Règles de contrôle d'accès

Les rubriques suivantes décrivent comment configurer les règles de contrôle d'accès :

Introduction aux règles de contrôle d'accès

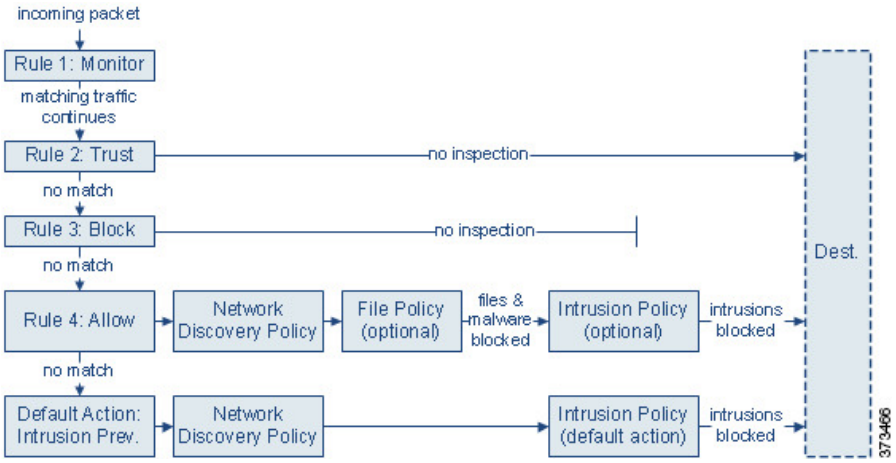
Dans une politique de contrôle d'accès, les *règles de contrôle d'accès* fournissent une méthode précise de gestion du trafic réseau sur plusieurs périphériques gérés.

Remarque Security Intelligence filtering (filtrage des renseignements de sécurité), le déchiffrement, l'identification de l'utilisateur et certains décodages et prétraitements ont lieu avant que les règles de contrôle d'accès évaluent le trafic réseau.

Le système fait correspondre le trafic aux règles de contrôle d'accès dans l'ordre que vous spécifiez. Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle de contrôle d'accès, lorsque *toutes* les conditions de la règle correspondent au trafic.

Chaque règle possède également une *action*, qui détermine si vous surveillez, faites confiance, bloquez ou autorisez le trafic correspondant. Lorsque vous autorisez le trafic, vous pouvez demander au système de l'inspecter d'abord à l'aide de politiques de prévention des intrusions ou de fichiers pour bloquer les exploitations, les programmes malveillants ou les fichiers interdits avant qu'ils n'atteignent vos ressources ou ne quittent votre réseau.

Le scénario suivant résume les façons dont le trafic peut être évalué par les règles de contrôle d'accès dans un déploiement de prévention des intrusions en ligne.



Dans ce scénario, le trafic est évalué comme suit :

- **Règle 1 : Monitor (surveiller)** évalue le trafic en premier Les règles de surveillance permettent de suivre et de journaliser le trafic réseau. Le système continue de faire correspondre le trafic à des règles supplémentaires pour déterminer s'il doit 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, à la page 6.)
- **Règle 2 : Trust (confiance)** évalue ensuite le trafic. Le trafic correspondant est autorisé à passer à sa destination sans autre inspection, bien qu'il soit toujours soumis aux exigences d'identité et à la limitation de débit. Le trafic qui ne correspond pas passe à la règle suivante.
- **Règle 3 : Block (bloquer)** évalue le trafic en troisième lieu. Le trafic correspondant est bloqué sans autre inspection. Le trafic qui ne correspond pas se poursuit jusqu'à la règle finale.
- **Règle 4 : Allow (Autoriser)** est la règle finale. Pour cette règle, le trafic correspondant est autorisé; cependant, les fichiers interdits, les programmes malveillants, les intrusions et les exploits au sein de ce trafic sont détectés et bloqués. Le reste du trafic non interdit et non malveillant est autorisé vers sa destination, bien qu'il soit toujours soumis à des exigences d'identité et à une limitation de débit. Vous pouvez configurer des règles Allow (autorisation) qui effectuent uniquement l'inspection de fichiers ou l'inspection de prévention des intrusions, ou encore aucune des deux.
- **L'action par défaut** gère tout le trafic qui ne correspond à aucune des règles. Dans ce scénario, l'action par défaut effectue la prévention des intrusions avant de permettre le passage du trafic non malveillant. Dans un autre déploiement, vous pourriez avoir une action par défaut qui approuve ou bloque tout le trafic, sans autre inspection. (Vous ne pouvez pas inspecter les fichiers ou les programmes malveillants sur le trafic géré par l'action par défaut.)

Le trafic que vous autorisez, que ce soit avec une règle de contrôle d'accès ou l'action par défaut, est automatiquement autorisé à être inspecté par la politique de découverte du réseau pour les données relatives à l'hôte, à l'application et à l'utilisateur. Vous n'activez pas explicitement la découverte, bien que vous puissiez 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. en outre, la découverte d'applications est limitée aux sessions chiffrées.

Notez que les règles de contrôle d'accès gèrent le trafic chiffré lorsque votre configuration de déchiffrement le permet, ou si vous ne configurez pas le déchiffrement. Cependant, certaines conditions de règles de contrôle d'accès nécessitent un trafic non chiffré, de sorte que le trafic chiffré peut correspondre à moins de règles. En outre, 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.

Gestion des règles de contrôle d'accès

Le tableau des règles de l'éditeur de politique de contrôle d'accès vous permet d'ajouter, de modifier, de catégoriser, de rechercher, de filtrer, de déplacer, d'activer, de désactiver, de supprimer et de gérer les règles de contrôle d'accès dans la politique actuelle.

Créer et ordonner correctement des règles est une tâche complexe, mais essentielle à la mise en place d'un déploiement efficace. Si vous ne planifiez pas votre politique avec soin, les règles peuvent prévaloir sur d'autres règles, nécessiter des licences supplémentaires ou contenir des configurations non valides. Pour que le système gère le trafic comme prévu, l'interface de contrôle d'accès est dotée d'un système d'avertissement et d'erreur robuste pour les règles.

Utilisez la barre de recherche pour filtrer la liste des règles de politique de contrôle d'accès. Vous pouvez désélectionner l'option **Afficher uniquement les règles de correspondance** pour afficher toutes les règles. Les règles correspondantes sont mises en surbrillance.

Pour chaque règle de contrôle d'accès, l'éditeur de politique affiche son nom, un résumé de ses conditions, l'action de la règle et des icônes qui communiquent les options ou l'état d'inspection de la règle. Ces icônes représentent :

- **Time Range Option** ( )
- **Politique d'intrusion** ( )
- **Politique sur les fichiers** ( )
- **Se connecter** ( )
- **Avertissement** ( )
- **Erreurs** ( )
- **Conflit de règles** ( )

Les règles désactivées sont grisées et marquées (désactivées) après le nom de la règle.

Pour créer ou modifier une règle, utilisez l'éditeur de règles de contrôle d'accès.

: vous pouvez :

- Configurer le nom de la règle et sélectionner son emplacement dans la partie supérieure de l'éditeur.
- Passer à la modification d'une autre règle en sélectionnant sa ligne au-dessus ou en dessous de l'éditeur.
- Utiliser la liste de gauche pour sélectionner l'action découlant de la règle et appliquer les politiques de prévention des intrusions et les ensembles de variables, les politiques de fichiers et la plage temporelle, ainsi que pour définir les options de journalisation.
- Utiliser les options à côté du nom de la règle pour sélectionner l'action liée à la règle, et appliquer les politiques de prévention des intrusions et les ensembles de variables, les politiques de fichiers et la plage temporelle, ainsi que pour définir les options de journalisation.

- Utiliser les colonnes **Sources** et **Destinations et applications** pour ajouter les critères correspondants. Vous pouvez ajouter des options à partir de la liste Tous ou passer aux différents onglets pour trouver plus facilement le type d'options que vous souhaitez, comme la zone ou les réseaux de sécurité.
- Ajouter des commentaires à la règle en bas de l'éditeur.

Sujets connexes

Composants des règles de contrôle d'accès, à la page 4
Bonnes pratiques pour les règles de contrôle d'accès

Composants des règles de contrôle d'accès

Outre son nom unique, chaque règle de contrôle d'accès comporte les composants de base suivants :

État

Par défaut, les règles sont activées. Si vous désactivez une règle, le système ne l'utilise pas et arrête de générer des avertissements et des erreurs pour cette règle.

Position

Les règles d'une politique de contrôle d'accès sont numérotées en commençant à 1. Si vous utilisez l'hérédité de politiques, la règle 1 est la première règle de la politique la plus externe. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. À l'exception des règles de surveillance, la première règle à laquelle le trafic correspond est celle qui gère ce trafic.

Les règles peuvent également appartenir à une section et à une catégorie, qui sont organisationnelles uniquement et n'affectent pas la position de la règle. La position de la règle traverse les sections et les catégories.

Section et catégorie

Pour vous aider à organiser les règles de contrôle d'accès, chaque politique de contrôle d'accès comporte deux sections de règles fournies par le système : Obligatoire et Par défaut. Pour mieux organiser les règles de contrôle d'accès, vous pouvez créer des catégories de règles personnalisées dans les sections Obligatoire et Par défaut.

Si vous utilisez l'hérédité de politiques, les règles de la politique actuelle sont imbriquées entre les sections Obligatoire et Default de sa politique parente.

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Les conditions peuvent être simples ou complexes; leur utilisation dépend souvent de la licence.

Le trafic doit satisfaire à toutes les conditions spécifiées dans une règle. Par exemple, si la condition d'application spécifie HTTP, mais pas HTTPS, la catégorie d'URL et les conditions de réputation ne s'appliqueront pas au trafic HTTPS.

Heure applicable

Vous pouvez préciser les jours et les heures auxquels une règle s'applique.

Action

L'action découlant d'une règle détermine comment le système traite le trafic correspondant. Vous pouvez surveiller, faire confiance, bloquer ou autoriser (avec ou sans inspection supplémentaire) le trafic correspondant. Le système n'effectue pas d'inspection approfondie du trafic de confiance, bloqué ou chiffré.

Inspection

Les options d'inspection approfondie régissent la façon dont le système inspecte et bloque le trafic malveillant que vous auriez autrement autorisé. Lorsque vous autorisez le trafic avec une règle, vous pouvez demander au système de l'inspecter d'abord à l'aide de politiques de prévention des intrusions ou de fichiers pour bloquer les exploitations, les programmes malveillants ou les fichiers interdits avant qu'ils n'atteignent vos ressources ou ne quittent votre réseau.

Logging (journalisation)

Les paramètres de journalisation d'une règle régissent les enregistrements que le système conserve du trafic qu'il gère. Vous pouvez conserver un enregistrement du trafic qui correspond à une règle. En général, vous pouvez enregistrer les sessions au début ou à la fin d'une connexion, ou les deux. Vous pouvez consigner les connexions à la base de données, au journal système (syslog) ou à un serveur de déroutement SNMP.

Commentaires

Chaque fois que vous enregistrez des modifications à une règle de contrôle d'accès, vous pouvez ajouter des commentaires.

Sujets connexes

Bonnes pratiques pour les règles de contrôle d'accès
Gestion des règles de contrôle d'accès, à la page 3
Créer et modifier les règles de contrôle d'accès, à la page 12
Actions de règles de contrôle d'accès, à la page 6
Conditions des règles de contrôle d'accès, à la page 13
Inspection approfondie à l'aide des politiques de fichier et de prévention des intrusions
Commentaires des règles de contrôle d'accès

Ordre des règles de contrôle d'accès

Les règles d'une politique de contrôle d'accès sont numérotées en commençant à 1. Le système fait correspondre le trafic aux règles par ordre décroissant par numéro de règle croissant.

Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle de contrôle d'accès, lorsque *toutes* les conditions de la règle correspondent au trafic. À l'exception des règles Monitor (surveillance), le système interrompt l'évaluation du trafic par rapport à des règles supplémentaires de priorité inférieure une fois que le trafic correspond à une règle.

Pour vous aider à organiser les règles de contrôle d'accès, chaque politique de contrôle d'accès comporte deux sections de règles fournies par le système : Obligatoire et Par défaut. Pour mieux vous organiser, vous pouvez créer des catégories de règles personnalisées dans les sections Obligatoire ou Par défaut. Une fois que vous avez créé une catégorie, vous ne pouvez plus la déplacer, mais vous pouvez la supprimer, la renommer et déplacer des règles à l'intérieur, à l'extérieur, au sein et autour d'elle. Le système attribue des numéros de règle aux sections et aux catégories.

Si vous utilisez l'héritage des politiques, les règles de la politique actuelle sont imbriquées entre les sections de règles obligatoires et par défaut de la politique parente. La règle 1 est la première règle de la politique la plus externe, et non la politique actuelle, et le système attribue des numéros de règle aux politiques, aux sections et aux catégories.

Tout rôle d'utilisateur prédéfini qui vous permet de modifier les politiques de contrôle d'accès vous permet également de déplacer et de modifier les règles de contrôle d'accès au sein des catégories de règles et entre elles. Vous pouvez, cependant, créer des rôles personnalisés qui empêchent les utilisateurs de déplacer et de modifier les règles. Tout utilisateur autorisé à modifier les politiques de contrôle d'accès peut ajouter des règles aux catégories personnalisées et modifier les règles de celles-ci sans restriction.

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.

Astuces Un ordre adéquat des règles de contrôle d'accès réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles. Bien que les règles que vous créez soient uniques à chaque organisation et chaque déploiement, il existe quelques consignes générales à suivre lors de la mise en ordre des règles qui peuvent optimiser les performances tout en répondant à vos besoins.

Sujets connexes

Bonnes pratiques pour les règles de tri

Actions de règles de contrôle d'accès

Chaque règle de contrôle d'accès comporte une *action* qui détermine la manière dont le système traite et enregistre le trafic correspondant. Vous pouvez surveiller, faire confiance, bloquer ou autoriser (avec ou sans inspection supplémentaire).

L' *action par défaut* de la politique de contrôle d'accès gère le trafic qui ne répond aux conditions d'aucune règle de contrôle d'accès avec une action autre que Surveiller.

Action du moniteur des règles de contrôle d'accès

L'action **Monitor** (Surveiller) n'est pas conçue pour autoriser ou refuser le trafic. Son objectif principal est plutôt de forcer la journalisation de la connexion, quelle que soit la façon dont le trafic correspondant est finalement géré.

Si une connexion correspond à une règle Monitor (Surveiller), la prochaine règle non-Monitor à laquelle la connexion correspond devrait déterminer le traitement du trafic et toute inspection supplémentaire. S'il n'y a pas de règle de correspondance supplémentaire, le système doit utiliser l'action par défaut.

Il existe cependant une exception. Si une règle Monitor (surveillance) contient des conditions de couche 7, comme une condition d'application, le système *permet aux premiers paquets de passer* et la connexion est établie (ou permet l'établissement de l'établissement de liaison SSL). Cela se produit même si la connexion est bloquée par une règle ultérieure; en effet, ces premiers paquets *ne sont pas évalués par rapport aux règles suivantes*. Pour que ces paquets n'atteignent pas leur destination sans être inspectés, vous pouvez spécifier une politique de prévention des intrusions à cette fin dans les paramètres avancés de la politique de contrôle d'accès; voir Inspection des paquets qui passent avant que le trafic ne soit identifié. Une fois que le système a terminé son identification de couche 7, il applique l'action appropriée au trafic de session restant.

Mise en garde Comme bonne pratique, *évitez de placer des conditions de couche 7 sur des règles de surveillance définies au sens large en haut de l'ordre de priorité de vos règles*, pour éviter d'autoriser par inadvertance le trafic dans votre réseau. En outre, si le trafic lié localement correspond à une règle de surveillance dans un déploiement de couche 3, ce trafic peut contourner l'inspection. Pour assurer l'inspection du trafic, activez **Inspect Local Router Traffic** (Inspecter le trafic du routeur local) dans les paramètres avancés du périphérique géré qui achemine le trafic.

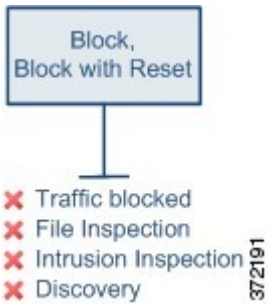
Action de confiance des règles de contrôle d'accès

L'action **Trust** (confiance) permet au trafic de passer sans inspection approfondie ni découverte du réseau. Le trafic de confiance est toujours soumis à des exigences d'identité et à la limitation de débit.

Remarque Certains protocoles, comme FTP et SIP, utilisent des canaux secondaires que le système ouvre pendant le processus d'inspection. Dans certains cas, le trafic de confiance peut contourner toute inspection et ces canaux secondaires ne peuvent pas être ouverts correctement. Si vous rencontrez ce problème, modifiez la règle de confiance en **Allow** (Autoriser).

Actions de blocage des règles de contrôle d'accès

Les actions **Block** (blocage) et **Block with reset** (blocage avec réinitialisation) refusent le trafic sans autre inspection d'aucune sorte.



Les règles de blocage avec réinitialisation réinitialisent la connexion, à l'exception des requêtes web pour lesquelles c'est la *Page de réponse HTTP* qui intervient. En effet, la page de réponse, que vous configurez pour s'afficher lorsque le système bloque les requêtes Web, ne peut pas s'afficher si la connexion est réinitialisée immédiatement.

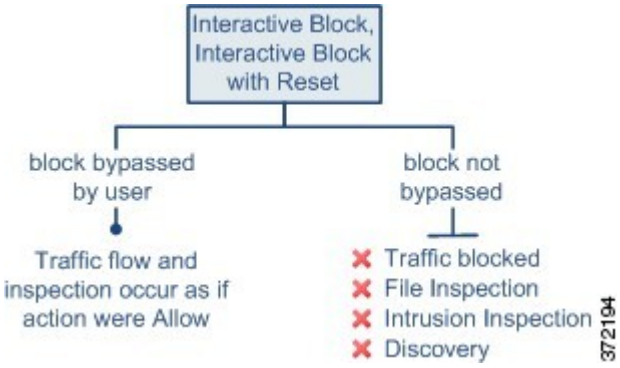
Pour en savoir plus, consultez Configurer les pages de réponse HTTP.

Sujets connexes

Configurer les pages de réponse HTTP

Actions de blocage interactif des règles de contrôle d'accès

Les actions Blocage interactif et **Blocage interactif avec réinitialisation** offrent aux utilisateurs Web la possibilité de continuer vers la destination prévue.



Si un utilisateur contourne le blocage, la règle imite une règle Allow (autorisation). Par conséquent, vous pouvez associer des règles de blocage interactif aux politiques de fichiers et de prévention des intrusions, et le trafic correspondant est également admissible pour la découverte de réseau.

Si un utilisateur ne contourne pas le blocage (ou ne peut pas le faire), la règle imite une règle de blocage. Le trafic correspondant est refusé sans autre inspection.

Notez que si vous activez le blocage interactif, vous ne pouvez pas réinitialiser *toutes* les connexions bloquées. En effet, la page de réponse ne peut pas s'afficher si la connexion est réinitialisée immédiatement. Utilisez l'action **Interactive Block with reset** (blocage interactif avec réinitialisation) pour bloquer (de manière non interactive) avec réinitialisation tout le trafic non Web, tout en activant le blocage interactif pour les demandes Web.

Pour en savoir plus, consultez Configurer les pages de réponse HTTP.

Sujets connexes

Actions de blocage de Règle de déchiffrement

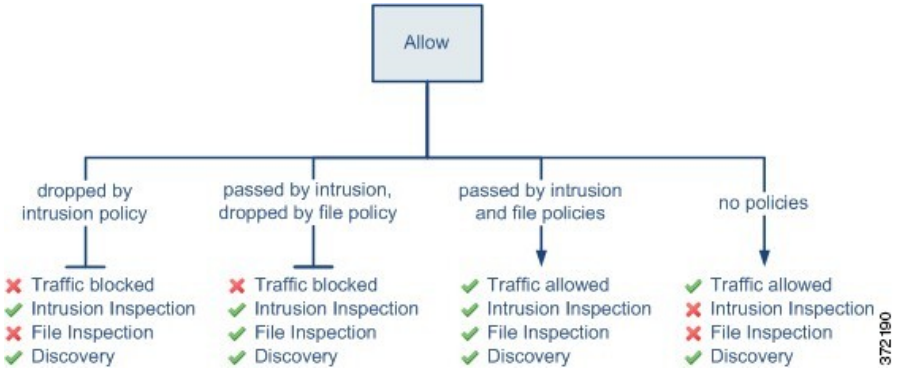
Action Allow (autorisation) des règles de contrôle d'accès

L'action **Allow** (autoriser) permet au trafic correspondant de passer, bien qu'il soit toujours soumis aux exigences d'identité et à la limitation de débit.

Vous pouvez également utiliser l'inspection approfondie pour inspecter davantage et bloquer le trafic non chiffré ou déchiffré avant qu'il n'atteigne sa destination :

- Vous pouvez utiliser une politique de prévention des intrusions pour analyser le trafic réseau en fonction des configurations de détection et de prévention des intrusions et abandonner les paquets fautifs selon la configuration.
- Vous pouvez effectuer le contrôle de fichier à l'aide d'une politique de fichiers. Le contrôle des fichiers vous permet de détecter et d'empêcher vos utilisateurs de téléverser (envoyer) ou de télécharger (recevoir) des fichiers de types spécifiques par le biais de protocoles d'application spécifiques.
- Vous pouvez effectuer une protection réseau avancée contre les programmes malveillants (AMP), également à l'aide d'une politique de fichiers. Défense contre les programmes malveillants peut inspecter les fichiers pour détecter les programmes malveillants et bloquer ces derniers détectés selon la configuration.

Le diagramme suivant illustre les types d'inspection effectués sur le trafic qui répond aux conditions d'une règle Allow (Autoriser) (ou d'une règle Interactive Block (Bloquer) contournée par l'utilisateur). Vous constaterez que l'inspection des fichiers a lieu avant l'inspection de prévention des intrusions; les fichiers bloqués ne sont pas inspectés pour les exploitations liées à une intrusion.



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 sont associées à une règle de contrôle d'accès. Vous pouvez, cependant, configurer l'un sans l'autre. 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.

Que le trafic soit inspecté ou abandonné par une politique de prévention des intrusions ou de fichier, le système peut l'inspecter à l'aide de la découverte de réseau. Cependant, autoriser le trafic ne garantit pas automatiquement l'inspection de découverte. Le système effectue la découverte uniquement pour les connexions impliquant des adresses IP explicitement surveillées par votre politique de découverte de réseau. en outre, la découverte d'applications est limitée aux sessions chiffrées.

Exigences et conditions préalables des règles de contrôle d'accès

Prise en charge des modèles

N’importe lequel

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Administrateur d’accès
- Administrateur de réseau

Lignes directrices et limites pour les règles de contrôle d’accès

- Si vous modifiez une règle de contrôle d'accès qui est activement utilisée, les modifications ne s'appliquent pas aux connexions établies au moment du déploiement. La règle mise à jour est utilisée pour la mise en correspondance avec les connexions futures. Cependant, si le système inspecte activement une connexion (par exemple, avec une politique de prévention des intrusions), *il* appliquera les critères de correspondance ou d’action modifiés aux connexions existantes.

  Pour défense contre les menaces , vous pouvez vous assurer que vos modifications s’appliquent à toutes les connexions actuelles en utilisant la commande CLI défense contre les menaces **clear conn** pour mettre fin aux connexions établies. Notez que vous ne devez le faire que s'il est acceptable de mettre fin à ces connexions, en partant du principe que les sources des connexions tenteront alors de rétablir la connexion et seront donc comparées de manière appropriée à la nouvelle règle.

- Les balises VLAN dans les règles d’accès s’appliquent uniquement aux ensembles en ligne ; elles ne peuvent pas être utilisées dans les règles d’accès appliquées aux interfaces de pare-feu.

- Pour utiliser des objets réseau de nom de domaine complet (FQDN) comme critères de source ou de destination, vous devez également configurer DNS pour les interfaces de données dans la politique des paramètres de plateforme. Le système n’utilise pas le paramètre du serveur DNS de gestion pour rechercher les objets de nom de domaine complet (FQDN) utilisés dans les règles de contrôle d’accès.

  Notez que le contrôle de l’accès par nom de domaine complet (FQDN) est un mécanisme du meilleur effort. Prenez en compte les points suivants:

  - Étant donné que les réponses DNS peuvent être contrefaites, utilisez uniquement des serveurs DNS internes entièrement fiables.

  - Certains noms de domaine complets, en particulier pour les serveurs très populaires, peuvent avoir des centaines, sinon des milliers d’adresses IP, et celles-ci peuvent changer fréquemment. Comme le système utilise les résultats de recherche DNS en cache, les utilisateurs peuvent obtenir des

adresses qui ne sont pas encore dans le cache et leurs connexions ne correspondent pas à la règle FQDN. Les règles qui utilisent des objets réseau FQDN ne fonctionnent efficacement que pour les noms qui se résolvent en moins de 100 adresses.

Nous vous recommandons de ne pas créer de règles d'objet réseau pour un nom de domaine complet qui se résout à plus de 100 adresses, car la probabilité que l'adresse d'une connexion en soit une qui a été résolue et disponible dans le cache DNS du périphérique est faible. Dans ces cas-là, utilisez une règle basée sur URL plutôt qu'une règle d'objet réseau FQDN.

- Pour les noms de domaine complets populaires, différents serveurs DNS peuvent renvoyer un ensemble d'adresses IP différent. Ainsi, si vos utilisateurs utilisent un serveur DNS différent de celui que vous configurez, les règles de contrôle d'accès basé sur le nom de domaine complet (FQDN) pourraient ne pas s'appliquer à toutes les adresses IP du site qui sont utilisées par vos clients, et vous n'obtiendrez pas les résultats escomptés pour vos règles .
- Certaines entrées de nom de domaine complet (FQDN) ont des valeurs de durée de vie très courte (TTL). Cela peut entraîner des recompilations fréquentes de la table de recherche, ce qui peut avoir une incidence sur les performances globales du système.

- Le nombre maximal d'objets par critère de correspondance par règle de contrôle d'accès est de 200. Par exemple, vous pouvez avoir jusqu'à 200 objets réseau dans une seule règle de contrôle d'accès.

Gestion des règles de contrôle d'accès

Les rubriques suivantes expliquent comment gérer les règles de contrôle d'accès.

Ajout d'une catégorie de règles de contrôle d'accès

Vous pouvez diviser les sections de règles obligatoires et par défaut d'une politique de contrôle d'accès en catégories personnalisées. Une fois que vous avez créé une catégorie, vous ne pouvez plus la déplacer, mais vous pouvez la supprimer, la renommer et déplacer des règles à l'intérieur, à l'extérieur, au sein et autour d'elle. Le système attribue des numéros de règle aux sections et aux catégories.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Add Category** (Ajouter une catégorie).

Astuces Si votre politique contient déjà des règles, vous pouvez cliquer dans une zone vide de la ligne correspondant à une règle existante pour définir la position de la nouvelle catégorie avant de l'ajouter. Vous pouvez également cliquer avec le bouton droit sur une règle existante et sélectionner **Insert new category**(Insérer une nouvelle catégorie).

Étape 2 Saisissez un **Nom**.

Étape 3 Dans la liste déroulante **Insert** (insérer), choisissez l'emplacement où vous souhaitez ajouter la catégorie :

- Pour insérer une catégorie sous toutes les catégories existantes d'une section, choisissez **dans Obligatoire** ou **dans Par défaut**.

- Pour insérer une catégorie au-dessus d'une catégorie existante, choisissez **au-dessus de la catégorie**, puis choisissez une catégorie.
- Pour insérer une catégorie au-dessus ou au-dessous d'une règle de contrôle d'accès, choisissez **au-dessus de la règle** ou **au-dessous de la règle**, puis saisissez un numéro de règle existante.

Étape 4 Cliquez sur **Apply** (Appliquer) .

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

Créer et modifier les règles de contrôle d'accès

Utilisez les règles de contrôle d'accès pour appliquer des actions à des classes de trafic spécifiques. Les règles vous permettent d'autoriser le trafic souhaitable et d'abandonner le trafic indésirable.

Procédure

Étape 1 L'éditeur de politique de contrôle d'accès propose les options suivantes :

- Pour ajouter une nouvelle règle, cliquez sur **Add Rule** (Ajouter une règle).
- Cliquez sur **Edit** () pour modifier une règle existante.
- Pour modifier plusieurs règles, utilisez les cases à cocher et sélectionnez plusieurs règles, puis choisissez **Edit** (Modifier) ou une autre action dans la liste **Sélectionner une action** à côté de la zone de recherche.
- Pour effectuer une modification en ligne, où vous modifiez la configuration d'un objet dans une condition de règle, effectuez un clic droit sur la valeur et choisissez **Edit** (Modifier). Vous pouvez également utiliser le menu contextuel pour supprimer un élément, l'ajouter au filtre, ou copier le texte ou la valeur.

Si**Afficher** () apparaît à côté d'une règle, la règle appartient à une politique ancêtre ou vous n'êtes pas autorisé (e) à modifier la règle.

Étape 2 S'il s'agit d'une nouvelle règle, saisissez un **Nom**.

Étape 3 Configurez les composants de la règle.

Si vous modifiez en bloc plusieurs règles, seul un sous-ensemble d'options est disponible.

- Position (position) : spécifiez la position de la règle; voir Ordre des règles de contrôle d'accès, à la page 5.
- Action : sélectionnez une **Action** de règle; voir Actions de règles de contrôle d'accès, à la page 6.
- Inspection approfondie : (facultatif) Pour les règles Allow (autorisation) et Interactive Block (blocage interactif), sélectionnez les options de **Politique de prévention des intrusions**, **Ensemble de variables** et **Politique de fichiers**. Vous pouvez appliquer les politiques de prévention des intrusions et de fichiers indépendamment; vous n'avez pas besoin de configurer les deux.
- Plage de temps : (facultatif) Pour les périphériques défense contre les menaces , choisissez les jours et les heures auxquels la règle est applicable. Si vous ne choisissez aucune option, la règle est toujours active. Pour de plus amples renseignements, consultez la section Création d'objets de plages temporelles.

- Logging (Journalisation) : cliquez sur **Logging** pour préciser les options de journalisation de la connexion et les interruptions SNMP.
- Conditions (conditions) : sélectionnez les objets que vous souhaitez ajouter, soit la source ou la destination, puis cliquez sur **Add to Sources** (Ajouter aux sources) ou **Add to Destinations and Applications** (Ajouter aux destinations ou applications) pour ajouter des conditions correspondantes pour les connexions. Vous pouvez cliquer sur un onglet pour restreindre la liste des objets disponibles, par exemple, aux réseaux, aux zones de sécurité, aux applications, etc. Cependant, les colonnes des sources et de la destination affichent toujours tous les objets sélectionnés, quel que soit l'onglet dans lequel vous vous trouvez. Consultez Conditions des règles de contrôle d'accès, à la page 13 pour obtenir de plus amples renseignements.
- Commentaires : ouvrez la liste de commentaires au bas de la boîte de dialogue, saisissez votre commentaire et cliquez sur **Post** (Publier) pour ajouter un commentaire.

Étape 4 Cliquez sur **OK** pour enregistrer la règle.

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

Prochaine étape

Si vous déployez des règles basées sur le temps, spécifiez le fuseau horaire du périphérique auquel la politique est attribuée. Consultez Fuseau horaire.

Déployer les changements de configuration.

Sujets connexes

Bonnes pratiques pour les règles de contrôle d'accès

Conditions des règles de contrôle d'accès

Les conditions de règle définissent les caractéristiques des connexions que vous souhaitez cibler avec chaque règle. Utilisez les conditions précisément pour affiner la règle afin de l'appliquer à tout le trafic et uniquement au trafic qui doit être géré par la règle. Les rubriques suivantes expliquent les conditions de correspondance que vous pouvez utiliser.

Conditions de règle de sécurité/zone de tunnel

Vous pouvez utiliser des zones de sécurité et des zones de tunnel pour sélectionner le trafic pour une règle.

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 zones de tunnel vous permettent d'identifier le trafic en tunnel, tel que GRE, qui doit être géré comme un tunnel plutôt que d'appliquer des règles de contrôle d'accès aux connexions encapsulées dans le tunnel.

Vous pouvez utiliser des zones de sécurité pour contrôler le trafic en fonction de ses interfaces 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 de sécurité 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.

Lorsque vous utilisez des zones de tunnel, assurez-vous de comporter des règles correspondantes dans la politique de préfiltre pour associer le trafic tunnelisé à la zone. Ensuite, vous pouvez sélectionner la zone de tunnel comme zone source dans une règle; les zones de tunnel ne peuvent pas être des destinations. Si vous ne possédez pas de règles de préfiltre pour modifier le zonage des tunnels dans la zone de tunnel, une règle de contrôle d'accès pour le tunnel ne s'appliquera jamais aux connexions. Vous pouvez spécifier des zones de sécurité de destination pour les tunnels cibles qui quittent le périphérique par des interfaces spécifiques.

Considérations relatives aux zones de sécurité

Tenez compte des éléments suivants lorsque vous décidez des critères de zone de sécurité :

- 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.
- Les règles de contrôle d'accès génèrent des entrées ACL (ACE) dans la configuration du périphérique pour assurer un traitement et des abandons précoces chaque fois que cela est possible. Si vous spécifiez des zones de sécurité dans les règles, des listes de contrôle d'accès (ACE) sont créées pour chaque interface de la zone, ce qui peut considérablement augmenter la taille de la liste de contrôle d'accès. Des listes de contrôle d'accès excessivement volumineuses générées à partir des règles de contrôle d'accès peuvent avoir une incidence sur les performances du système.
- 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 sont les objets de réseau ou les emplacements géographiques qui définissent les adresses de réseau ou les emplacements du trafic.

- Pour faire correspondre le trafic provenant d'une adresse IP ou d'un emplacement géographique, ajoutez les critères à la liste Sources.
- Pour faire correspondre le trafic provenant d'une adresse IP ou d'un emplacement géographique, ajoutez les critères à la liste Destination.
- Si vous ajoutez des conditions de réseau source et de destination à une règle, le trafic correspondant doit provenir de l'une des adresses IP spécifiées et être destiné à l'une des adresses IP de destination.

Lorsque vous ajoutez ce critère, vous sélectionnez les onglets suivants :

- **Network** (réseau) : Sélectionnez les objets ou groupes réseau qui définissent les adresses IP source ou de destination du trafic que vous souhaitez contrôler.

  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.

  Vous pouvez utiliser des objets qui définissent l'adresse utilisant le nom de domaine complet (FQDN); l'adresse est déterminée au moyen d'une recherche DNS. Toutefois, les objets de nom de domaine complet (FQDN) ne sont pas pris en charge pour les sections suivantes dans les politiques de contrôle d'accès : Original Client networks (réseaux client d'origine), SGT/ISE attributes (attributs SGT/ISE), Network

Analysis And Intrusion policy (politique d'analyse de réseau et de prévention des intrusions), Security Intelligence (renseignements sur la sécurité), Threat Detection (détection des menaces), et Elephant Flow Settings (paramètres du flux d'éléphants).

- **Geolocation** (géolocalisation) : Sélectionnez l'emplacement géographique pour contrôler le trafic en fonction de son pays ou continent de source ou de destination. La sélection d'un continent sélectionne tous les pays du continent. En plus de sélectionner l'emplacement géographique directement dans la règle, vous pouvez également sélectionner un objet de géolocalisation que vous avez créé pour définir l'emplacement. En utilisant la localisation géographique, vous pouvez facilement restreindre l'accès à un pays en particulier sans avoir besoin de connaître toutes les adresses IP potentielles qui y sont utilisées.

Remarque Pour vous assurer que vous utilisez des données de localisation géographique à jour pour filtrer votre trafic, Cisco vous recommande fortement de mettre à jour régulièrement la base de données de géolocalisation (GeoDB).

Client d'origine dans conditions de réseau (filtrage du trafic par serveur mandataire)

Pour certaines règles, vous pouvez gérer le trafic par mandataire en fonction du client d'origine. Utilisez une condition de réseau source pour préciser les serveurs mandataires, puis ajoutez une contrainte de client d'origine pour préciser les adresses IP du client d'origine. Le système utilise le champ d'en-tête X-Forwarded-For (XFF), True-Client-IP ou HTTP défini sur mesure d'un paquet pour déterminer l'adresse IP du client d'origine.

Le trafic correspond à la règle si l'adresse IP du mandataire correspond à la contraintes de réseau source de la règle **et** si l'adresse IP du client d'origine correspond à la contrainte de client d'origine de la règle. Par exemple, pour autoriser le trafic à partir d'une adresse d'origine spécifique du client, mais uniquement s'il utilise un serveur mandataire en particulier, créez trois règles de contrôle d'accès :

Règle de contrôle d'accès 1 : bloque le trafic par mandataire à partir d'une adresse IP spécifique (209.165.201.1)

Réseaux sources : 209.165.201.1
Réseaux client d'origine : aucun/tous
Action : Bloc (Bloquer)

Règle de contrôle d'accès 2 : autoriser le trafic par mandataire à partir de la même adresse IP, mais uniquement si vous choisissez le serveur mandataire pour ce trafic (209.165.200.225 ou 209.165.200.238).

Réseaux sources : 209.165.200.225 et 209.165.200.238
Réseaux client d'origine : 209.165.201.1
Action : Allow (Autoriser)

Règle de contrôle d'accès 3 : bloque le trafic par mandataire à partir de la même adresse IP si elle utilise un autre serveur mandataire.

Réseaux sources : tous
Réseaux client d'origine : 209.165.201.1
Action : Bloc (Bloquer)

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.

Conditions des règles d'utilisateur

Les conditions des règles d'utilisateur correspondent au trafic en fonction de l'utilisateur qui initie la connexion ou du groupe auquel l'utilisateur appartient. Par exemple, vous pouvez configurer une règle de blocage pour interdire à tout membre du groupe des finances d'accéder à une ressource réseau.

Pour les règles de contrôle d'accès uniquement, vous devez d'abord associer une politique d'identité à la politique de contrôle d'accès, comme indiqué dans Association d'autres politiques au contrôle d'accès.

En plus de configurer les utilisateurs et les groupes pour les domaines configurés, vous pouvez définir des politiques pour les utilisateurs d'identités spéciales suivants :

- Échec de l'authentification : utilisateur qui a échoué à l'authentification avec le portail captif.
- Invité : utilisateurs configurés comme utilisateurs invités dans le portail captif.
- Aucune authentification requise : utilisateurs qui correspondent à une action de règle **Aucune authentification requise n'est requise**.

- Inconnu : utilisateurs qui ne peuvent pas être identifiés; par exemple, les utilisateurs qui ne sont pas téléchargés par un domaine configuré.

Conditions des règles d'application

Lorsque le système analyse le trafic IP, il peut identifier et classer les applications couramment utilisées sur votre réseau. Cette *connaissance des applications* basée sur la découverte constitue la base du *contrôle des applications*, c'est-à-dire la capacité de contrôler le trafic des applications.

Les *filtres d'applications* fournis par le système vous aident à effectuer le contrôle des applications en organisant les applications en fonction de caractéristiques de base: type, risque, pertinence commerciale, catégorie et balises. Vous pouvez créer des filtres définis par l'utilisateur réutilisables en fonction de combinaisons de filtres fournis par le système ou de combinaisons personnalisées d'applications.

Au moins un détecteur doit être activé pour chaque condition de règle d'application dans la politique. Si aucun détecteur n'est activé pour une application, le système active automatiquement tous les détecteurs fournis par le système pour l'application; s'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour l'application. Pour en savoir plus sur les détecteurs d'application, consultez Principes fondamentaux des détecteurs d'applications.

Vous pouvez utiliser à la fois des filtres d'application et des applications spécifiées individuellement pour assurer une couverture complète. Cependant, lisez la note suivante avant de commander vos règles de contrôle d'accès.

Avantages des filtres d'application

Les filtres d'applications vous aident à configurer rapidement le contrôle des applications. Par exemple, vous pouvez facilement utiliser les filtres fournis par le système pour créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible intérêt pour l'entreprise. Si un utilisateur tente d'utiliser l'une de ces applications, le système bloque la session.

L'utilisation de filtres d'application simplifie la création et l'administration des politiques. Cela vous garantit que le système contrôle le trafic des applications comme prévu. Étant donné que Cisco met fréquemment à jour et ajoute des détecteurs d'applications par l'intermédiaire des mises à jour du système et de la base de données de vulnérabilités (VDB), vous pouvez vous assurer que le système utilise des détecteurs à jour pour surveiller le trafic des applications. Vous pouvez également créer vos propres détecteurs et attribuer des caractéristiques aux applications qu'ils détectent, en les ajoutant automatiquement aux filtres existants.

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 1 : 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.

Caractéristiques	Description	Exemple
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`.

Sujets connexes

Bonnes pratiques pour la configuration du contrôle des applications

Configuration des conditions d'application et des filtres

Pour créer une condition d'application ou un filtre, choisissez les applications dont vous souhaitez contrôler le trafic dans une liste d'applications disponibles. Il est facultatif (et recommandé) de restreindre les applications disponibles à l'aide de filtres. Vous pouvez utiliser des filtres et des applications précisées individuellement dans la même condition.

Avant de commencer

- Le profilage adaptatif doit être activé (son état par défaut) comme décrit dans Configuration des profils adaptatifs pour que les règles de contrôle d'accès effectuent le contrôle d'application.
- Si vous mettez en œuvre des restrictions de contenu, suivez la procédure dans Utilisation de règles de contrôle d'accès pour appliquer une restriction de contenu au lieu de celle-ci.
- Pour les modèles de périphériques classiques, vous devez avoir la licence de contrôle pour configurer ces conditions.

Procédure

Étape 1 Appelez la règle ou l'éditeur de configuration :

- Contrôle d'accès, déchiffrement, condition de règle QoS : dans l'éditeur de règles, cliquez sur **Applications**.
- Conditions de la règle d'identité : dans l'éditeur de règles, cliquez sur **Realms and Settings** (domaines et paramètres) et activez l'authentification active. voir Créer une règle d'identité.
- Application filter (filtre d'application) : dans la page Application Filters (filtres d'applications) du gestionnaire d'objets, ajoutez ou modifiez un filtre d'application. Fournissez un **nom** unique pour le filtre.

- Intelligent Application Bypass (IAB) (Contournement d'application intelligent) : Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced**(Avancé) et modifiez les paramètres de l'IAB, puis cliquez sur **Bypassable Applications and Filters** (Applications et filtres contournables).

Étape 2 Recherchez et choisissez les applications que vous souhaitez ajouter dans la liste des **applications disponibles**.

Pour restreindre les applications affichées dans les **applications disponibles**, sélectionnez un ou plusieurs **filtres d'applications** ou recherchez des applications individuelles.

Astuces Cliquez sur **Information** ( ) à côté d'une application pour afficher un résumé et des liens de recherche sur Internet. **Unlock** marque des applications que le système peut identifier uniquement dans le trafic déchiffré.

Lorsque vous choisissez des filtres, individuellement ou en combinaison, la liste des applications disponibles est mise à jour pour afficher uniquement les applications qui répondent à vos critères. Vous pouvez choisir une combinaison de filtres fournis par le système, mais pas de filtres définis par l'utilisateur.

- Plusieurs filtres pour la même caractéristique (risque, pertinence commerciale, etc.) : Le trafic d'application doit correspondre à un seul des filtres. Par exemple, si vous choisissez les filtres à risque moyen et à risque élevé, la liste des applications disponibles affichera toutes les applications à risque moyen et élevé.
- Filtres pour différentes caractéristiques d'application : le trafic de l'application doit correspondre aux deux types de filtres. Par exemple, si vous choisissez les filtres de pertinence commerciale faible et élevé à risque, la liste des applications disponibles affichera uniquement les applications qui répondent aux deux critères.

Étape 3 Cliquez sur **Add Application** (ajouter une application), ou **Add to Rule** (ajouter à la règle) ou effectuez un glisser-déposer.

Astuces Avant d'ajouter d'autres filtres et applications, cliquez sur **Clear Filters** (effacer les filtres) pour effacer vos choix actuels.

Étape 4 Enregistrez ou continuez de modifier la règle ou la configuration.

Prochaine étape

- Déployer les changements de configuration.

Conditions de règle de port, de protocole et de code ICMP

Les conditions des ports correspondent au trafic en fonction des ports de source et de destination. Selon le type de règle, le « port » peut signifier l'un des éléments suivants :

- TCP et UDP : vous pouvez contrôler le trafic TCP et UDP en fonction du port. Le système représente cette configuration à l'aide du numéro de protocole entre parenthèses, ainsi que d'un port ou d'une plage de ports facultatif. Par exemple : TCP(6)/22.
- ICMP : vous pouvez contrôler le trafic ICMP et ICMPv6 (IPv6-ICMP) en fonction de son protocole de couche Internet, ainsi que d'un type et d'un code facultatifs. Par exemple : ICMP(1):3:3.
- Protocol (protocole) : Vous pouvez contrôler le trafic à l'aide d'autres protocoles qui n'utilisent pas de ports.

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.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic. Notez que le filtrage des applications n'est pas disponible dans les règles de préfiltre.

Le filtrage des applications est également recommandé pour les applications, comme FTP, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port de destination dans une seule règle de contrôle d'accès.

Mise en correspondance du trafic non TCP avec les conditions du port

Vous pouvez mettre en correspondance des protocoles non basés sur les ports. Par défaut, si vous ne spécifiez pas de condition de port, vous faites correspondre le trafic IP. Bien que vous puissiez configurer des conditions de port pour qu'elles correspondent au trafic non-TCP, il existe certaines restrictions :

- Access control Rules : Pour les périphériques classiques, vous pouvez faire correspondre le trafic encapsulé en GRE avec une règle de contrôle d'accès en utilisant le protocole GRE (47) comme condition de port de destination. À une règle soumise à des contraintes GRE, vous pouvez ajouter uniquement des conditions basées sur le réseau : zone, adresse IP, port et balise VLAN. En outre, le système utilise des en-têtes externes pour faire correspondre **tout** le trafic dans les politiques de contrôle d'accès avec les règles contraintes de GRE. Pour les périphériques défense contre les menaces, utilisez les règles de tunnel dans la politique de préfiltre pour contrôler le trafic encapsulé GRE.
- Règlesdedéchiffrement : ces règles prennent uniquement en charge les conditions de port TCP.
- ÉCHO IMCP : un port ICMP de destination avec le type défini à 0 ou un port ICMPv6 de destination avec le type défini à 129 correspond uniquement aux réponses écho non sollicitées. Les réponses ECHO ICMP envoyées en réponse aux demandes ECHO ICMP sont ignorées. Pour qu'une règle corresponde à n'importe quel écho ICMP, utilisez ICMP de type 8 ou ICMPv6 de type 128.

Conditions de règle d'URL

Utilisez des conditions d'URL pour contrôler les sites Web auxquels les utilisateurs de votre réseau peuvent accéder.

Pour obtenir des renseignements complets, consultez Filtrage d'URL.

Conditions de règle d'attributs dynamiques

Les attributs dynamiques sont les suivants :

- Objets dynamiques (provenant, par exemple, de Connecteur d'attributs dynamiques Cisco Secure)

  Le connecteur d'attributs dynamiquesvous permet de collecter des données (telles que les réseaux et les adresses IP) auprès des fournisseurs de services en nuage et de les envoyer à () afin qu'elles puissent être utilisées dans les règles de contrôle d'accès. .

  Pour plus d'informations sur connecteur d'attributs dynamiques, voir les informations figurant dans la suite de ce guide.

- Objets SGT
- Objets IP d'emplacement
- Objets de type de périphérique
- Profil de point terminal

Les attributs dynamiques peuvent être utilisés comme critères de source et de destination dans les règles de contrôle d'accès. Utilisez les consignes suivantes :

- Des objets de types différents sont réunis par AND ensemble
- Les objets de type similaire sont soumis à une opération OU

Par exemple, si vous choisissez les critères de destination de la source SGT 1, SGT 2 et le type de périphérique 1; la règle est mise en correspondance si le type de périphérique 1 est détecté sur SGT 1 ou SGT 2.

À propos des objets dynamiques créés par l'API

Un *objet dynamique* est un objet qui spécifie une ou plusieurs adresses IP récupérées à l'aide des appels d'API REST ou à l'aide de la Connecteur d'attributs dynamiques Cisco Secure, qui est capable de mettre à jour les adresses IP à partir de sources dans le nuage. Ces objets dynamiques peuvent être utilisés dans les règles de contrôle d'accès sans qu'il soit nécessaire de déployer la politique de contrôle d'accès par la suite.

Pour plus d'informations sur connecteur d'attributs dynamiques, voir les informations figurant dans la suite de ce guide.

Les différences entre les objets dynamiques et les objets réseau sont les suivantes :

- Les objets dynamiques créés à l'aide de connecteur d'attributs dynamiques sont envoyés vers centre de gestion dès qu'ils sont créés et sont mis à jour à des intervalles réguliers.
- Objets dynamiques créés par l'API :
  - Sont des adresses IP, avec ou sans ou sans classe de routage inter-domaine (CIDR), qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.
  - Ne prend pas en charge les noms de domaine complets ou les plages d'adresses.
  - Doit être mis à jour à l'aide d'une API.

Sujets connexes

Ajouter ou modifier un objet dynamique créé par l'API

Configurer les conditions d'attributs dynamiques

Lorsque vous configurez des attributs dynamiques pour une règle de contrôle d'accès, les objets du même type font l'objet d'un OU et les objets de types différents font l'objet d'un ET. Un exemple est présenté à la fin de cette rubrique.

Remarque Cette procédure est basée sur l'interface utilisateur existante. Dans la nouvelle présentation de l'interface utilisateur, vous pouvez ajouter des attributs dynamiques en cliquant sur **Ajouter** (+) dans les champs **Sources** et **destinations et Applications**.

Avant de commencer

Créer des objets dynamiques et comprendre comment ces objets sont utilisés dans la politique de contrôle d'accès.

Pour en savoir plus sur les objets dynamiques, consultez À propos des objets dynamiques créés par l'API.

Pour en savoir plus sur l'utilisation des objets dynamiques dans la politique de contrôle d'accès, consultez Conditions de règle d'attributs dynamiques, à la page 21.

Procédure

Étape 1 Dans l'éditeur de règles, cliquez sur **Attributs dynamiques**.

Étape 2 Effectuez l'une des opérations suivantes dans la section Attributs disponibles :

- Saisissez une partie du nom complet d'un attribut dans le champ.
- Cliquez sur **Balise de groupe de sécurité** ou sur **Objets dynamiques** pour afficher uniquement les objets de ce type.

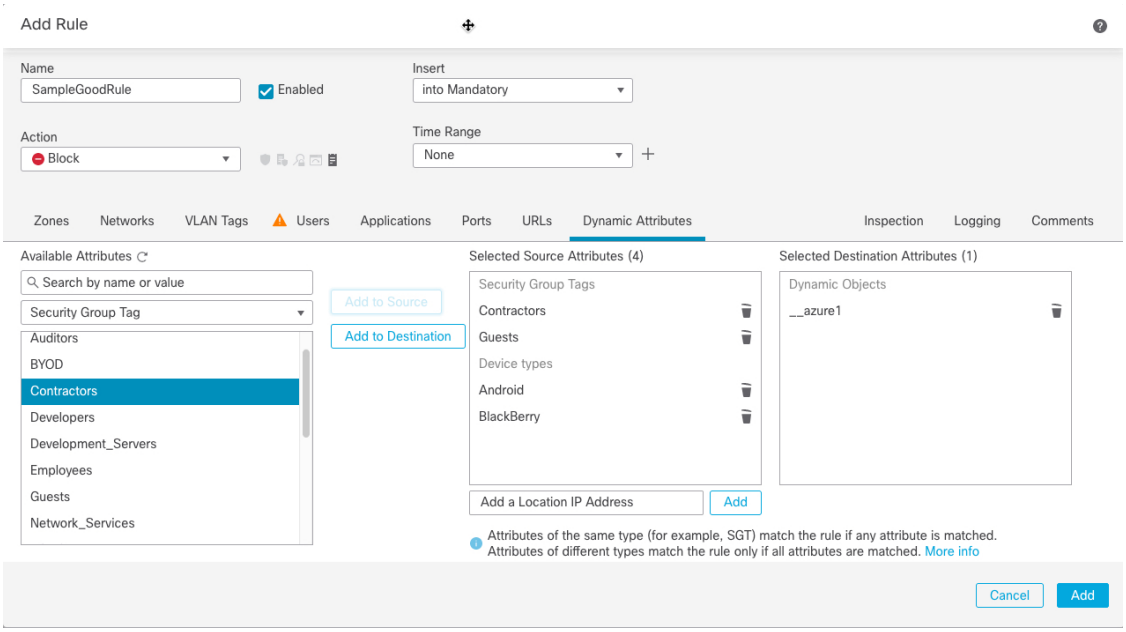
Étape 3 Pour appliquer les objets que vous avez sélectionnés aux critères de correspondance de source, cliquez sur **Add to Source** (Ajouter à la source).

Étape 4 Pour appliquer les objets que vous avez sélectionnés aux critères de correspondance de la destination, cliquez sur **Add to Destination** (Ajouter à la destination).

Étape 5 Lorsque vous avez terminé de configurer le domaine, cliquez sur **Save** (Enregistrer).

Exemple : utilisation de plusieurs conditions de source dans une règle de blocage

L'exemple suivant bloque l'accès à l'objet dynamique au trafic provenant des étiquettes de groupe de sécurité Sous-traitants ou Invités et des types de périphériques Android ou Blackberry **__azure1**.



Prochaine étape

- Déployer les changements de configuration.

Conditions des règles de date et d'heure

Vous pouvez spécifier une plage temporelle continue ou une période récurrente.

Par exemple, une règle ne peut s'appliquer que pendant les heures de travail en semaine, chaque fin de semaine ou pendant une période d'arrêt pendant un jour férié.

Les règles basées sur le temps sont appliquées en fonction de l'heure locale du périphérique qui traite le trafic.

Les règles basées sur le temps sont prises en charge uniquement sur les périphériques FTD. Si vous affectez une politique avec une règle basée sur le temps à un autre type de périphérique, la restriction de temps associée à la règle est ignorée sur ce périphérique. Vous verrez des avertissements dans ce cas.

Activation et désactivation des règles de contrôle d'accès

Lorsque vous créez une règle de contrôle d'accès, elle est activée par défaut. Si vous désactivez une règle, le système ne l'utilise pas pour évaluer le trafic réseau et arrête de générer des avertissements et des erreurs pour cette règle. Lorsque vous consultez la liste des règles d'une politique de contrôle d'accès, les règles désactivées sont grisées, bien que vous puissiez toujours les modifier.

Vous pouvez également activer ou désactiver une règle de contrôle d'accès à l'aide de l'éditeur de règles.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, effectuez un clic droit sur la règle et choisissez un état de règle.

Si**Afficher** ( ) apparaît à côté d'une règle, la règle appartient à une politique ancêtre ou vous n'êtes pas autorisé (e) à modifier la règle.

Étape 2 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Copie des règles de contrôle d'accès d'une politique de contrôle d'accès vers une autre

Vous pouvez copier des règles de contrôle d'accès d'une politique de contrôle d'accès à une autre. Vous pouvez copier les règles dans la section **par défaut** ou dans la section **obligatoire** de la politique de contrôle d'accès.

Tous les paramètres des règles copiées, à l'exception des commentaires, sont conservés dans la version cible du collage.

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- Pour copier une seule règle, effectuez un clic droit sur la règle et sélectionnez **Copy to Different Policy** (Copier dans une autre politique).
- Pour copier plusieurs règles, cochez leurs cases, puis sélectionnez **Copy to Différentes politiques** (Copier dans plusieurs politiques) dans le menu **Select Bulk Action** (sélectionner l'action de masse).

Étape 2 Sélectionnez la politique de contrôle d'accès de destination dans la liste déroulante **Access Policy** (politique d'accès).

Étape 3 Dans la liste déroulante **Place Rules** (Placer les règles), choisissez l'emplacement des règles copiées. Vous pouvez les placer en en bas des sections obligatoires ou par défaut.

Étape 4 Cliquez sur **Copy** (copier).

Prochaine étape

- Déployer les changements de configuration.

Déplacement des règles de contrôle d'accès vers une politique de préfiltre

Vous pouvez déplacer des règles de contrôle d'accès d'une politique de contrôle d'accès vers la politique de préfiltre associée (autre que la politique par défaut).

Vous devez d'abord appliquer une politique de préfiltre définie par l'utilisateur à la politique de contrôle d'accès. Les règles de contrôle d'accès ne peuvent pas être déplacées vers la politique de préfiltre par défaut, car la politique de préfiltre par défaut ne peut pas contenir de règles.

Avant de commencer

Prenez note des conditions suivantes avant de continuer :

- Lors du déplacement d'une règle de contrôle d'accès vers une politique de préfiltre, les paramètres de la couche 7 (L7) de la règle de contrôle d'accès ne peuvent pas être déplacés. Les paramètres L7 sont abandonnés pendant l'opération.
- Les commentaires de la configuration de la règle de contrôle d'accès sont perdus après le déplacement de la règle. Cependant, un nouveau commentaire est ajouté dans la règle déplacée mentionnant la politique de contrôle d'accès à la source.
- Vous ne pouvez pas déplacer des règles de contrôle d'accès avec **Monitor** (surveillance) défini comme paramètre d'**action**.
- Le paramètre **Action** dans la règle de contrôle d'accès est remplacé par une action appropriée dans la règle de préfiltre lors du déplacement. Pour savoir à quoi correspond chaque action de la règle de contrôle d'accès, consultez le tableau suivant :

Action de la règle de contrôle d'accès	Action de la règle de préfiltre
Autoriser	Analyser
Bloquer	Bloquer
Bloc avec action de réinitialisation	Bloquer
Bloc interactif	Bloquer
Bloc interactif avec action de réinitialisation	Bloquer
Faire confiance	Chemin d'accès rapide

- De même, en fonction de l'action configurée dans la règle de contrôle d'accès, la configuration de la journalisation est définie sur un paramètre approprié après le déplacement de la règle, comme l'indique le tableau suivant.

Action de la règle de contrôle d'accès	Journalisation des configurations dans la règle de préfiltre activée
Autoriser	Aucune des cases n'est cochée.
Bloquer	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP

Action de la règle de contrôle d'accès	Journalisation des configurations dans la règle de préfiltre activée
Bloc avec action de réinitialisation	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP
Bloc interactif	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP
Bloc interactif avec action de réinitialisation	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP
Confiance	• Journaliser au début de la connexion • Journaliser à la fin de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP

- Lors du déplacement des règles de la politique source, si un autre utilisateur modifie ces règles, vous obtenez un message. Vous pouvez continuer le processus après avoir actualisé la page.

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- Pour déplacer une seule règle, effectuez un clic droit sur la règle et sélectionnez **Déplacer vers la politique de préfiltre**.
- Pour déplacer plusieurs règles, cochez leurs cases, puis sélectionnez **Move to Prefilter Policy** (Déplacer vers la politique de préfiltre) du menu **Select Bulk Action** (Sélectionner l'action en bloc).

Étape 2 Dans la liste déroulante **Place Rules** (Placer les règles), choisissez l'emplacement des règles déplacées :

- Pour la positionner comme dernier ensemble de règles, choisissez **En bas de**.
- Pour la positionner comme premier ensemble de règles, choisissez **En haut de**.

Étape 3 Cliquez sur **Move** (Déplacer).

Prochaine étape

- Déployer les changements de configuration.

Positionnement d'une règle de contrôle d'accès

Vous pouvez déplacer une règle existante dans une politique de contrôle d'accès ou insérer de nouvelles règles à l'emplacement souhaité. Lorsque vous ajoutez une règle vers une catégorie ou que vous déplacez une règle, le système la place en dernier dans la catégorie.

Avant de commencer

Passez en revue les consignes d'ordre des règles dans Bonnes pratiques pour les règles de contrôle d'accès.

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- New Rule (nouvelle règle) : insérez une nouvelle règle en passant votre curseur sur la ligne entre les règles existantes et en cliquant sur **Add Rule** (ajouter une règle). L'emplacement est sélectionné dans la **zone Insérer** de la boîte de dialogue Add Rule (ajouter une règle); vous pouvez sélectionner une autre règle pour ajuster l'emplacement. Vous pouvez également sélectionner **Ajouter une règle ci-dessus** ou **Ajouter une règle ci-dessous** dans le menu contextuel.
- Règles existantes lors de l'affichage du tableau des règles : cliquez sur la règle et faites-la glisser vers la nouvelle position.
- Règles existantes lors de l'affichage du tableau des règles : cliquez avec le bouton droit de la souris sur une règle unique et sélectionnez **Repositionner la règle**. Pour déplacer plusieurs règles en tant que groupe, cochez leurs cases, puis sélectionnez les **Repositionner les règles** dans le menu **Sélectionner une action en bloc**.
- Règle existante lors de la modification de la règle cliquez sur l'icône **Repositionner la règle** à côté du nom de la règle.

Étape 2 Choisissez l'emplacement où vous souhaitez déplacer ou insérer la règle :

- Choisissez **dans Obligatoire** ou **dans Par défaut**.
- Choisissez **dans la catégorie**, puis choisissez la catégorie.
- Choisissez **au-dessus de la règle** ou **sous la règle**, puis sélectionnez la règle.

Étape 3 Cliquez sur **Déplacer** ou **Confirmer** et enregistrez la règle si vous la modifiez.

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

Prochaine étape

- Déployer les changements de configuration.

Ajout de commentaires à une règle de contrôle d'accès

Lorsque vous créez ou modifiez une règle de contrôle d'accès, vous pouvez ajouter un commentaire. 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. Vous pouvez afficher une liste de tous les commentaires sur une règle ainsi que l'utilisateur qui a ajouté chaque commentaire et la date à laquelle le commentaire a été ajouté.

Lorsque vous enregistrez une règle, tous les commentaires effectués depuis le dernier enregistrement passent en lecture seule.

Pour rechercher des commentaires sur les règles de contrôle d'accès, utilisez la barre des « règles de recherche » sur la page de la liste des règles.

Procédure

Étape 1 Dans l'éditeur de règles de contrôle d'accès, cliquez sur **Commentaires**.

Étape 2 Saisissez votre commentaire et cliquez sur **Ajouter un commentaire**. Vous pouvez modifier ou supprimer ce commentaire jusqu'à ce que vous enregistriez la règle.

Étape 3 Enregistrer la règle

Bonnes pratiques des règles de contrôle d'accès

Les rubriques suivantes donnent des exemples de règles de contrôle d'accès.

Comment contrôler l'accès à l'aide des zones de sécurité

Imaginez un déploiement dans lequel vous souhaitez que les hôtes aient un accès illimité à Internet, mais que vous souhaitez néanmoins protéger en inspectant le trafic entrant à la recherche de prévention des intrusions et de programmes malveillants.

Tout d'abord, créez deux zones de sécurité : interne et externe. Attribuez ensuite des paires d'interfaces sur un ou plusieurs périphériques à ces zones, en ayant une interface dans chaque paire dans la zone interne et une dans la zone externe. Les hôtes connectés au réseau du côté interne représentent vos ressources protégées.

Remarque Vous n'êtes pas tenu de regrouper toutes les interfaces internes (ou externes) dans une seule zone. Choisissez le regroupement qui est logique pour vos politiques de déploiement et de sécurité.

Configurez ensuite une règle de contrôle d'accès avec une condition de zone de destination définie à Internal. Cette règle simple fait correspondre le trafic qui quitte le périphérique à partir de n'importe quelle interface dans la zone interne. Pour inspecter le trafic correspondant à la recherche de prévention des intrusions et de

programmes malveillants, choisissez une action de règle **Allow**(autorisation) , puis associez la règle à une politique de prévention des intrusions et à une politique de fichier.

Comment contrôler l'utilisation des applications

Le Web est une plateforme désormais omniprésente pour la distribution des applications dans l'entreprise, qu'il s'agisse de plateformes d'applications basées sur un navigateur Web ou d'applications multimédias qui utilisent des protocoles Web pour l'entrée et la sortie des réseaux d'entreprise.

Défense contre les menaces inspecte les connexions pour déterminer l'application utilisée. Cela permet d'établir des règles de contrôle d'accès ciblées sur les applications, plutôt que de cibler des ports TCP/UDP spécifiques. Ainsi, vous pouvez bloquer ou autoriser sélectivement les applications Web même si elles utilisent le même port.

Bien que vous puissiez sélectionner des applications spécifiques à autoriser ou à bloquer, vous pouvez également rédiger des règles en fonction du type, de la catégorie, de l'étiquette, du risque ou de la pertinence de l'entreprise. Par exemple, vous pouvez créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est bloquée.

Cisco procède fréquemment à la mise à jour ou à l'ajout de détecteurs d'applications supplémentaires au moyen des mises à jour du système et de la base de données sur les vulnérabilités (VDB). Ainsi, une règle bloquant les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

Dans ce scénario, nous bloquerons toute application appartenant à la catégorie **anonymizer/proxy** (anonymiseur/serveur mandataire).

Procédure

Étape 1 Choisissez **Policies** > **Access Control** (Politiques > Contrôle d'accès) et modifiez la politique de contrôle d'accès.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle) et configurez la règle pour le contrôle des applications.

a) Donnez un nom significatif à la règle, par exemple Block_Anonymizers.

b) Sélectionnez **Block (Bloquer**) pour **Action**.

c) En supposant que vous avez configuré des zones et que vous souhaitez que cette règle s'applique au trafic passant de l'intérieur vers l'extérieur, sélectionnez l'onglet **Zones** (zones) et choisissez votre zone interne comme zone source et la zone externe comme zone de destination.

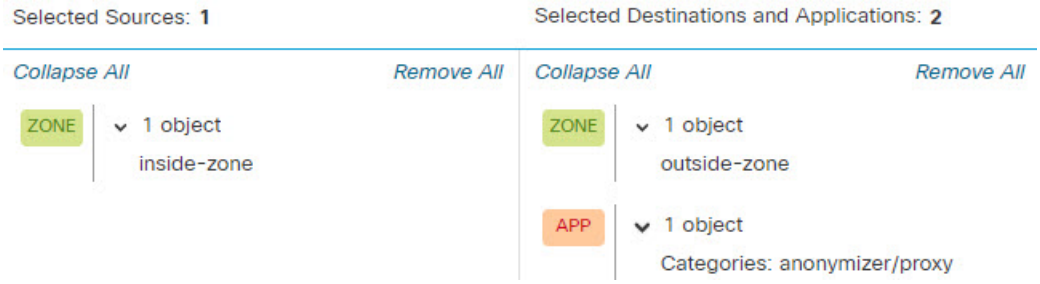
d) Cliquez sur l'onglet **Applications**, sélectionnez les applications à mettre en correspondance et cliquez sur **Add Application** (Ajouter une application).

Lorsque vous sélectionnez des critères, tels que la catégorie et le niveau de risque, la liste à droite des critères est mise à jour pour afficher exactement les applications correspondant aux critères. La règle que vous établissez s'applique à ces applications.

Examinez attentivement cette liste. Par exemple, vous pourriez être tenté de bloquer toutes les applications à très haut risque. Cependant, à ce jour, l'application TFPT est considérée comme à très haut risque. La plupart des entreprises ne veulent pas bloquer cette application. Prenez le temps d'expérimenter en adoptant

différents critères de filtrage pour voir quelles applications correspondent à vos sélections. Gardez à l'esprit que ces listes peuvent changer à chaque mise à jour de VDB.

Pour les besoins de cet exemple, sélectionnez les anonymiseurs et serveurs mandataires (anonymizers/proxies) dans la liste des catégories (Categories). Les critères de correspondance devraient maintenant ressembler au graphique suivant.



e) Cliquez sur **Logging** (Journalisation) à côté de l'action découlant de la règle et activez la journalisation au début de la connexion. Vous pouvez sélectionner un serveur Syslog si vous en utilisez un.

Vous devez activer la journalisation pour obtenir des informations sur les connexions bloquées par cette règle.

Étape 3 Déplacez la règle pour qu'elle vienne après les règles qui utilisent uniquement les critères de protocole et de port, mais qui n'autorisent pas le trafic qui devrait être bloqué par la règle d'application.

Les applications correspondantes nécessitent une inspection Snort. Comme l'inspection Snort n'est pas requise par les règles qui utilisent uniquement le protocole et le port, vous pouvez améliorer les performances du système en regroupant ces règles simples au sommet de la politique de contrôle d'accès, autant que possible.

Étape 4 Déployez les modifications.

Vous pouvez utiliser le nombre de règles d'application et les tableaux de bord d'analyse pour voir comment cette règle fonctionne et à quelle fréquence les utilisateurs essaient ces applications.

Comment bloquer les menaces

Vous pouvez mettre en œuvre le filtrage IPS (Intrusion Prevention System) de nouvelle génération en ajoutant des politiques de prévention des intrusions à vos règles de contrôle d'accès. Les politiques de prévention des intrusions analysent le trafic réseau et comparent le contenu du trafic aux menaces connues. Si une connexion correspond à une menace que vous surveillez, le système la coupe, empêchant ainsi l'attaque.

Tous les autres traitements de trafic ont lieu avant que le trafic réseau ne fasse l'objet d'un examen pour détecter les intrusions. En associant une politique de prévention des intrusions à une règle de contrôle d'accès, vous informez le système qu'avant que 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.

Vous pouvez configurer des politiques de prévention des intrusions uniquement sur des règles qui autorisent (**allow**) le trafic. Aucune inspection n'est effectuée sur les règles définies pour attribuer la confiance (**trust**) à un trafic ou le bloquer (**block**). En outre, vous pouvez configurer une politique de prévention des intrusions comme action par défaut si vous ne souhaitez pas utiliser un blocage simple.

En plus d'inspecter le trafic que vous autorisez afin de détecter d'éventuelles intrusions, vous pouvez utiliser la politique de renseignement de sécurité pour bloquer de manière préventive tout le trafic en provenance ou à destination d'adresses IP ou d'adresses URL connues comme mauvaises.

Cet exemple ajoute une politique de prévention des intrusions qui permet au réseau interne 192.168.1.0/24 d'accéder à l'extérieur, et suppose que vous possédez déjà des règles de blocage pour éliminer sélectivement les connexions indésirables, tout en ajoutant une politique de Security Intelligence pour effectuer un blocage préemptif.

Avant de commencer

Vous devez appliquer la licence IPS à tout périphérique géré qui utilise cette règle.

Cet exemple suppose que vous avez déjà créé des zones de sécurité pour les interfaces internes et externes, et l'objet réseau pour le réseau interne.

Procédure

Étape 1 Créez la règle de contrôle d'accès qui applique la politique de prévention des intrusions.

a) Lors de la modification de la politique de contrôle d'accès, cliquez sur **Add Rule** (ajouter une règle).

b) Donnez à la règle un nom pertinent, tel que Inside_Outside, et assurez-vous que l'action de règle est **Allow**(autorisation) .

c) Pour la politique de prévention des intrusions (**Intrusion Policy**), sélectionnez Balanced Security and Connectivity (Sécurité et connectivité équilibrées). Vous pouvez soit accepter l'ensemble de variables par défaut, soit sélectionner le vôtre si vous souhaitez le personnaliser.

La politique **Balanced Security and Connectivity**(sécurité et connectivité équilibrées) convient à la plupart des réseaux. Elle offre une bonne protection contre les intrusions sans être trop agressive, ce qui peut entraîner l'abandon d'un trafic que vous pourriez ne pas vouloir supprimer. Si vous déterminez que vous perdez trop de trafic, vous pouvez simplifier l'inspection en lien avec la prévention des intrusions en sélectionnant la politique **Connectivity over Security** (connectivité avant sécurité).

Si vous avez besoin de plus d'agressivité en matière de sécurité, essayez la politique **Security over Connectivity** (sécurité avant connectivité). La politique de détection maximale (**Maximum Detection**) accorde encore plus d'importance à la sécurité de l'infrastructure réseau, ce qui peut avoir un impact opérationnel encore plus important.

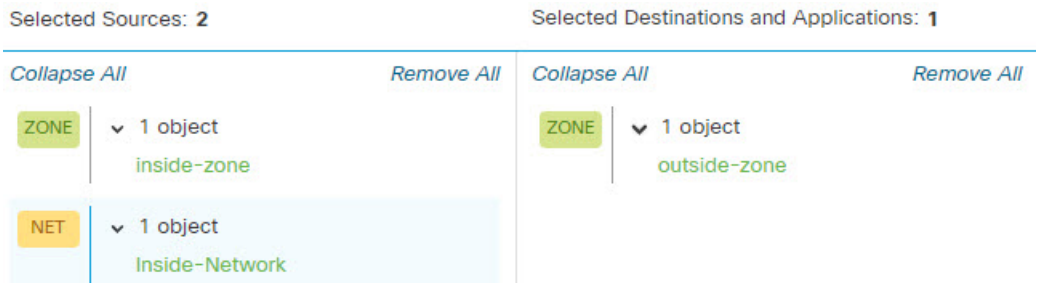
Si vous créez votre propre politique personnalisée, vous pouvez sélectionner celle-ci à la place.

Une discussion relatives aux ensembles de variables dépasse le cadre de cet exemple. Lisez les chapitres sur la politique de prévention des intrusions pour obtenir des informations détaillées sur les ensembles de variables et les politiques personnalisées.

d) Sélectionnez l'onglet **Zones** (zones) et ajoutez votre zone de sécurité interne aux critères de source et la zone externe aux critères de destination.

e) Sélectionnez l'onglet **Networks** (réseaux) et ajoutez l'objet réseau qui définit votre réseau interne aux critères de source.

Les critères de correspondance devraient ressembler à ce qui suit :



f) Cliquez sur **Logging** (journalisation) et activez la journalisation au début ou à la fin de la connexion, ou les deux, selon vos besoins.
g) Cliquez sur **Apply** (Appliquer) pour enregistrer la règle, puis sur **Save** (Enregistrer) pour enregistrer la politique mise à jour.
h) Déplacez la règle à l'emplacement approprié de la politique de contrôle d'accès.

Étape 2 Configurez la politique de renseignement de sécurité pour supprimer de manière préventive les connexions avec des sites et des hôtes connus comme mauvais.

En utilisant les renseignements de sécurité pour bloquer les connexions avec les hôtes ou les sites qui sont connus pour être des menaces, vous évitez à votre système le temps nécessaire pour effectuer une inspection approfondie des paquets afin de repérer les menaces dans chaque connexion. Les renseignements de sécurité permettent de bloquer rapidement le trafic indésirable, laissant plus de temps au système pour gérer le trafic important pour vous.

a) Lors de la modification de la politique de contrôle d'accès, cliquez sur le lien **Security Intelligence** (Renseignements sur la sécurité) dans le chemin de paquets.

   Le lien comprend deux politiques : la politique DNS en haut, et les renseignements sur la sécurité (réseau et URL) en bas. Dans cet exemple, nous configurons les listes de réseaux et d'URL. Par défaut, ces listes comprennent déjà les listes globales Bloquer et Ne pas bloquer, mais ces listes sont vides par défaut jusqu'à ce que vous y ajoutiez des éléments.

b) Après avoir sélectionné les **réseaux** et la zone de sécurité **Toute**, faites défiler la liste vers le bas jusqu'à ce que vous atteigniez les listes globales et la première catégorie de renseignements sur la sécurité (probablement Attaquants). Cliquez sur Attaquants, puis faites défiler la liste jusqu'à la fin des catégories (probablement Tor_exit_node) et appuyez sur Maj + Clic pour sélectionner toutes les catégories. Cliquez sur **Add to Block List** (Ajouter à la liste de blocage).
c) Sélectionnez l'onglet **URL**, puis la zone de sécurité **Any** (toutes les zones de sécurité), puis utilisez la touche Maj + clic pour sélectionner les versions d'URL des mêmes catégories. Cliquez sur **Add to Block List** (Ajouter à la liste de blocage).
d) Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.
e) Au besoin, vous pouvez ajouter des objets de réseau et d'URL aux listes de blocage ou Ne pas bloquer.

   Les listes **Do Not Block** ne sont pas vraiment des listes encadrant les autorisations. Ce sont plutôt des listes d'exceptions. Si une adresse ou une URL dans la liste d'exceptions apparaît également dans la liste des contacts bloqués, la connexion pour l'adresse ou l'URL est transmise à la politique de contrôle d'accès. De cette façon, vous pouvez bloquer un flux, mais si vous constatez plus tard qu'une adresse ou un site souhaitable est bloqué, vous pouvez utiliser la liste des exceptions pour remplacer ce blocage sans devoir supprimer complètement le flux. Gardez à l'esprit que ces connexions sont ensuite évaluées par le contrôle d'accès et, si elles sont configurées, par des politiques de prévention des intrusions. Ainsi, si des connexions

contiennent des menaces, elles peuvent être identifiées et bloquées lors d'une inspection de prévention des intrusions.

Utilisez les événements et les tableaux de bord pour déterminer quel trafic est réellement bloqué par la politique et si vous devez ajouter des adresses ou des URL aux listes **Ne pas bloquer**.

Étape 3 Déployez vos modifications.

Comment bloquer le trafic QUIC

Nous vous recommandons de bloquer le trafic QUIC en tant que bonne pratique. Le protocole QUIC est activé par défaut des navigateurs Chrome. Lorsque vous essayez d'accéder aux applications Google à l'aide du navigateur Chrome, une session vers un serveur Google est établie à l'aide du protocole QUIC au lieu de TLS/SSL. QUIC est un protocole pilote qui en est à ses débuts de développement. Il utilise des méthodes de chiffrement exclusives.

Le protocole HTTPS (Secure Hypertext Transfer Protocol) utilise le protocole TCP (Transmission Control Protocol), tout comme le protocole HTTP (Hypertext Transfer Protocol). Le protocole de contrôle de transmission est axé sur la connexion ou dynamique. HTTPS utilise le port TCP 443 et HTTP utilise le port TCP 80. HTTP/3 fonctionne sur la base du protocole QUIC. Pour QUIC, HTTP/3 repose sur le protocole UDP (User Datagram Protocol), et non sur TCP.

Le mode QUIC pourrait avoir un impact négatif sur la sécurité du réseau par inadvertance. Les périphériques de sécurité, comme les pare-feu et les capteurs de réseau, ne sont généralement pas en mesure d'accéder aux informations accessibles avec les sessions TCP existantes. Le trafic QUIC étant bloqué par le pare-feu, le navigateur Chrome utilise le protocole TLS/SSL traditionnel. Notez que cela n'entraîne aucune perte de fonctionnalité du navigateur. Firewall obtient une visibilité et un contrôle améliorés des applications Google avec ou sans le déchiffrement SSL. Le trafic QUIC n'est donc pas surveillé comme il devrait l'être et n'est pas acheminé vers les protections Web du pare-feu.

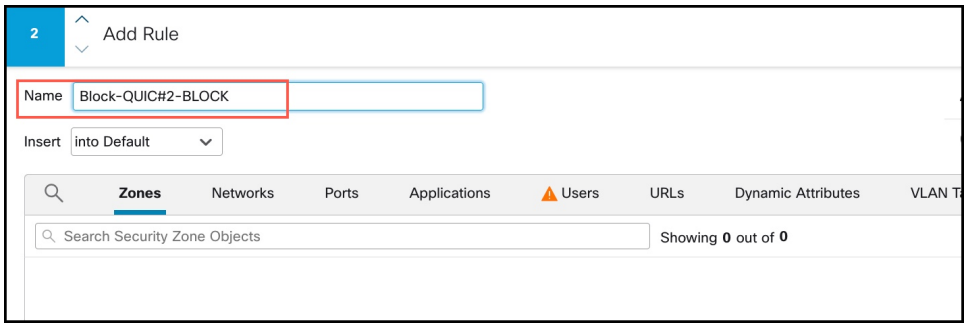
Dans ce scénario, nous montrons comment créer une règle de contrôle d'accès pour bloquer le trafic QUIC et HTTP/3.

Procédure

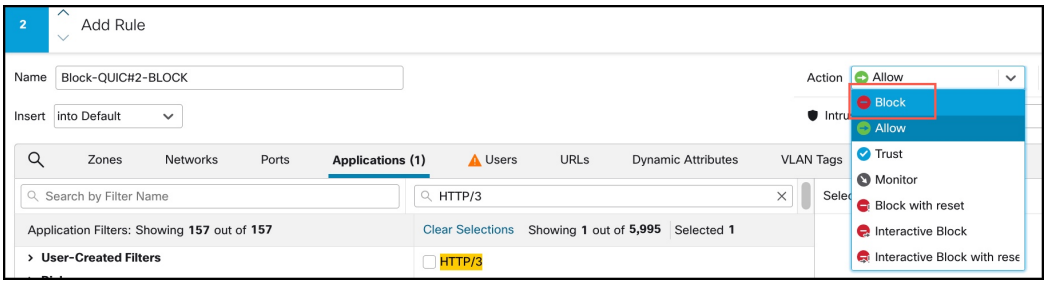
Étape 1 Choisissez **Policies** > **Access Control** (Politiques > Contrôle d'accès) et modifiez la politique de contrôle d'accès.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Saisissez un nom significatif pour la règle, tel que Block-QUIC.

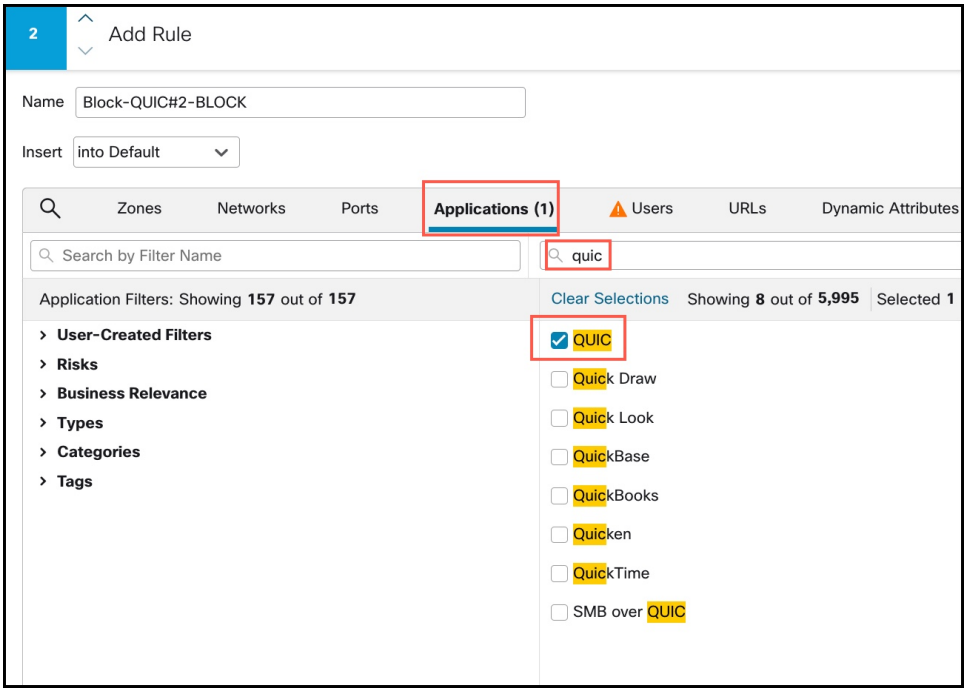


Étape 4 Dans la liste déroulante **Actions**, sélectionnez **Bloquer**.

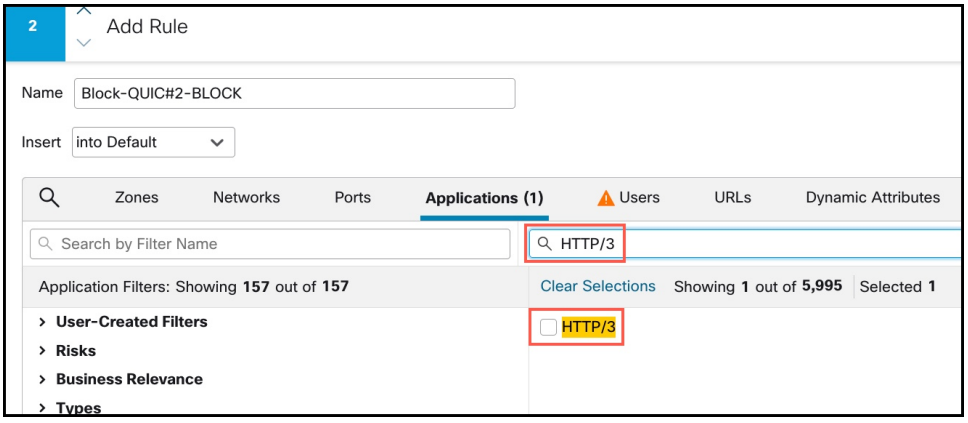


Étape 5 Cliquez sur l'onglet **Applications**.

Étape 6 Recherchez « quic » dans la zone de recherche et cochez la case de l'application QUIC.



Étape 7 Recherchez « HTTP/3 » dans la zone de recherche et cochez la case HTTP/3.



Étape 8 Cliquez sur **Add Application** (Ajouter une application) à ajouter aux Destinations et Applications.

Étape 9 Cliquez sur **Logging** (Journalisation) à côté de l'action découlant de la règle et activez la journalisation au début de la connexion. Vous devez activer la journalisation pour obtenir des informations sur les connexions bloquées par cette règle.

Étape 10 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle, puis sur **Save** (Enregistrer) pour enregistrer la politique mise à jour.

Étape 11 Déplacez la règle à l'emplacement approprié de la politique de contrôle d'accès.

Étape 12 Déployez vos modifications.

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.