Profils adaptatifs

Les rubriques suivantes décrivent comment configurer des profils adaptatifs :

À propos des profils adaptatifs

Les profils adaptatifs doivent être activés pour :

- Effectuer un contrôle des applications et des fichiers, y compris la protection contre les programmes malveillants (AMP), et permettre aux règles de prévention des intrusions d'utiliser les métadonnées de service.

Mise en garde Le profilage adaptatif **doit** être activé (son état par défaut) comme décrit dans Configuration des profils adaptatifs, à la page 4 pour que les règles de contrôle d'accès effectuent le contrôle des applications et des fichiers, y compris la protection contre les programmes malveillants (AMP), et pour que les règles de prévention des intrusions utilisent les métadonnées de service.

- Pour les déploiements passifs, activez les mises à jour de profils adaptatifs pour défragmenter et réassembler le trafic IP en fonction des systèmes d'exploitation des hôtes de destination.

Remarque Dans un déploiement en ligne, Cisco vous recommande d'activer le mode en ligne et de configurer le préprocesseur de normalisation en ligne avec l'option **Normalize TCP Payload** (normaliser la charge utile TCP) activée.

Licences requises pour les profils adaptatifs

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les profils adaptatifs

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Mises à jour des profils adaptatifs

En règle générale, le système utilise les paramètres statiques de votre politique d'analyse de réseau pour prétraiter et analyser le trafic. Avec Mises à niveau des profils adaptatifs, le système peut adapter le comportement de traitement en utilisant les informations sur l'hôte détectées par la découverte du réseau ou importées par un tiers.

Mises à niveau des profils, à l'instar des profils basés sur la cible que vous pouvez configurer manuellement dans une politique d'analyse de réseau, participent à la défragmentation des paquets IP et au réassemblage des flux de la même manière que le système d'exploitation sur l'hôte cible. Le moteur de règles de prévention des intrusions analyse ensuite les données dans le même format que celui utilisé par l'hôte de destination.

Les profils basés sur la cible configurés manuellement appliquent soit le profil de système d'exploitation par défaut que vous sélectionnez, soit des profils que vous liez à des hôtes spécifiques. Mises à niveau des profils, cependant, permet de passer au profil de système d'exploitation approprié en fonction du système d'exploitation dans le profil d'hôte de l'hôte cible.

Voici un scénario dans lequel vous configurez Mises à niveau des profils pour le sous-réseau 10.6.0.0/16 et définissez la politique basée sur la cible de défragmentation IP par défaut sur Linux. Le centre de gestion dans lequel vous configurez les paramètres comporte une cartographie du réseau qui inclut le sous-réseau 10.6.0.0/16.

- Lorsque le système détecte du trafic de l'hôte A, qui ne se trouve pas dans le sous-réseau 10.6.0.0/16, il utilise la politique Linux basée sur la cible pour réassembler les fragments IP.
- Lorsque le système détecte du trafic de l'hôte B, qui se trouve dans le sous-réseau 10.6.0.0/16, il récupère les données du système d'exploitation de l'hôte B dans la cartographie du réseau. Le système utilise un profil basé sur ce système d'exploitation pour défragmenter le trafic destiné à l'hôte B.

Mises à jour des profils d'utilisateurs adaptatifs et règles recommandées par Cisco

La fonctionnalité Mises à niveau des profils adaptatifs est un paramètre avancé d'une politique de contrôle d'accès qui s'applique globalement à toutes les politiques de prévention des intrusions appelées par cette politique de contrôle d'accès. La fonctionnalité de règles recommandées par Cisco s'applique à la politique de prévention des intrusions individuelle pour laquelle vous la configurez.

Comme les règles recommandées par Cisco, Mises à niveau des profils compare les métadonnées d'une règle aux informations sur l'hôte pour déterminer si une règle doit s'appliquer à un hôte particulier. Cependant, alors que les règles recommandées par Cisco fournissent des recommandations pour activer ou désactiver les règles qui utilisent ces informations, Mises à niveau des profils utilise les informations pour appliquer des règles spécifiques à un trafic spécifique.

Les règles recommandées par Cisco nécessitent votre intervention pour mettre en œuvre les modifications suggérées aux états des règles. Mises à niveau des profils, en revanche, ne modifient pas les politiques de prévention des intrusions. Le traitement des règles basé sur les mises à jour de profils s'effectue paquet par paquet.

De plus, les règles recommandées par Cisco peuvent entraîner la désactivation de règles. Mises à niveau des profils, en revanche, n'affecte que l'application des règles qui sont déjà activées dans les politiques de prévention des intrusions. Mises à niveau des profils ne modifie jamais l'état de la règle.

Vous pouvez utiliser les Mises à niveau des profils et les règles recommandées par Cisco . Les Mises à niveau des profils utilisent l'état d'une règle lorsque votre politique de prévention des intrusions est déployée pour déterminer s'il faut l'inclure comme candidat à l'application, et vos choix d'accepter ou de refuser les recommandations sont reflétés dans l'état de la règle. Vous pouvez utiliser les deux fonctionnalités pour vous assurer que vous avez activé ou désactivé les règles les plus appropriées pour chaque réseau que vous surveillez, puis pour appliquer les règles activées le plus efficacement possible à un trafic spécifique.

Sujets connexes

À propos des règles recommandées par Cisco

Options de profils adaptatifs

Activer

L'activation de cette option est requise pour :

- les règles de contrôle d'accès pour contrôler les applications et les fichiers, y compris la protection contre les programmes malveillants (AMP)
- les règles de prévention des intrusions pour utiliser les métadonnées de service

Par défaut, cette option est activée.

Remarque Pour activer les profils adaptatifs dans Snort 3, les options **Enable** (activer) et **Enable Profile Updates** (activer les mises à jour de profils) doivent être sélectionnées.

Activer les mises à jour des profils

Dans les déploiements passifs, activez les mises à jour de profils pour défragmenter et réassembler le trafic IP en fonction du profil du système d'exploitation utilisé par les hôtes dans la cartographie de votre réseau.

Pour Snort 3, cette option doit être activée si les profils adaptatifs sont activés.

Profils adaptatifs - Intervalle des mises à jour des attributs

Lorsque les mises à jour de profils sont activées, vous contrôler la fréquence en minutes à laquelle les données de la cartographie du réseau sont synchronisées, du centre de gestion avec ses périphériques gérés. Le système utilise les données pour déterminer les profils à utiliser lors du traitement du trafic. L'augmentation de la valeur de cette option peut améliorer les performances dans un réseau de grande taille.

Profils adaptatifs - Réseaux

Lorsque les mises à jour de profils sont activées, vous pouvez également améliorer les performances en contraignant Mises à niveau des profils à une liste d'adresses IP, de blocs d'adresses et de variables réseau séparées par des virgules. Si vous utilisez une variable de réseau, le système utilise la valeur de la variable dans l'ensemble de variables lié à la politique de prévention des intrusions par défaut pour votre politique de contrôle d'accès. Par exemple, vous pouvez entrer : **`192.168.1.101, 192.168.4.0/24, $HOME_NET`**. IPv4 et IPv6 sont pris en charge.

La valeur par défaut (**`0.0.0.0/0`**) applique les mises à jour de profil adaptatifs à tous les réseaux.

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. Si vous activez et appliquez Mises à niveau des profils dans une politique antécédente, Cisco vous recommande de conserver la contrainte de réseau par défaut de **`0.0.0.0/0`**, ou d'utiliser une variable de réseau avec une valeur `quelconque`. Ce paramètre applique Mises à niveau des profils à tous les hôtes surveillés dans tous les sous-domaines.

Sujets connexes

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

Configuration des profils adaptatifs

Dans un déploiement passif, Cisco vous recommande de configurer Mises à niveau des profils adaptatifs. Dans un déploiement en ligne, configurez le préprocesseur de normalisation en ligne avec l'option **Normalize TCP Payload** (Normaliser la charge utile TCP) activée.

Mise en garde Le profilage adaptatif **doit** être activé (son état par défaut) comme décrit dans cette procédure pour que les règles de contrôle d'accès effectuent le contrôle des applications ou des fichiers, y compris AMP, et pour que les règles de prévention des intrusions utilisent les métadonnées de service.

Avant de commencer

La politique de contrôle d'accès doit avoir une politique de découverte de réseau activée pour la découverte d'un hôte ou d'un service, sinon les données de l'hôte doivent être importées à partir d'une source tierce.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Edit** (✎) au niveau de la politique que vous souhaitez modifier.

Étape 2 Cliquez sur **More** > **Advanced Settings**(autres paramètres avancés), puis sur **Edit** (✎) à côté de la section des **paramètres d'amélioration de la détection**.

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Définissez les options de profil adaptatif comme décrit dans Options de profils adaptatifs, à la page 3.

Étape 4 Cliquez sur **OK**.

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

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Le préprocesseur de normalisation en ligne
Scénarios de redémarrage de Snort

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.