverte et les intrusions, mais pas les fichiers ni les programmes malveillants interdits. Vous **ne pouvez pas** associer de politique de fichier à l'action par défaut de contrôle d'accès.

Remarque Parfois, lorsqu'une connexion est analysée par une politique de contrôle d'accès, le système doit traiter les premiers paquets de cette connexion, **en leur permettant de passer**, avant de pouvoir décider quelle règle de contrôle d'accès (le cas échéant) gérera le trafic. Cependant, pour que ces paquets n'atteignent pas leur destination sans être inspectés, vous pouvez définir une politique de prévention des intrusions (dans les paramètres avancés de la politique de contrôle d'accès) pour inspecter ces paquets et générer des incidents d'intrusion.

Ordre d'inspection de fichier et d'intrusion

Dans votre politique de contrôle d'accès, vous pouvez associer plusieurs règles Allow (autorisation) et Interactive Block (blocage interactif) à différentes politiques de prévention des intrusions et de fichiers pour faire correspondre les profils d'inspection à divers types de trafic.

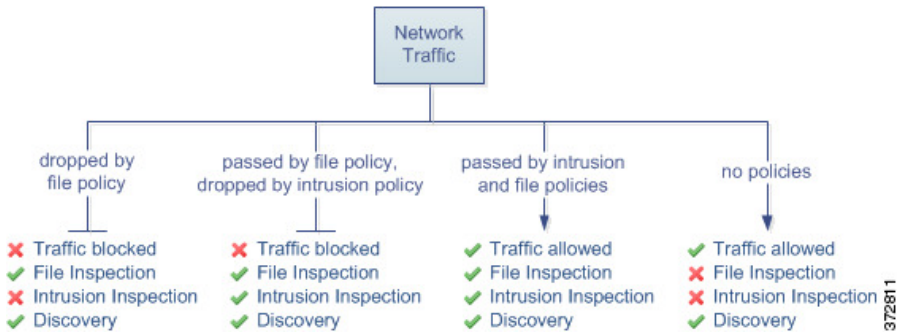
Remarque Le trafic autorisé par une action par défaut de la prévention des intrusions ou de la découverte de réseau seulement peut être inspecté pour détecter des données de découverte et des intrusions, mais pas pour les fichiers interdits ou les programmes malveillants. Vous **ne pouvez pas** associer de politique de fichier à l'action par défaut de contrôle d'accès.

Vous n'êtes pas tenu d'effectuer à la fois l'inspection des fichiers et l'inspection des intrusions dans la même règle. Pour une connexion correspondant à une règle Allow (autorisation) ou Interactive Block (blocage interactif) :

- sans politique de fichiers, le flux de trafic est déterminé par la politique de prévention des intrusions
- sans politique de prévention des intrusions, le flux de trafic est déterminé par la politique de fichiers
- sans l'un ou l'autre, le trafic autorisé est inspecté uniquement par la découverte de réseau

Astuces Le système n'effectue aucune sorte d'inspection sur le trafic de confiance. Bien que la configuration d'une règle d'autorisation sans politique de prévention des intrusions ni de fichier ne transmette le trafic comme une règle de confiance, les règles d'autorisation vous permettent d'effectuer la découverte sur le trafic correspondant.

Le diagramme ci-dessous illustre les types d'inspection que vous pouvez effectuer sur le trafic qui répond aux conditions d'une règle de contrôle d'accès Allow (autorisation) ou Interactive Block (blocage interactif) contourné par l'utilisateur. Par souci de simplicité, le diagramme affiche le flux de trafic pour les situations où à la fois (ou aucune) une politique de prévention des intrusions et une politique de fichiers ne sont associées à une seule règle de contrôle d'accès.



Pour toute connexion unique gérée par une règle de contrôle d'accès, l'inspection des fichiers a lieu avant l'inspection de prévention des intrusions. C'est-à-dire que le système n'inspecte pas les fichiers bloqués par une politique de fichiers pour détecter les intrusions. Dans l'inspection des fichiers, le blocage simple par type prévaut sur l'inspection et le blocage des programmes malveillants.

Par exemple, envisageons un scénario dans lequel vous souhaitez normalement autoriser une partie du trafic réseau comme défini dans une règle de contrôle d'accès. Cependant, par mesure de précaution, vous souhaitez bloquer le téléchargement de fichiers exécutables, examiner les fichiers PDF téléchargés pour détecter les programmes malveillants, bloquer toutes les instances que vous trouvez et effectuer une inspection de prévention des intrusions sur le trafic.

Vous créez une politique de contrôle d'accès avec une règle qui correspond aux caractéristiques du trafic que vous souhaitez autoriser provisoirement, et vous l'associez à la fois à une politique de prévention des intrusions et à une politique de fichiers. La politique de fichiers bloque le téléchargement de tous les exécutables, et inspecte et bloque les fichiers PDF contenant des programmes malveillants :

- Tout d'abord, le système bloque le téléchargement de tous les fichiers exécutables, en fonction d'une simple correspondance de type spécifiée dans la politique de fichiers. Puisqu'ils sont immédiatement bloqués, ces fichiers ne sont soumis à l'inspection des programmes malveillants ni des intrusions.
- Ensuite, le système recherche dans le nuage les fichiers PDF téléchargés sur un hôte de votre réseau. Tous les fichiers PDF contenant des programmes malveillants sont bloqués et ne sont pas soumis à l'inspection de prévention des intrusions.
- Enfin, le système utilise la politique de prévention des intrusions associée à la règle de contrôle d'accès pour inspecter le trafic restant, y compris les fichiers non bloqués par la politique de fichiers.

Remarque Jusqu'à ce qu'un fichier soit détecté et bloqué dans une session, les paquets de la session peuvent être soumis à une inspection de prévention des intrusions.

Héritage de la politique de contrôle d'accès

Particulièrement utiles dans les déploiements multidomaine, vous pouvez imbriquer des politiques de contrôle d'accès, où chaque politique hérite des règles et des paramètres d'une politique ancêtre (ou *de base*). Vous pouvez appliquer cet apprentissage ou permettre aux politiques de niveau inférieur de remplacer leurs ascendants.

Le contrôle d'accès utilise une implémentation hiérarchique basée sur des politiques. Tout comme vous créez une hiérarchie de domaines, vous pouvez créer une hiérarchie correspondante de politiques de contrôle d'accès.

Une politique de contrôle d'accès *descendante*, ou *enfant*, hérite des règles et des paramètres de son *parent* direct, ou politique de base. Cette politique de base peut avoir sa propre politique parente dont elle hérite des règles et des paramètres, etc.

Les règles d'une politique de contrôle d'accès sont imbriquées entre les sections de règles Obligatoire et par défaut de sa politique parente. Cette implémentation permet d'appliquer les règles obligatoires des politiques ascendantes, mais permet à la politique actuelle d'écrire des règles qui prévalent sur les règles par défaut des politiques ascendantes.

Vous pouvez verrouiller les paramètres suivants pour les appliquer dans toutes les politiques descendantes. Les politiques descendantes peuvent remplacer les paramètres déverrouillés.

- Informations sur la sécurité : connexions autorisées ou bloquées en fonction des dernières informations sur la réputation pour les adresses IP, les URL et les noms de domaine.
- Pages de réponse HTTP : affichage d'une page de réponse personnalisée ou fournie par le système lorsque vous bloquez la demande de site Web d'un utilisateur.
- Advanced settings (paramètres avancés) : pour spécifier les sous-politiques associées, les paramètres d'analyse de réseau, les paramètres de performance et d'autres options générales.

Lorsque vous utilisez l'hérédité des politiques, l'action par défaut pour le descendant du niveau le plus bas détermine le traitement final du trafic. Bien qu'une politique de contrôle d'accès puisse hériter de son action par défaut d'une politique ancêtre, vous ne pouvez pas appliquer cet apprentissage.

Héritage des politiques et architecture multi-détenteur.

La mise en œuvre du contrôle d'accès basée sur des politiques hiérarchiques complète l'architecture multi-détenteur.

Dans un déploiement multidomaine typique, la hiérarchie de la politique de contrôle d'accès correspond à la structure du domaine et vous appliquez la politique de contrôle d'accès du niveau le plus bas aux périphériques gérés. Cette implémentation permet une application sélective du contrôle d'accès à un niveau supérieur de domaine, tandis que les administrateurs de domaine de niveau inférieur peuvent adapter les paramètres spécifiques au déploiement. (Vous devez utiliser des rôles, pas seulement l'hérédité et l'application des politiques, pour restreindre le nombre d'administrateurs dans les domaines descendants.)

Par exemple, en tant qu'administrateur de domaine global pour votre organisation, vous pouvez créer une politique de contrôle d'accès au niveau global. Vous pouvez ensuite exiger que tous vos périphériques, qui sont divisés en sous-domaines par fonction, utilisent cette politique de niveau global comme politique de base.

Lorsque les administrateurs de sous-domaine se connectent à Cisco Secure Firewall Management Center pour configurer le contrôle d'accès, ils peuvent déployer la politique de niveau global telle quelle. Ils peuvent aussi créer et déployer une politique de contrôle d'accès descendante dans les limites de la politique de niveau global.

Remarque Bien que la mise en œuvre la plus utile de l'hérédité et de l'application du contrôle d'accès complète l'hébergement multi-détenteur, vous pouvez créer une hiérarchie de politiques de contrôle d'accès au sein d'un seul domaine. Vous pouvez également affecter et déployer des politiques de contrôle d'accès à tous les niveaux.

Bonnes pratiques de contrôle des applications

Les rubriques suivantes traitent des bonnes pratiques que nous recommandons pour contrôler les applications à l'aide de règles de contrôle d'accès.

Recommandations pour le contrôle des applications

Gardez à l'esprit les directives et les limites suivantes concernant le contrôle des applications :

Vérification de l'activation du profilage adaptatif

Si le profilage adaptatif n'est pas activé (son état par défaut), les règles de contrôle d'accès ne peuvent pas effectuer de contrôle d'application.

Détecteurs d'application à activation automatique

Si aucun détecteur n'est activé pour une application que vous souhaitez détecter, le système active automatiquement tous les détecteurs fournis par le système pour l'application. S'il n'y en a pas, le système activera le détecteur défini par l'utilisateur le plus récemment modifié pour l'application.

Configurez votre politique pour examiner les paquets qui doivent passer avant qu'une application ne soit identifiée

Le système ne peut pas effectuer le contrôle des applications, y compris le contournement intelligent des applications (IAB) et la limitation du débit, avant *que les deux* cas de figure suivants ne se produisent :

- Une connexion surveillée est établie entre un client et le serveur
- Le système identifie l'application dans la session

Cette identification devrait se produire dans 3 à 5 paquets, ou après l'échange du certificat du serveur dans l'établissement de liaison SSL si le trafic est chiffré.

Important! Pour vous assurer que votre système examine ces paquets initiaux, consultez Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic.

Si le trafic précoce correspond à tous les autres critères mais que l'identification de l'application est incomplète, le système permet au paquet de passer et la connexion est établie (ou l'établissement de liaison SSL se termine). Une fois que le système a terminé son identification, le système applique l'action appropriée au trafic de session restant.

Remarque Un serveur doit respecter les exigences du protocole d'une application pour que le système puisse la reconnaître. Par exemple, si vous avez un serveur qui envoie un paquet keep-alive plutôt qu'un accusé de réception alors qu'un accusé de réception est attendu, cette application pourrait ne pas être identifiée et la connexion ne correspondra pas à la règle basée sur l'application. Au lieu de cela, elle sera gérée par une autre règle de correspondance ou par l'action par défaut. Cela peut signifier que les connexions que vous souhaitez autoriser peuvent être refusées à la place. Si vous rencontrez ce problème et que vous ne pouvez pas réparer le serveur pour qu'il suive les normes de protocole, vous devez écrire une règle non basée sur l'application pour couvrir le trafic pour ce serveur, par exemple en faisant correspondre l'adresse IP et le numéro de port.

Créer des règles distinctes pour le filtrage d'URL et d'application

Créez chaque fois que possible des règles distinctes pour le filtrage d'URL et d'application, car la combinaison des critères d'application et d'URL peut entraîner des résultats inattendus, en particulier pour le trafic chiffré.

Les règles qui incluent les critères d'application et d'URL doivent être placées après les règles d'application uniquement ou d'URL uniquement, sauf si la règle application + URL fait exception à une règle plus générale d'application uniquement ou d'URL uniquement.

Règles d'URL avant les règles application et autres

Pour optimiser la mise en correspondance d'URL, placez des règles qui incluent les conditions d'URL avant les autres règles, en particulier si les règles d'URL sont des règles de blocage et que les autres règles répondent aux deux critères suivants :

- Ils comprennent des conditions d'application.
- Le trafic à inspecter est chiffré.

Application Control pour le trafic chiffré et déchiffré

Le système peut identifier et filtrer le trafic chiffré et déchiffré :

- Trafic chiffré : Le système peut détecter le trafic d'applications chiffré avec StartTLS, y compris SMTPS, POPS, FTPS, TelnetS et IMAPS. En outre, il peut identifier certaines applications chiffrées en fonction de l'indication du nom du serveur dans le message TLS ClientHello ou de la valeur du nom distinctif du sujet provenant du certificat du serveur. Ces applications sont balisées « `protocole SSL` »; dans une règle SSL, vous pouvez choisir uniquement ces applications. Les applications sans cette balise ne peuvent être détectées que dans le trafic non chiffré ou déchiffré.
- Trafic déchiffré : le système attribue la balise de `trafic déchiffré` aux applications qu'il peut détecter dans le trafic déchiffré uniquement, non chiffré ou non chiffré.

Découverte de l'identité du serveur TLS et contrôle des applications

La dernière version du protocole TLS (Transport Layer Security) 1.3, définie par la RFC 8446, est le protocole privilégié de nombreux serveurs Web pour fournir des communications sécurisées. Étant donné que le protocole TLS 1.3 chiffre le certificat du serveur pour plus de sécurité, et que le certificat est nécessaire pour correspondre aux critères de filtrage d'application et d'URL dans les règles de contrôle d'accès, le système Firepower permet d'extraire le certificat du serveur *sans* déchiffrer le paquet en entier.

Nous vous recommandons fortement de l'activer pour tout trafic que vous souhaitez mettre en correspondance avec des critères d'application ou d'URL, en particulier si vous souhaitez effectuer une inspection approfondie de ce trafic. Un politique de déchiffrement n'est pas requis, car *le trafic n'est pas déchiffré* lors du processus d'extraction du certificat de serveur.

Pour en savoir plus, consultez Paramètres avancés de politique de contrôle d'accès.

Exempting Applications from Active Authorization

Dans une politique d'identité, vous pouvez exempter certaines applications de l'authentification active, permettant au trafic de continuer à accéder au contrôle. Ces applications sont marquées `Exclusion d'agent d'utilisateur`. Dans une règle d'identité, vous ne pouvez choisir que ces applications.

Gestion des paquets de trafic d'application sans charges utiles

Lors du contrôle d'accès, le système applique la politique par défaut aux paquets qui n'ont pas de charge utile dans une connexion où une application est identifiée.

Gestion du trafic des applications référencées

Pour gérer le trafic référencé par un serveur Web, tel que le trafic publicitaire, faites correspondre l'application référencée plutôt que l'application de référence.

Contrôle du trafic des applications qui utilise plusieurs protocoles (Skype, Zoho)

Certaines applications utilisent plusieurs protocoles. Pour contrôler leur trafic, assurez-vous que votre politique de contrôle d'accès couvre toutes les options pertinentes. Par exemple :

- Skype : Pour contrôler le trafic Skype, choisissez la balise **Skype** dans la liste des **filtres d'application** plutôt que de sélectionner des applications individuelles. Cela garantit que le système peut détecter et contrôler tout le trafic de Skype de la même manière.
- Zoho : pour contrôler Zoho mail, sélectionnez *Zoho* et **Zohomail** dans la liste des applications disponibles.

Moteurs de recherche pris en charge pour les fonctionnalités de restriction de contenu

Le système prend en charge le filtrage de recherche sécurisée uniquement pour des moteurs de recherche précis. Le système attribue la `balise prise en charge par Safesearch` au trafic d'application provenant de ces moteurs de recherche.

Contrôle du trafic des applications d'évitement

Consultez Remarques et limites propres aux applications, à la page 17.

Bonnes pratiques pour la configuration du contrôle des applications

Nous vous recommandons de contrôler l'accès des applications au réseau comme suit :

- Pour autoriser ou bloquer l'accès d'une application d'un réseau moins sécurisé à un réseau plus sécurisé : Utiliser les conditions de **port** (port de destination sélectionné) sur la règle de contrôle d'accès.

  Par exemple, autorisez le trafic ICMP d'Internet (moins sécurisé) vers un réseau interne (plus sécurisé).

- Pour autoriser ou bloquer l'accès aux applications par des groupes d'utilisateurs : utilisez les conditions d'**application** dans la règle de contrôle d'accès.

  Par exemple, empêcher les membres du groupe Sous-traitants d'accéder à Facebook

Mise en garde Ne pas configurer correctement vos règles de contrôle d'accès peut avoir des résultats inattendus, notamment autoriser le trafic qui devrait être bloqué. En général, les règles de contrôle d'application doivent être situées plus bas dans votre liste de contrôle d'accès, car la mise en correspondance de ces règles prend plus de temps que les règles basées sur l'adresse IP, par exemple.

Les règles de contrôle d'accès qui utilisent des conditions *spécifiques* (comme les réseaux et les adresses IP) doivent être classées *avant* les règles qui utilisent des conditions générales (comme les applications). Si vous connaissez bien le modèle Open Systems Interconnect (OSI), utilisez une numérotation similaire dans le concept. Les règles avec des conditions pour les couches 1, 2 et 3 (physique, liaison de données et réseau) doivent être classées en premier dans vos règles de contrôle d'accès. Les conditions pour les couches 5, 6 et 7 (session, présentation et application) doivent être classées plus loin dans vos règles de contrôle d'accès. Pour en savoir plus sur le modèle OSI, consultez cet article de Wikipedia.

Le tableau suivant fournit un exemple de configuration de vos règles de contrôle d'accès :

Type de contrôle	Action	Zones, réseaux, balises VLAN	Utilisateurs	Applications	Ports	Adresses URL	Attributs SGT/ISE	Inspection, journalisation, commentaires
Application d'un réseau du plus sécurisé vers un autre du réseau moins sécurisé lorsque l'application utilise un port (par exemple, SSH)	Votre choix (**Autoriser** dans cet exemple)	Zones ou réseaux de destination utilisant l'interface externe	N'importe lequel	Ne pas définir	Ports disponibles : **SSH** Ajouter aux **Ports de destination sélectionnés**	N'importe lequel	À utiliser uniquement avec ISE/ISE-PIC.	N'importe lequel
Application d'un réseau du plus sécurisé au moins sécurisé lorsque l'application n'utilise pas de port (par exemple, ICMP)	Votre choix (**Autoriser** dans cet exemple)	Zones ou réseaux de destination utilisant l'interface externe	N'importe lequel	Ne pas définir	**Protocole** de ports de destination sélectionnés : **ICMP** **Type** : **Tout**	Ne pas définir	À utiliser uniquement avec ISE/ISE-PIC.	N'importe lequel

Type de contrôle	Action	Zones, réseaux, balises VLAN	Utilisateurs	Applications	Ports	Adresses URL	Attributs SGT/ISE	Inspection, journalisation, commentaires
Accès à l'application par un groupe d'utilisateurs	Votre choix (**Block** (Bloquer) dans cet exemple))	Votre choix	Choisissez un groupe d'utilisateurs (groupe des sous-traitants dans cet exemple)	Choisissez le nom de l'application (**Facebook** dans cet exemple)	Ne pas définir	Ne pas définir	À utiliser uniquement avec ISE/ISE-PIC.	Votre choix

Caractéristiques des applications

Le système caractérise chaque application qu'il détecte à l'aide des critères décrits dans le tableau suivant. Utilisez ces caractéristiques comme filtres d'application.

Tableau 3 : Caractéristiques des applications

Caractéristiques	Description	Exemple
Type	Les protocoles d'application représentent les communications entre les hôtes. Les clients représentent des logiciels exécutés sur un hôte. Les applications Web représentent le contenu ou l'URL demandée pour le trafic HTTP.	HTTP et SSH sont des protocoles d'application. Les navigateurs Web et les clients de courriel sont des clients. MPEG video et Facebook sont des applications Web.
Risque	La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation.	Les applications homologue à homologue ont tendance à présenter un risque très élevé.
Pertinence commerciale	La probabilité que l'application soit utilisée dans le cadre des activités commerciales de votre organisation, plutôt qu'à des fins récréatives.	Les applications de jeu ont généralement une très faible pertinence commerciale.
Type	Une classification générale de l'application qui décrit sa fonction la plus essentielle. Chaque application appartient à au moins une catégorie.	Facebook fait partie de la catégorie des réseaux sociaux.
Balise	Des informations supplémentaires sur l'application. Les applications peuvent avoir un nombre illimité de balises, y compris aucune.	Les applications Web de vidéo en flux continu sont souvent marquées pour `une bande passante élevée` et `affichent des publicités`.

Remarques et limites propres aux applications

- Portail d'administration Office 365 :

  Limitation : si la politique d'accès a activé la journalisation au début et à la fin, le premier paquet sera détecté comme Office 365 et la fin de la connexion sera détectée comme portail d'administration Office 365. Cela ne devrait pas affecter le blocage.

- Skype

  Voir la section Recommandations pour le contrôle des applications, à la page 12.

- GoToMeeting

  Afin de détecter entièrement GoToMeeting, votre règle doit inclure toutes les applications suivantes :

  - GoToMeeting
  - Citrix Online
  - Plateforme Citrix GoToMeeting
  - LogMeIn
  - STUN

- Zoho :

  Voir la section Recommandations pour le contrôle des applications, à la page 12.

- Applications de contournement telles que Bittorrent, Tor, Psiphon et Ultrasurf :

  Pour les applications furtives, seuls les scénarios au niveau de confiance le plus élevé sont détectés par défaut. Si vous devez prendre des mesures concernant ce trafic (par exemple, bloquer ou mettre en œuvre la QoS), il peut être nécessaire de configurer une détection plus agressive et plus efficace. Pour ce faire, communiquez avec Cisco TAC pour passer en revue vos configurations, car ces modifications peuvent entraîner des faux positifs.

- WeChat :

  Il n'est pas possible de bloquer sélectivement les médias WeChat si vous autorisez WeChat.

- Protocole de bureau à distance RDP (Remote Desktop Protocol)

  Si l'autorisation de l'application RDP n'autorise pas les transferts de fichiers, vérifiez que la règle pour RDP inclut les ports 3389 TCP et UDP. Le transfert de fichiers RDP utilise UDP.

Bonnes pratiques pour les règles de contrôle d'accès

Il est essentiel de créer et de classer correctement les règles dans le bon ordre pour créer un déploiement efficace. Les rubriques suivantes résument les directives de performance des règles.

Remarque Lorsque vous déployez des modifications de configuration, le système évalue toutes les règles ensemble et crée un ensemble élargi de critères que les appareils cibles utilisent pour évaluer le trafic réseau. Si ces critères dépassent les ressources (mémoire physique, processeurs, etc.) d'un périphérique cible, vous ne pouvez pas le déployer sur ce périphérique.

Bonnes pratiques en matière de contrôle d'accès

Passez en revue les exigences et les bonnes pratiques générales suivantes :

- Utilisez une politique de préfiltre pour fournir un blocage précoce du trafic indésirable et pour accélérer le trafic qui ne bénéficie pas de l'inspection de contrôle d'accès. Pour en savoir plus, consultez Bonnes pratiques de préfiltrage Fastpath.
- Bien que vous puissiez configurer le système sans octroyer de licence pour votre déploiement, de nombreuses fonctionnalités nécessitent l'activation des licences appropriées avant le déploiement.
- Lorsque vous déployez une politique de contrôle d'accès, ses règles ne sont pas appliquées aux connexions existantes. Le trafic sur une connexion existante n'est pas lié par la nouvelle politique qui est déployée. En outre, le nombre de résultats de politique est incrémenté uniquement pour le premier paquet d'une connexion qui correspond à une politique. Ainsi, le trafic sur une connexion existante qui pourrait correspondre à une politique est omis du nombre de résultats. Pour que les règles de politique soient appliquées efficacement, effacez les sessions de connexions existantes, puis déployez la politique.
- Chaque fois que cela est possible, combinez plusieurs objets réseau en un seul groupe d'objets. Le système crée automatiquement un groupe d'objets (lors du déploiement) lorsque vous sélectionnez plusieurs objets (pour la source ou la destination séparément). La sélection de groupes existants peut éviter la duplication de groupes d'objets et réduire l'impact potentiel sur l'utilisation de la CPU lorsque le nombre d'objets en double est élevé.
- Pour que le système puisse affecter le trafic, vous devez déployer les configurations pertinentes sur les périphériques gérés à l'aide d'interfaces routées, commutées ou transparentes, ou de paires d'interfaces en ligne.

  Parfois, le système vous empêche de déployer des configurations en ligne sur les périphériques déployés de manière passive, y compris les périphériques en ligne en mode TAP.

  Dans d'autres cas, la politique peut être déployée avec succès, mais tenter de bloquer ou de modifier le trafic à l'aide de périphériques déployés de manière passive peut avoir des résultats inattendus. Par exemple, le système peut signaler plusieurs événements de début de connexion pour chaque connexion bloquée, car les connexions bloquées ne sont pas bloquées dans les déploiements passifs.
- Certaines fonctionnalités, notamment le filtrage d'URL, la détection d'applications, la limitation de débit et le contournement intelligent des applications, doivent autoriser le passage de certains paquets pour que le système puisse identifier le trafic.

  Pour éviter que ces paquets atteignent leur destination sans être inspectés, consultez Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic et Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic.
- Vous ne pouvez pas effectuer d'inspection de fichier ou de programme malveillant sur le trafic géré par l'action par défaut de la politique de contrôle d'accès.

- En outre, certaines fonctionnalités ne sont disponibles que sur certains modèles de périphériques. Les icônes d'avertissement et les boîtes de dialogue de confirmation désignent des fonctionnalités non prises en charge.
- Si vous utilisez syslog ou stockez des événements en externe, évitez les caractères spéciaux dans les noms d'objets tels que les noms de politiques et de règles. Les noms d'objet ne doivent pas contenir de caractères spéciaux, tels que des virgules, que l'application destinataire peut utiliser comme séparateurs.
- La journalisation des connexions gérées par l'action par défaut est initialement désactivée, bien que vous puissiez l'activer.
- Les bonnes bonnes pratiques en matière de création, de commande et de mise en œuvre de règles de contrôle d'accès sont décrites dans Bonnes pratiques pour les règles de contrôle d'accès, à la page 17 et les rubriques secondaires.

Bonnes pratiques pour les règles de tri

Directives générales

- En général, placez les règles de priorité supérieure qui doivent s'appliquer à tout le trafic près du sommet de la politique.
- Les règles spécifiques doivent précéder les règles générales, en particulier lorsqu'elles sont des exceptions aux règles générales.

  Sinon, le trafic correspondra d'abord à la règle générale et n'atteindra jamais la règle spécifique applicable.
- Les règles qui abandonnent le trafic en fonction uniquement de critères des couches 3/4 (comme l'adresse IP, la zone de sécurité et le numéro de port) doivent être appliquées dès que possible. Les règles basées sur ces critères ne nécessitent pas d'inspection pour identifier les connexions correspondantes.
- Chaque fois que cela est possible, mettez des règles de suppression spécifiques près du sommet de la politique. Cela garantit la prise de décision le plus tôt possible concernant le trafic indésirable.
- Les règles de filtrage d'URL, basées sur l'application et la géolocalisation, et autres règles qui nécessitent une inspection, devraient suivre les règles qui abandonnent le trafic en fonction de critères des couches 3/4 uniquement (comme l'adresse IP, la zone de sécurité et le numéro de port), mais avant les règles. qui précisent les politiques en matière de fichiers et de prévention des intrusions.
- Placez les règles de filtrage d'URL au-dessus des règles d'application, et faîtes-les suivre des règles d'application des règles de micro-application et des règles de filtrage d'application de sous-classification du protocole industriel commun (CIP).
- Les règles qui précisent les politiques de fichiers et les politiques de prévention des intrusions doivent figurer en bas de l'ordre des règles. Ces règles nécessitent une inspection approfondie exigeante en ressources. Pour des raisons de performance, vous devez d'abord éliminer le plus grand nombre de menaces possible à l'aide de méthodes moins intensives, afin de minimiser le nombre de menaces potentielles nécessitant une inspection approfondie.
- Classez toujours les règles pour répondre aux besoins de votre organisation.

Les exceptions et les ajouts aux directives ci-dessus sont indiqués dans les sections ci-dessous.

Préemption des règles

Il y a préemption de règle lorsqu'une règle ne correspondra jamais au trafic parce qu'une règle antérieure dans l'ordre d'évaluation correspond au trafic en premier. Les conditions d'une règle déterminent si elle préempte les autres règles. Dans l'exemple suivant, la deuxième règle ne peut pas bloquer le trafic de l'administrateur, car la première règle le permet :

Règle de contrôle d'accès 1 : autoriser les utilisateurs administrateurs
Règle de contrôle d'accès 2 : bloquer les utilisateurs administrateurs

Tout type de condition de règle peut préempter une règle ultérieure. La plage VLAN dans la première règle SSL inclut le VLAN dans la deuxième règle, de sorte que la première règle préempte la seconde :

Règle SSL 1 : ne pas déchiffrer le VLAN 22-33
Règle SSL 2 : bloquer le VLAN 27

Dans l'exemple suivant, la règle 1 correspond à n'importe quel VLAN, car aucun VLAN n'est configuré, donc la règle 1 préempte la règle 2, qui tente de correspondre au VLAN 2 :

Règle de contrôle d'accès 1 : autoriser le réseau source 10.4.0.0/16
Règle de contrôle d'accès 2 : autoriser le réseau source 10.4.0.0/16, VLAN 2

Une règle préempte également une règle ultérieure identique où toutes les conditions configurées sont les mêmes :

Règle 1 de QoS : limite de débit VLAN 1, URL www.netffix.com
Règle 2 de QoS : limite de débit VLAN 1, URL www.netffix.com

Une règle ultérieure ne serait pas préemptée si une condition est différente :

Règle 1 de QoS : limite de débit VLAN 1, URL www.netffix.com
Règle de QoS 2 : limite de débit du VLAN 2, URL www.netffix.com

Exemple : commande de règles SSL pour éviter la préemption

Voici un scénario dans lequel une autorité de certification de confiance (autorité de certification valide) a émis par erreur un certificat d'autorité de certification à une entité malveillante (autorité de certification incorrecte), mais n'a pas encore retiré ce certificat. Vous souhaitez utiliser une politique SSL pour bloquer le trafic chiffré avec des certificats émis par l'autorité de certification non fiable, mais autorisez le trafic dans la chaîne de confiance de l'autorité de certification de confiance. Après avoir téléchargé les certificats d'autorité de certification et tous les certificats d'autorité de certification intermédiaires, configurez une politique SSL avec des règles dans l'ordre suivant :

Règle SSL n° 1 : émetteur de blocage CN=www.badca.com
Règle SSL n° 2 : ne pas déchiffrer l'émetteur CN=www. goodca.com

Si vous inversez les règles, vous commencez par faire correspondre tout le trafic approuvé par l'autorité de certification correcte, y compris le trafic approuvé par l'autorité de certification défaillante. Comme aucun trafic ne correspond jamais à la règle d'autorité de certification défaillante suivante, le trafic malveillant peut être autorisé au lieu d'être bloqué.

Actions des règles et ordre des règles

L'action découlant d'une règle détermine comment le système traite le trafic correspondant. Améliorez le rendement en plaçant les règles qui n'exécutent pas de tâches ou qui ne garantissent pas un traitement plus

poussé du trafic avant les règles qui nécessitent beaucoup de ressources. Le système peut alors détourner le trafic qu'il aurait pu inspecter autrement.

Les exemples suivants montrent comment vous pouvez ordonner les règles dans différentes politiques, compte tenu d'un ensemble de règles où aucune n'est plus critique et où la préemption n'est pas un problème.

Si vos règles comprennent des conditions d'application, consultez également Bonnes pratiques pour la configuration du contrôle des applications, à la page 14.

Ordre optimal : règles de déchiffrement

Non seulement le déchiffrement nécessite des ressources, mais il faut aussi une analyse plus approfondie du trafic déchiffré. Placez les règles qui déchiffrent le trafic en dernier.

Remarque Certains périphériques gérés prennent en charge le chiffrement et le déchiffrement du trafic TLS/SSL au niveau matériel, ce qui améliore considérablement les performances. Pour obtenir plus de renseignements, consultez Accélération du chiffrement TLS.

1. Surveillance : règles qui consignent les connexions correspondantes, mais ne prennent aucune autre mesure sur le trafic.
2. Blocage, Blocage avec réinitialisation : règles qui bloquent le trafic sans autre inspection.
3. Ne pas déchiffrer : règles qui ne déchiffrent pas le trafic chiffré, en transmettant la session chiffrée aux règles de contrôle d'accès. Les charges utiles de ces sessions ne sont pas soumises à une inspection approfondie.
4. Déchiffrer - Clé connue : règles qui déchiffrent le trafic entrant avec une clé privée connue.
5. Déchiffrer - resigner : règles qui déchiffrent le trafic sortant en signant de nouveau le certificat du serveur.

Ordre optimal : règles de contrôle d'accès

L'inspection des intrusions, des fichiers et des programmes malveillants nécessite des ressources, en particulier si vous utilisez plusieurs politiques de prévention des intrusions et ensembles de variables personnalisés. Placez les règles de contrôle d'accès qui appellent l'inspection approfondie en dernier.

1. Surveillance : règles qui consignent les connexions correspondantes, mais ne prennent aucune autre mesure sur le trafic. (Cependant, consultez l'exception importante et la mise en garde en Action du moniteur des règles de contrôle d'accès.)
2. Confiance, Blocage, Blocage avec réinitialisation : règles qui gèrent le trafic sans autre inspection. Notez que le trafic de confiance est soumis à des exigences d'authentification imposées par une politique d'identité et à une limitation de débit.
3. Autoriser, Blocage interactif (sans inspection approfondie) : règles qui n'inspectent pas le trafic de manière plus approfondie, mais qui permettent la découverte. Veuillez noter que le trafic autorisé est soumis aux exigences d'authentification imposées par une politique d'identité et à la limitation de débit.
4. Autoriser, blocage interactif (inspection approfondie) : règles associées aux fichiers ou aux politiques de prévention des intrusions qui effectuent une inspection approfondie à la recherche de fichiers interdits, de programmes malveillants et d'exploits.

Ordre des règles relatives aux applications

Les règles avec des conditions d'application sont plus susceptibles de correspondre au trafic si vous les déplacez vers un ordre inférieur dans votre liste de règles.

Les règles de contrôle d'accès qui utilisent des conditions *spécifiques* (comme les réseaux et les adresses IP) doivent être classées *avant* les règles qui utilisent des conditions générales (comme les applications). Si vous connaissez bien le modèle Open Systems Interconnect (OSI), utilisez une numérotation similaire dans le concept. Les règles avec des conditions pour les couches 1, 2 et 3 (physique, liaison de données et réseau) doivent être classées en premier dans vos règles de contrôle d'accès. Les conditions pour les couches 5, 6 et 7 (session, présentation et application) doivent être classées plus loin dans vos règles de contrôle d'accès. Pour en savoir plus sur le modèle OSI, consultez cet article de Wikipedia.

Pour plus d'informations et un exemple, consultez Bonnes pratiques pour la configuration du contrôle des applications, à la page 14 et Recommandations pour le contrôle des applications, à la page 12.

Ordre des règles d'URL

Pour optimiser la mise en correspondance d'URL, placez des règles qui incluent les conditions d'URL avant les autres règles, en particulier si les règles d'URL sont des règles de blocage et que les autres règles répondent aux deux critères suivants :

- Ils comprennent des conditions d'application.
- Le trafic à inspecter est chiffré.

Si vous configurez des exceptions à une règle, placez l'exception avant l'autre règle.

Bonnes pratiques pour simplifier et cibler les règles

Simplifier : ne pas surconfigurer

Minimiser les critères de règles individuelles. Utiliser le moins possible d'éléments individuels dans les conditions de règles. Par exemple, dans des conditions de réseau, utilisez des blocs d'adresses IP plutôt que des adresses IP individuelles.

Si une condition est suffisante pour correspondre au trafic que vous souhaitez gérer, n'en utilisez pas deux. L'utilisation de conditions redondantes peut étendre considérablement la configuration déployée, ce qui peut entraîner des problèmes de performances du périphérique et un comportement inattendu du périphérique dans une grappe et une unité à haute disponibilité se rejoignent. Par exemple :

- Utilisez avec prudence les zones de sécurité qui représentent plusieurs interfaces. Si vous spécifiez les réseaux de source et de destination comme conditions, et que ceux-ci sont suffisants pour correspondre au trafic que vous ciblez, il n'est pas nécessaire de préciser une zone de sécurité.
- Si vous souhaitez faire correspondre un ensemble d'interfaces internes à TOUTE destination sur Internet (par exemple), utilisez simplement une zone de sécurité source qui inclut vos interfaces internes. Aucun critère d'interface de réseau ou de destination n'est nécessaire.

La combinaison d'éléments dans des objets n'améliore **pas** les performances. Par exemple, l'utilisation d'un objet réseau qui contient 50 adresses IP individuelles vous offre uniquement un avantage sur le plan de l'organisation, et non de la performance, par rapport à l'inclusion de ces adresses IP dans la condition individuellement.

Pour obtenir des recommandations relatives à la détection d'applications, consultez Bonnes pratiques pour la configuration du contrôle des applications, à la page 14.

Objectif : restreindre fortement les règles exigeantes en ressources, en particulier par interface

Dans la mesure du possible, utilisez des conditions de règle pour définir étroitement le trafic géré par les règles exigeantes en ressources. Les règles ciblées sont également importantes, car les règles associées à des conditions larges peuvent correspondre à de nombreux types de trafic et peuvent préempter des règles plus spécifiques ultérieurement. Voici des exemples de règles exigeantes en ressources :

- Règles TLS/SSL qui déchiffrent le trafic : Non seulement le déchiffrement, mais une analyse plus approfondie du trafic déchiffré, nécessite des ressources. Limiter le trafic et, si possible, bloquer ou choisir de ne pas déchiffrer le trafic chiffré.

  Certains modèles Défense contre les menaces effectuent le chiffrement et le déchiffrement TLS/SSL de façon matérielle, ce qui améliore considérablement les performances. Pour obtenir plus de renseignements, consultez Accélération du chiffrement TLS.

- Les règles de contrôle d'accès qui font appel à une inspection approfondie : l'inspection des intrusions, des fichiers et des programmes malveillants nécessite des ressources, en particulier si vous utilisez plusieurs politiques de prévention des intrusions et ensembles de variables personnalisés. Assurez-vous de n'appeler l'inspection approfondie que si nécessaire.

Pour des performances optimales, limitez les règles par interface. Si une règle exclut toutes les interfaces d'un périphérique, cette règle n'affecte pas les performances de ce périphérique.

Nombre maximal de règles de contrôle d'accès et de politiques de prévention des intrusions

Le nombre maximal de règles de contrôle d'accès ou de politiques de prévention des intrusions prises en charge par un périphérique cible dépend de nombreux facteurs, notamment la complexité de la politique, la mémoire physique et le nombre de processeurs du périphérique.

Si vous dépassez le maximum pris en charge par votre appareil, vous ne pouvez pas déployer votre politique de contrôle d'accès et devez la réévaluer.

Directives pour les politiques de prévention des intrusions :

- Dans une politique de contrôle d'accès, vous pouvez associer une politique de prévention des intrusions à chaque règle d'autorisation et de blocage interactif, ainsi qu'à l'action par défaut. Chaque **paire** de politique de prévention des intrusions et d'ensemble de variables compte pour une politique.

- Vous souhaiterez peut-être consolider les politiques de prévention des intrusions ou des ensembles de variables afin de pouvoir associer une seule paire de variables de politiques de prévention des intrusions à plusieurs règles de contrôle d'accès. Sur certains périphériques, vous constaterez peut-être que vous ne pouvez utiliser qu'un seul ensemble de variables pour toutes vos politiques de prévention des intrusions, ou même une seule paire politique de prévention des intrusions-variable pour l'ensemble du périphérique .

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.