Intrusion Prevention System Device Manager 5.1 - Ajuster la signature

Contenu

Introduction

Le Système de prévention d'intrusion (IPS) 5.1 contient plus de 1000 signatures par défaut de fonction intégrée. Vous ne pouvez pas renommer ou supprimer des signatures de la liste de signatures intégrées, mais vous pouvez retirer des signatures pour les retirer de l'engine de détection. Vous pouvez plus tard lancer les signatures retirées. Cependant, ce processus exige des engines de détection de reconstruire leur configuration, qui prend du temps et pourrait retarder le traitement du trafic. Vous pouvez accorder les signatures intégrées quand vous ajustez plusieurs paramètres de signature. Des signatures intégrées qui ont été modifiées s'appellent les *signatures accordées*.

Ce document montre les étapes pour l'utiliser afin d'accorder la signature utilisant le gestionnaire de périphériques IPS (IDM). IDM est un basé sur le WEB, l'application Java qui te permet de configurer et gérer votre capteur. Le web server pour IDM réside sur le capteur. Vous pouvez l'accéder à par des navigateurs Web d'Internet Explorer, de Netscape, ou de Mozilla.

Remarque: Vous pouvez créer les signatures, qui s'appellent les *signatures faites sur commande*. Les id faits sur commande de signature commencent à 60000. Vous pouvez les configurer pour plusieurs choses, telles qu'apparier des chaînes sur des connexions d'UDP, le cheminement des inondations de réseau, et les balayages. Chaque signature est créée utilisant une engine de signature spécifiquement conçue pour le type de trafic qui est surveillé.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le gestionnaire de périphériques 5.x de Système de protection contre les intrusions Cisco.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Afin de configurer un capteur pour surveiller le trafic réseau pour une signature particulière, vous devez activer la signature. Par défaut, les signatures les plus essentielles sont activées quand vous installez la mise à jour de signature. Quand on détecte une attaque qui apparie une signature activée, le capteur génère une alerte, qui est enregistrée dans la mémoire de l'événement du capteur. Les alertes, aussi bien que d'autres événements, peuvent être récupérés de la mémoire d'événement par les clients basés sur le WEB. Par défaut, le capteur se connecte toutes les alertes informationnelles ou le plus élevé.

Quelques signatures ont des sous-titre-signatures. C'est-à-dire, la signature est divisée en sous-catégories. Quand vous configurez une sous-titre-signature, les modifications apportées aux paramètres d'une sous-titre-signature s'appliquent seulement à cette sous-titre-signature. Par exemple, si vous éditez la sous-titre-signature 1 de la signature 3050 et changez la sévérité, la modification de sévérité s'applique seulement à la sous-titre-signature 1 et pas à 3050 2, 3050 3, et 3050 4.

Signatures d'optimisation

A + icône indique que plus d'options sont disponibles pour ce paramètre. Cliquez sur **+** icône pour développer la section et pour visualiser les paramètres restants.

Une icône verte indique que le paramètre utilise actuellement la valeur par défaut. Cliquez sur l'icône verte pour la changer au rouge, qui lance le champ de paramètre ainsi vous pouvez éditer la valeur.

Procédure pas à pas

Terminez-vous ces étapes afin d'accorder des signatures :

1. Ouvrez une session à IDM utilisant un compte avec des privilèges d'administrateur ou d'opérateur.
2. Choisissez la **configuration > la définition de signature > la configuration de signature**.Le volet de configuration de signature apparaît.

3. Afin de localiser une signature, choisissez une option la triant du **choisi par la** liste.Par exemple, si vous recherchez une signature d'inondation d'UDP, choisissez les **inondations L2/L3/L4 Protocol** et puis d'**UDP**.Le volet de configuration de signature régénère et affiche seulement ces signatures qui apparient vos critères les triant.
4. Afin d'accorder une signature existante, sélectionnez la signature et terminez-vous ces étapes :Cliquez sur Edit pour ouvrir la boîte de dialogue de signature d'éditer.Passez en revue les valeurs de paramètre et changez la valeur de n'importe quel paramètre que vous voulez accorder.**Remarque:** Afin de choisir plus d'une action d'événement, maintenez la **touche Ctrl**.Sous l'état, choisissez **oui** d'activer la signature.**Remarque:** La signature doit être activée pour que le capteur détecte activement l'attaque spécifiée par la signature.Sous l'état, spécifiez si cette signature est retirée. Cliquez sur **non** pour lancer la signature. Ceci place la signature dans l'engine.**Remarque:** Une signature doit être lancée pour que le capteur détecte activement l'attaque spécifiée par la signature.**Remarque:** Cliquez sur l'**annulation** afin d'annuler vos modifications et fermer la boîte de dialogue de signature d'éditer.Cliquez sur **OK**.La signature éditée apparaît maintenant dans la liste avec le positionnement de type à accorder.**Remarque:** Si vous voulez annuler vos modifications, cliquez sur la **remise**.
5. Cliquez sur Apply pour appliquer vos modifications et pour sauvegarder la configuration révisée.

Informations connexes

- Système de protection contre les intrusions Cisco
- Support et documentation techniques - Cisco Systems