Contournement intelligent des applications

Les rubriques suivantes décrivent comment configurer les politiques de contrôle d'accès pour utiliser Intelligent Application Bypass (IAB)

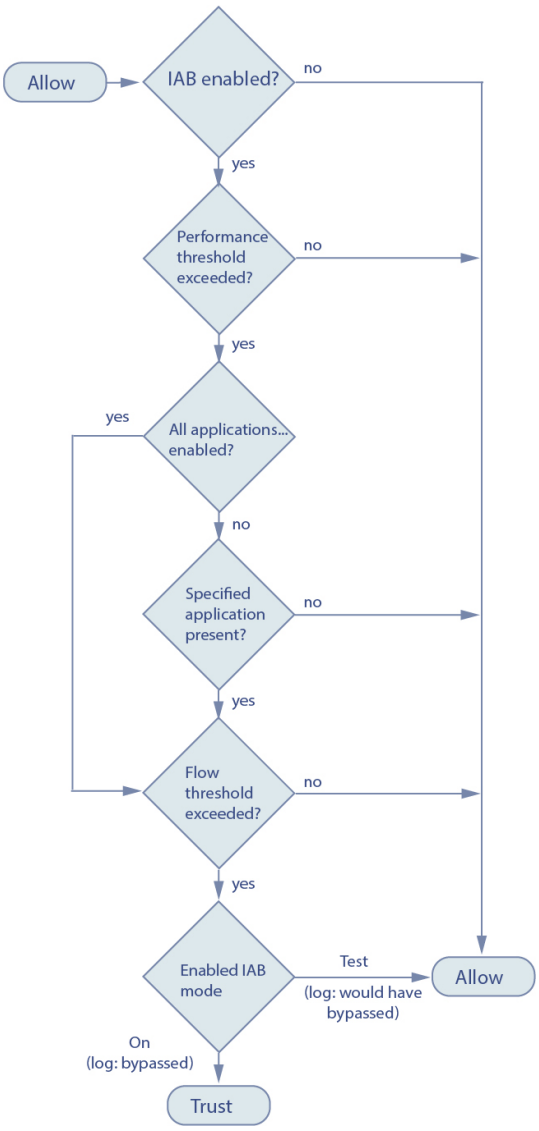
- Introduction au IAB (Contournement intelligent d'application), à la page 1
- Options IAB, à la page 2
- Exigences et conditions préalables pour le contournement intelligent des applications, à la page 4
- Configuration du contournement intelligent des applications, à la page 4
- Journalisation et analyse de l'IAB, à la page 5

Introduction au IAB (Contournement intelligent d'application)

L'IAB (Intelligent Application Bypass, contournement intelligent des aplications) identifie les applications suffisamment fiables pour traverser votre réseau sans autre inspection si les seuils de performance et de flux sont dépassés. Par exemple, si une sauvegarde quotidienne a un impact considérable sur les performances du système, vous pouvez configurer des seuils qui, s'ils sont dépassés, font confiance au trafic généré par votre application de sauvegarde. Vous pouvez également configurer l'IAB de sorte que, lorsqu'un seuil de performance d'inspection est dépassé, l'IAB fait confiance à tout le trafic qui dépasse un seuil de contournement de flux, quel que soit le type d'application.

Le système met en œuvre l'IAB sur le trafic autorisé par les règles de contrôle d'accès ou l'action par défaut de la politique de contrôle d'accès, avant que le trafic ne soit soumis à une inspection approfondie. Un mode de test vous permet de déterminer si des seuils sont dépassés et, le cas échéant, d'identifier les flux d'application qui auraient été contournés si vous aviez activé l'IAB (appelé *mode de contournement*).

Le graphique suivant illustre le processus décisionnel de l'IAB :



Options IAB

État

Active ou désactive l'IAB.

Intervalle de l'échantillon de la performance

Spécifie l'intervalle en secondes entre les analyses d'échantillonnage des performances de l'IAB, pendant lequel le système recueille les mesures de performance du système à des fins de comparaison avec les seuils de performance de l'IAB. La valeur **0** désactive l'IAB.

Applications et filtres contournables

Cette fonctionnalité offre deux options qui s'excluent mutuellement :

Applications/filtres
: Fournit un éditeur dans lequel vous pouvez définir des applications et des ensembles d'applications (filtres) pouvant être contournés. Consultez Conditions des règles d'application.

Toutes les applications, y compris les applications non identifiées
: Lorsqu'un seuil de performance d'inspection est dépassé, fait confiance à tout le trafic qui dépasse un seuil de contournement de flux, quel que soit le type d'application.

Performance et seuils de flux

Vous devez configurer au moins un seuil de performance d'inspection et un seuil de contournement de flux. Lorsqu'un seuil de performance est dépassé, le système examine les seuils de flux et, si un seuil est dépassé, il fait confiance au trafic spécifié. Si vous activez plusieurs de l'un ou l'autre, un seul de chaque doit être dépassé.

Les seuils de performance d'inspection fournissent des limites de performance d'inspection de prévention des intrusions qui, en cas de dépassement, déclenchent l'inspection des seuils de flux. L'IAB n'utilise pas les seuils de performance d'inspection définis à `0`. Vous pouvez configurer un ou plusieurs des seuils de performance d'inspection suivants :

Pourcentage d'abandon

Nombre moyen de paquets abandonnés en tant que pourcentage du total de paquets, lorsque des paquets sont abandonnés en raison de surcharges de performances causées par les règles de prévention des intrusions, les politiques de fichiers, la décompression onéreuses, etc. Cela ne fait pas référence aux paquets abandonnés par les configurations normales telles que les règles de prévention des intrusions. Notez que la spécification d'un entier supérieur à 1 active IAB lorsque le pourcentage de paquets spécifié est abandonné. Lorsque vous spécifiez `1`, tout pourcentage compris entre 0 et 1 active l'IAB. Cela permet à un petit nombre de paquets d'activer IAB.

Pourcentage d'utilisation du processeur

Pourcentage moyen de ressources de processeur utilisées.

Latence des paquets

Latence des paquets (microsecondes)

Débit du flux

Vitesse à laquelle le système traite les flux, mesurée en nombre de flux par seconde. Notez que cette option configure l'IAB pour mesurer le *débit*, pas le *nombre* de flux.

Les seuils de contournement de flux fournissent des limites de flux qui, si elles sont dépassées, amènent l'IAB à faire confiance au trafic d'application contournable en mode de contournement ou qui permettent au trafic d'application d'être soumis à une inspection plus approfondie en mode de test. L'IAB n'utilise pas les seuils de contournement de flux définis à `0`. Vous pouvez configurer un ou plusieurs des seuils de contournement de flux suivants :

Octets par flux

Le nombre maximal de kilo-octets qu'un flux peut inclure.

Paquets par flux

Le nombre maximal de paquets qu'un flux peut inclure.

Durée du flux

Le nombre maximal de secondes pendant lesquelles un flux peut rester ouvert.

Vélocité du flux

Le débit de transfert maximal en kilo-octets par seconde.

Exigences et conditions préalables pour le contournement intelligent des applications

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configuration du contournement intelligent des applications

⚠

Mise en garde Tous les déploiements n'exigent pas un IAB, et ceux qui en dépendent pourraient l'utiliser de manière limitée. N'activez pas IAB, sauf si vous avez une connaissance approfondie de votre trafic réseau, en particulier du trafic des applications, et des performances du système, y compris les causes des problèmes de performance anticipés. Avant d'exécuter IAB en mode de contournement, assurez-vous que l'approbation du trafic spécifié ne vous expose pas à un risque.

Avant de commencer

Pour les périphériques classiques, vous devez avoir la licence de contrôle.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced Settings** (paramètres avancés) de la flèche déroulante **More** (Plus) à la fin de la ligne de flux de paquets. Puis cliquez sur **Edit** (✎) à côté de **Paramètres de contournement intelligent des applications**.

Étape 2 Configurer les options IAB :

- **State (état)** : permet de **désactiver** ou **d**'activer l'IAB ou de l'activer en mode **test**.
- **Performance Sample Interval** (Intervalle d'échantillonnage de performance) : Saisissez l'intervalle en secondes entre les analyses d'échantillonnage des performances d'IAB. Si vous activez IAB, même en mode de test, saisissez une valeur non nulle. La valeur `0` désactive IAB.
- **Applications et filtres contournables** : choisissez parmi les possibilités suivantes :
  - Cliquez sur le nombre d'applications et de filtres contournés et spécifiez les applications dont vous souhaitez contourner le trafic. voir Configuration des conditions d'application et des filtres.
  - Cliquez sur **Toutes les applications, y compris les applications non identifiées,** afin que, lorsqu'un seuil de performance d'inspection est dépassé, IAB fasse confiance à tout le trafic qui dépasse un seuil de contournement de flux, quel que soit le type d'application.
- **Inspection Performance Thresholds** (Seuils de performance de l'inspection) : Cliquez sur **Configure** (configurer) et saisissez au moins une valeur de seuil.
- **Flow Bypass Thresholds**(seuils de contournement de flux) : Cliquez sur **Configure** (configurer) et saisissez au moins une valeur de seuil.

Vous devez préciser au moins un seuil de performance d'inspection et un seuil de contournement de flux. les deux doivent être dépassés pour que IAB fasse confiance au trafic. Si vous saisissez plus d'un seuil de chaque type, un seul seuil de chaque type doit être dépassé. Pour de plus amples renseignements, voir Options IAB, à la page 2.

Étape 3 Cliquez sur **OK** pour enregistrer les paramètres IAB.

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

Prochaine étape

- Étant donné que certains paquets doivent être autorisés à passer avant qu'une application puisse être détectée, vous devez configurer votre système pour qu'il examine 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.

- Déployer les changements de configuration.

Journalisation et analyse de l'IAB

L'IAB force un événement de fin de connexion qui consigne les flux contournés et les flux qui auraient été contournés, que vous ayez ou non activé la journalisation de la connexion. Les événements de connexion indiquent des flux qui sont contournés en mode de contournement ou qui auraient été contournés en mode de test. Les gadgets du tableau de bord et les rapports personnalisés en fonction des événements de connexion peuvent afficher des statistiques à long terme sur les flux contournés et qui auraient été contournés.

Événements de connexion IAB

Action

Lorsque **Reason** (Motif) inclut `Intelligent App Bypass` (Contournement intelligent des applications) :

`Allow` -

indique que la configuration IAB appliquée était en mode test et que le trafic pour l'application spécifiée par le **protocole d'application** reste disponible pour l'inspection.

`Trust` -

indique que la configuration IAB appliquée était en mode de contournement et que le trafic pour l'application spécifiée par le **protocole d'application** est autorisé à traverser le réseau sans autre inspection.

Motif

`Intelligent App Bypass` indique que l'IAB a déclenché l'événement en mode de contournement ou de test.

Protocole d'application

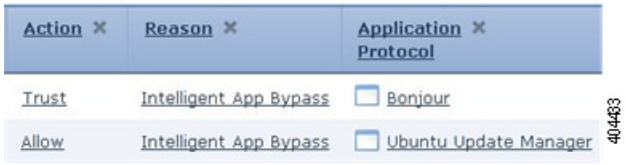
Ce champ affiche le protocole d'application qui a déclenché l'événement.

Exemple

Dans le graphique tronqué suivant, certains champs sont omis. Le graphique montre les champs **Action**, **Reason** et **Application Protocol** pour deux événements de connexion résultant de paramètres IAB différents dans deux politiques de contrôle d'accès distinctes.

Pour le premier événement, l'action `Trust` (confiance) indique qu'IAB a été activé en mode de contournement et que le trafic du protocole Bonjour a été autorisé à passer sans autre inspection.

Pour le deuxième événement, l'action `Allow` (autorisation) indique qu'IAB a été activé en mode de test, donc le trafic d'Ubuntu Update Manager a été soumis à une inspection plus approfondie, mais aurait été contourné si IAB avait été en mode de contournement.



Exemple

Dans le graphique tronqué suivant, certains champs sont omis. Le flux du deuxième événement a été à la fois contourné (**Action** : `Trust`; **Reason** : `Intelligent App Bypass`) et inspecté par une règle de prévention des intrusions (**Reason** : `Intrusion Monitor`). La raison du `moniteur de prévention des intrusions` indique qu'une règle de prévention des intrusions définie sur **Générer des événements** a détecté un exploit pendant la connexion mais n'a pas bloqué ce dernier. Dans l'exemple, cela s'est produit avant que l'application ne soit détectée. Une fois l'application détectée, l'IAB a reconnu l'application comme contournable et a approuvé le flux.

Gadgets du tableau de bord IAB personnalisée

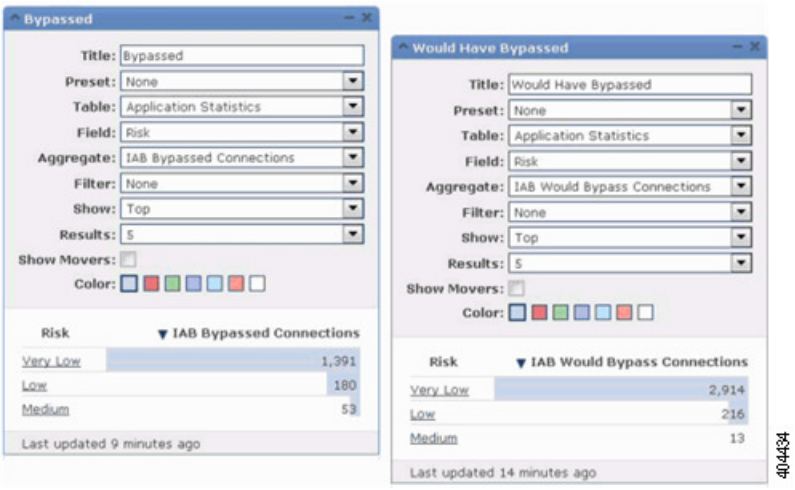
Vous pouvez créer un gadget de tableau de bord d'analyse personnalisée pour afficher les statistiques à long terme de l'IAB en fonction des événements de connexion. Précisez les éléments suivants lors de la création du gadget :

- **Prédéfini** : `aucun`
- **Table** : `Statistiques sur les applications`
- **Champ** : n'importe lequel
- **Agrégat** : l'un ou l'autre :
  - `Connexions de contournement d'IAB`
  - `IAB contournerait les connexions`
- **Filtre** : n'importe lequel

Exemples

Dans les exemples de gadgets de tableau de bord d'analyse personnalisée suivants :

- L'exemple *Bypassed* montre les statistiques du trafic d'applications contourné, car les applications ont été définies comme contournables et IAB a été activé comme mode de contournement dans la politique de contrôle d'accès déployée.
- L'exemple *aurait été contourné* présente les statistiques du trafic d'application qui aurait été contourné, car les applications ont été définies comme contournables et qu'IAB a été activé en mode de test dans la politique de contrôle d'accès déployée. .



Rapports personnalisés IAB

Vous pouvez créer un rapport personnalisé pour afficher les statistiques à long terme IAB en fonction des événements de connexion. Spécifiez les éléments suivants lors de la création du rapport :

- **Table** : `Statistiques sur les applications`

- **Prédéfini** : `aucun`
- **Filtre** : n'importe lequel
- **Axe X** : n'importe lequel
- **AXE Y** : l'un ou l'autre :
  - `Connexions de contournement d'IAB`
  - `IAB contournerait les connexions`

Exemples

Le graphique suivant montre deux exemples de rapports abrégés :

- L'exemple *Bypassed* montre les statistiques du trafic d'applications contourné, car les applications ont été définies comme contournables et IAB a été activé comme mode de contournement dans la politique de contrôle d'accès déployée.
- L'exemple *aurait été contourné* présente les statistiques du trafic d'application qui aurait été contourné, car les applications ont été définies comme contournables et qu'IAB a été activé en mode de test dans la politique de contrôle d'accès déployée.

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.