Qualité de service

Les rubriques suivantes décrivent comment utiliser la fonctionnalité de qualité de service (QoS) pour contrôler le trafic réseau à l'aide de périphériques défense contre les menaces :

Introduction à QoS (Qualité de service)

La qualité de service, ou QoS, limite le débit (via des politiques) du trafic réseau autorisé ou approuvé par le contrôle d'accès. Le système n'évalue pas le trafic de limite de débit qui a été acheminé en mode fastpath.

Bien que la QoS ne soit prise en charge que sur les interfaces défense contre les menaces routées des périphériques, elle n'est pas prise en charge sur les interfaces VTI et VPN de site à site.

Journalisation des connexions au débit limité

Il n'y a aucune configuration de journalisation pour la QoS. Le débit d'une connexion peut être limité sans qu'elle soit enregistrée, et vous ne pouvez pas enregistrer une connexion simplement parce qu'elle était à débit limité. Pour afficher les informations sur la QoS dans les événements de connexion, vous devez consigner indépendamment les fins des connexions appropriées dans la base de données centre de gestion.

Les événements de connexion pour les connexions à débit limité contiennent des renseignements sur le volume de trafic abandonné et les configurations de QoS qui ont limité le trafic. Vous pouvez afficher ces informations dans des vues d'événements (flux de travail), des tableaux de bord et des rapports.

À propos des politiques QoS

Les politiques de QoS déployées sur les périphériques gérés régissent la limitation de débit. Chaque politique QoS peut cibler plusieurs périphériques; chaque périphérique ne peut avoir qu'une politique QoS déployée à la fois.

Le système fait correspondre le trafic aux règles de QoS dans l'ordre que vous spécifiez. Le débit du système limite le trafic en fonction de la première règle, où toutes les conditions de règle correspondent au trafic. Le trafic qui ne correspond à aucune des règles n'est pas limité en débit.

Remarque Le nombre total de règles, y compris les règles de QoS, sur le périphérique ne peut pas dépasser 255. Lorsque ce seuil est atteint, un message d'avertissement de déploiement s'affiche. Pour un déploiement réussi, vous devez réduire le nombre de règles.

Vous devez restreindre les règles de QoS par interface source ou destination (routage). Le système applique la limitation de débit *indépendamment* sur *chacune* de ces interfaces; vous ne pouvez pas spécifier de limite de débit agrégé pour un ensemble d'interfaces.

Les règles de QoS peuvent également évaluer le trafic aux limites en fonction d'autres caractéristiques du réseau, ainsi que des informations contextuelles telles que l'application, l'URL, l'identité de l'utilisateur et les balises de groupe de sécurité personnalisées (SGT).

Vous pouvez limiter le trafic de téléchargement et de téléversement indépendamment. Le système détermine les directions de téléchargement et de téléversement en fonction de l'initiateur de la connexion.

Remarque La QoS n'est pas subordonnée à une configuration de contrôle d'accès principale; vous configurez la QoS indépendamment. Cependant, les politiques de contrôle d'accès et de QoS déployées sur le même appareil partagent des configurations d'identité; voir Association d'autres politiques au contrôle d'accès.

Politiques de QoS et multidétention

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Les administrateurs des domaines ascendants peuvent déployer la même politique QoS sur les périphériques de domaines descendants différents. Les administrateurs de ces domaines descendants peuvent utiliser cette politique QoS en lecture seule déployée par les ancêtres ou la remplacer par une politique locale.

Exigences et prérequis de QoS

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur d'accès

Administrateur de réseau

Limitation de débit avec les politiques QoS

Pour appliquer une limitation de débit basée sur des politiques, configurez et déployez des politiques QoS sur les périphériques gérés. Chaque politique QoS peut cibler plusieurs périphériques; chaque périphérique ne peut avoir qu'une politique QoS déployée à la fois.

Une seule personne doit modifier une politique à la fois, en utilisant une seule fenêtre de navigateur. Si plusieurs utilisateurs enregistrent la même politique, les dernières modifications enregistrées sont conservées. Pour votre commodité, le système affiche des informations sur la personne qui (le cas échéant) modifie actuellement chaque politique. Pour protéger la confidentialité de votre session, un avertissement s'affiche après 30 minutes d'inactivité sur l'éditeur de politique. Après 60 minutes, le système annule vos modifications.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **QoS**.

Étape 2 Cliquer sur **New Policy** (Nouvelle politique) pour créer une nouvelle politique QoS et, éventuellement, affecter des périphériques cibles. voir Création d'une politique de qualité de service (QoS), à la page 4.

Vous pouvez également **Copier** ( ) ou **Edit** ( ) une politique existante.

Étape 3 Configurer les règles QoS; voir Configuration des règles QoS, à la page 5 et Conditions des règles QoS, à la page 7.

La fenêtre Rules (Règles) dans l'éditeur de politique QoS répertorie chaque règle dans l'ordre d'évaluation et affichent un résumé des conditions de règle et des configurations de limitations de débit. Un menu contextuel offre des options de gestion des règles, notamment le déplacement, l'activation et la désactivation.

Utile dans les déploiements plus importants, vous pouvez **filtrer par périphérique** pour afficher uniquement les règles qui affectent un appareil ou un groupe de périphériques spécifique. Vous pouvez également rechercher des règles et à l'intérieur de celles-ci ; le système fait correspondre le texte que vous saisissez dans le champ **Règles de recherche** aux noms des règles et aux valeurs des conditions, y compris les objets et les groupes d'objets.

Remarque Créer et ordonner correctement des règles est une tâche complexe, mais essentielle à la mise en place d'un déploiement efficace. Si vous n'effectuez pas une planification rigoureuse, les règles peuvent prévaloir sur d'autres règles, nécessiter des licences supplémentaires ou contenir des configurations non valides. Les icônes représentent des commentaires, des avertissements et des erreurs. Si des problèmes persistent, cliquez sur **Show Warnings** (Afficher les avertissements) pour afficher une liste. Pour en savoir plus, consultez Bonnes pratiques pour les règles de contrôle d'accès.

Étape 4 Cliquer sur **Policy Assignments** (Afficher les affectations) pour identifier les périphériques gérés ciblés par la politique. voir Définition des périphériques cibles pour une politique QoS, à la page 4.

Si vous avez identifié des périphériques cibles lors de la création de la politique, vérifiez vos choix.

Étape 5 Enregistrer la politique de qualité de service QoS.

Étape 6 Étant donné que cette fonctionnalité doit permettre le passage de certains paquets, vous devez configurer votre système pour examiner ces paquets. 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.

Étape 7 Déployer les changements de configuration.

Création d'une politique de qualité de service (QoS)

Une nouvelle politique de qualité de service QoS sans règle n'effectue aucune limitation de débit.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **QoS**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 4 (Facultatif) Choisissez les **périphériques disponibles** où vous souhaitez déployer la politique, puis cliquez sur **Add to Policy**(ajouter à la politique) ou effectuez un glisser-déposer sur les **périphériques sélectionnés**. Pour restreindre les périphériques qui s'affichent, saisissez une chaîne de recherche dans le champ **Search** (recherche).

Vous devez affecter des périphériques avant de déployer la politique.

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

Prochaine étape

- Configurer et déployer la politique QoS; voir Limitation de débit avec les politiques QoS, à la page 3.

Définition des périphériques cibles pour une politique QoS

Chaque politique QoS peut cibler plusieurs périphériques; chaque périphérique ne peut avoir qu'une politique QoS déployée à la fois.

Procédure

Étape 1 Dans l'éditeur de politique QoS, cliquez sur **Policy Affectations**(affectations de politiques).

Étape 2 Concevez votre liste de cibles :

- Add (ajouter) : choisissez un ou plusieurs **Available Devices** (périphériques disponible), puis cliquez sur **Add to Policy** (ajouter à la politique) ou faites un glisser-déposer vers la liste des **périphériques sélectionnés**.
- Supprimer : cliquez sur **Supprimer** ( ) à côté d'un seul périphérique, ou choisissez plusieurs périphériques, effectuez un clic droit, puis choisissez **Delete Selected**(Supprimer la sélection).
- Rechercher : saisissez une chaîne de recherche dans le champ de recherche. Cliquez sur **Effacer** ( ) pour effacer la recherche.

Étape 3 Cliquez sur **OK** pour enregistrer les affectations de politique.

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

Prochaine étape

- Déployer les changements de configuration.

Configuration des règles QoS

Lorsque vous créez ou modifiez une règle, utilisez la partie supérieure de l'éditeur de règles pour configurer les propriétés générales de la règle. Utilisez la partie inférieure de l'éditeur de règles pour configurer les conditions et les commentaires des règles.

Procédure

Étape 1 Dans l'éditeur de politique Règles de qualité de service :

- Add Rule (ajouter une règle) : Cliquez sur **Add Rule** (ajouter une règle).
- Edit Rule (modifier la règle) : cliquez sur **Edit** ( ).

Étape 2 Saisissez un **Nom**.

Étape 3 Configurez les composants de la règle.

- Enabled (activer) : spécifiez si la règle est activée (**Enabled)**.
- Apply QoS On (appliquer QoS à) : Choisissez les interfaces pour lesquelles vous souhaitez évaluer la limite, soit des **interfaces dans les objets d'interface de destination, soit des interfaces dans des objets** d'**interface source**. Votre choix doit correspondre à une contraintes d'interface remplies (et non à **des** contraintes).
- Traffic Limit Per Interface (Limites de trafic par interface) : saisissez une limite de **téléchargement** et une **limite de téléversement** en Mbit/s. La valeur par défaut **Illimité** empêche le trafic correspondant d'être limité dans cette direction.
- Conditions : cliquez sur la condition correspondante que vous souhaitez ajouter. Vous devez configurer une condition d'interface de source ou de destination correspondant à votre choix pour **Apply QoS On** (Appliquer la qualité de service (QoS)).
- Commentaires : cliquez sur **Commentaires**. Pour ajouter un commentaire, cliquez sur **Nouveau commentaire**, saisissez un commentaire, puis cliquez sur **OK**. Vous pouvez modifier ou supprimer ce commentaire jusqu'à ce que vous enregistriez la règle.

Pour des informations détaillées sur les composants des règles, voir Composants de la règle QoS, à la page 6.

Étape 4 Enregistrer la règle

Étape 5 Dans l'éditeur de politique, définissez la position de la règle. Cliquez dessus et faites-la glisser ou utilisez le menu contextuel pour la couper et la coller.

Les règles sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle qui correspond au trafic est la règle qui gère ce trafic. Un bon ordre des règles réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles.

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

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Bonnes pratiques pour les règles de contrôle d'accès

Composants de la règle QoS

State Enabled/Disabled (État Activé/Désactivé)

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.

Interfaces (appliquer la politique de qualité de service QoS)

Vous ne pouvez pas enregistrer une règle de QoS qui limite tout le trafic. Pour chaque règle QoS, vous devez appliquer la QoS aux :

- Interfaces dans les objets d'interface source : le débit limite le trafic dans les interfaces source de la règle. Si vous choisissez cette option, vous devez ajouter au moins une restriction d'interface source (ne peut pas être **toute**).
- Interfaces dans les objets d'interface de destination le débit limite le trafic dans les interfaces de destination de la règle. Si vous choisissez cette option, vous devez ajouter au moins une restriction d'interface de destination (ne peut pas être **toute**).

Limite de trafic par interface

Une règle QoS applique la limitation de débit *indépendamment* sur *chacune* des interfaces que vous spécifiez avec l'option Apply QoS On (Appliquer la QoS sur). Vous ne pouvez pas spécifier de limite de débit agrégé pour un ensemble d'interfaces.

Vous pouvez limiter le débit du trafic en Mbits par seconde. La valeur par défaut **Illimité** empêche le trafic correspondant d'être limité.

Vous pouvez limiter le trafic de téléchargement et de téléversement indépendamment. Le système détermine les directions de téléchargement et de téléversement en fonction de l'initiateur de la connexion.

Si vous spécifiez une limite supérieure au débit maximal d'une interface, le système n'évaluera pas la limite du trafic correspondant. Le débit maximal peut être affecté par la configuration matérielle d'une interface, que vous spécifiez dans les propriétés de chaque périphérique (**Devices (appareils)** > **Device Management (gestion des appareils)**).

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Vous pouvez configurer chaque règle avec plusieurs conditions. Le trafic doit correspondre à toutes les conditions pour respecter la règle. Chaque type de condition a son propre onglet dans l'éditeur de règles. Pour en savoir plus, consultez Conditions des règles QoS, à la page 7.

Commentaires

Chaque fois que vous enregistrez des modifications à une règle, vous pouvez ajouter des commentaires. 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.

Dans l'éditeur de politiques, le système affiche le nombre de commentaires d'une règle. Dans l'éditeur de règles, utilisez l'onglet Commentaires pour afficher les commentaires existants et en ajouter de nouveaux.

Conditions des règles QoS

Les conditions précisent le trafic spécifique géré par la règle. Vous pouvez configurer chaque règle avec plusieurs conditions. Le trafic doit correspondre à toutes les conditions pour respecter la règle. Chaque type de condition a son propre onglet dans l'éditeur de règles. Vous pouvez limiter le trafic à l'aide de :

Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Conditions des règles d'interface, à la page 7
Conditions des règles de réseau, à la page 7
Conditions des règles d'utilisateur, à la page 8
Conditions des règles d'application, à la page 8
Conditions de règle de port, à la page 10
Conditions de règle d'URL, à la page 11
Conditions de règle SGT personnalisée, à la page 12

Conditions des règles d'interface

Les conditions de règles d'interface contrôlent le trafic en fonction de ses interfaces de source et de destination.

Selon le type de règle et les périphériques de votre déploiement, vous pouvez utiliser des *objets d'interface* prédéfinis appelés *zones de sécurité* ou des *groupes d'interface* pour créer des conditions d'interface. Les objets d'interface segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques: consultez Interface.

Astuces Restreindre les règles par interface est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle exclut toutes les interfaces d'un périphérique, cette règle n'affecte pas les performances de ce périphérique.

Tout comme toutes les interfaces d'un objet d'interface doivent être du même type (en ligne, passive, commutée, routée ou ASA FirePOWER), tous les objets d'interface utilisés dans une condition d'interface doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas de trafic, dans les déploiements passifs, vous ne pouvez pas restreindre les règles par interface de destination.

Conditions des règles de réseau

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

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

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

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

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

Conditions 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.
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

Conditions de règle de port

Les conditions de port vous permettent de contrôler le trafic en fonction de ses ports source et de destination.

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

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.

Le filtrage des applications est également recommandé pour les applications, comme FTD, 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 source dans une seule règle de contrôle d'accès.

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 SGT personnalisée

Si vous ne configurez pas ISE/ISE-PIC comme source d'identité, vous pouvez contrôler le trafic à l'aide des balises de groupe de sécurité (SGT) qui n'ont **pas** été attribuées par ISE. Une balise de groupe de sécurité (SGT) spécifie les privilèges d'une source de trafic dans un réseau sécurisé.

Les conditions de règle SGT *personnalisées* utilisent des objets SGT créés manuellement pour filtrer le trafic, plutôt que les valeurs SGT ISE obtenues lors de la connexion du système à un serveur ISE. Ces objets SGT créés manuellement correspondent aux attributs SGT du trafic que vous souhaitez contrôler. Le contrôle du trafic à l'aide de balises SGT personnalisées n'est pas considéré comme un contrôle de l'utilisateur.

Conditions de règle ISE SGT ou règle SGT personnalisée

Certaines règles vous permettent de contrôler le trafic en fonction de la balise SGT attribuée. Selon le type de règle et la configuration de votre source d'identité, vous pouvez utiliser des groupes SGT affectés par ISE ou des groupes SGT personnalisés pour faire correspondre le trafic aux attributs SGT affectés.

Remarque Si vous utilisez les balises SGT de Cisco ISE pour mettre en correspondance le trafic, même si un attribut SGT n'est pas affecté à un paquet, le paquet correspond toujours à une règle SGT de l'ISE si la SGT associée à l'adresse IP source du paquet est connue dans ISE.

Type de condition	Nécessite	Segments SGT répertoriés dans l'éditeur de règles
SGT ISE	Source d'identité ISE	Fenêtres SGT obtenues en interrogeant le serveur ISE, avec des métadonnées automatiquement mises à jour
SGT personnalisé	Pas de source d'identité ISE/ISE-PIC.	Objets SGT statiques que vous créez

Transition automatique des règles SGT personnalisées aux règles ISE SGT

Si vous créez des règles qui correspondent aux règles SGT personnalisées, puis configurez ISE/ISE-PIC comme source d'identité, le système :

- Désactive les options de **balise de groupe de sécurité** dans le gestionnaire d'objets. Bien que le système conserve les objets SGT existants, vous ne pouvez pas les modifier ni en ajouter de nouveaux.
- Conserve les règles existantes avec des conditions SGT personnalisées. Cependant, ces règles ne correspondent pas au trafic. Vous ne pouvez pas non plus ajouter de critères SGT personnalisés aux règles existantes ni créer de nouvelles règles avec des conditions SGT personnalisées.

Si vous configurez ISE, Cisco vous recommande de supprimer ou de désactiver les règles existantes avec des conditions SGT personnalisées. Au lieu de cela, utilisez les conditions d'attribut ISE pour faire correspondre le trafic avec les attributs SGT.

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.