Alertes externes pour les incidents d'intrusion

Les rubriques suivantes décrivent comment configurer les alertes externes pour les incidents d'intrusion :

À propos des alertes externes pour les incidents d'intrusion

Les notifications externes d'incidents d'intrusion peuvent faciliter la surveillance des systèmes essentiels :

- SNMP : configuré selon la politique de prévention des intrusions et envoyé à partir de périphériques gérés. Vous pouvez activer les alertes SNMP par règle de prévention des intrusions.
- Syslog : configuré selon la politique de prévention des intrusions et envoyé à partir de périphériques gérés Lorsque vous activez les alertes du journal système dans une politique de prévention des intrusions, vous l'activez pour chaque règle de la politique.
- Courriel : configuré dans toutes les politiques de prévention des intrusions et envoyé à partir de Cisco Secure Firewall Management Center. Vous pouvez activer les alertes par courriel par règle de prévention des intrusions, ainsi que limiter leur durée et leur fréquence.

Gardez à l'esprit que si vous avez configuré la suppression ou le seuillage des incidents d'intrusion, le système pourrait ne pas générer d'incidents d'intrusion (et donc ne pas envoyer d'alertes) à chaque fois qu'une règle se déclenche.

Dans un déploiement multidomaine, vous pouvez configurer les alertes externes dans n'importe quel domaine. Dans les domaines ascendants, le système génère des notifications pour les incidents d'intrusion dans les domaines descendants.

Remarque Cisco Secure Firewall Management Center utilise également SNMP, syslog et *des réponses aux alertes* par courriel pour envoyer différents types d'alertes externes. voir Réponses aux alertes Cisco Secure Firewall Management Center. Le système n'utilise **pas** les réponses aux alertes pour envoyer des alertes en fonction d'incidents d'intrusion individuels.

Sujets connexes

Filtres de notification d'incident d'intrusion dans une politique d'intrusion

Exigences de licence pour les alertes externes des incidents d'intrusion

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables aux alertes externes des incidents d'intrusion

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Configuration des alertes SNMP pour les incidents d'intrusion

Après avoir activé les alertes SNMP externes dans une politique de prévention des intrusions, vous pouvez configurer des règles individuelles pour envoyer des alertes SNMP lorsqu'elles se déclenchent. Ces alertes sont envoyées à partir du périphérique géré.

Procédure

Étape 1 Dans le volet de navigation de l'éditeur de politique de prévention des intrusions, cliquez sur **Advanced Settings** (Paramètres avancés).

Étape 2 Assurez-vous que **les alertes SNMP** sont **activées**, puis cliquez sur **Edit** (modifier).

Un message au bas de la page identifie la couche de politique de prévention des intrusions qui contient la configuration.

Étape 3 Choisissez une **version SNMP**, puis spécifiez les options de configuration comme décrit dans Options d'alerte de prévention des intrusions SNMP, à la page 3.

Étape 4 Dans le volet de navigation, cliquez sur **Règles**.

Étape 5 Dans le volet des règles, choisissez les règles selon lesquelles vous souhaitez définir les alertes SNMP, puis choisissez **Alerting** > **Add SNMP Alert** (Mise en place des alertes > Ajouter une alerte SNMP).

Étape 6 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, sélectionnez **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Options d'alerte de prévention des intrusions SNMP

Si votre système de gestion de réseau nécessite un fichier de base (MIB) de gestion informationnelle, vous pouvez l'obtenir à partir du Cisco Secure Firewall Management Center à l'adresse `/etc/sf/DCEALERT.MIB`.

Options SNMP v2

Option	Description
Type de trappe	Le type de déroutement à utiliser pour les adresses IP qui apparaissent dans les alertes. Si votre système de gestion de réseau restitue correctement le type d'adresse INET_IPV4, sélectionnez-le **comme binaire**. Sinon, choisissez-le **comme chaîne de caractères**. Par exemple, HP OpenView requiert **en tant que Chaîne**.
Pot de miel	Le serveur qui recevra les notifications de déroutement de SNMP. Vous pouvez spécifier une seule adresse IP ou un seul nom d'hôte.
Community String (chaîne pour désigner la communauté)	Nom de la communauté

Options SNMP v3

Les périphériques gérés encodent les alertes SNMPv3 avec une valeur d'ID de moteur. Pour décoder les alertes, votre serveur SNMP a besoin de cette valeur, qui est la version hexadécimale de l'adresse IP de l'interface de gestion du périphérique expéditeur, à laquelle est ajouté « 01 ».

Par exemple, si le périphérique qui envoie l'alerte SNMP a une adresse IP d'interface de gestion 172.16.1.50, la valeur de l'ID du moteur est 0xAC10013201.

Option	Description
Type de trappe	Le type de déroutement à utiliser pour les adresses IP qui apparaissent dans les alertes. Si votre système de gestion de réseau restitue correctement le type d'adresse INET_IPV4, sélectionnez-le **comme binaire**. Sinon, choisissez-le **comme chaîne de caractères**. Par exemple, HP OpenView requiert **en tant que Chaîne**.
Pot de miel	Le serveur qui recevra les notifications de déroutement de SNMP. Vous pouvez spécifier une seule adresse IP ou un seul nom d'hôte.
Mot de passe d'authentification	Le mot de passe requis pour l'authentification. SNMPv3 utilise la fonction de hachage de Message Digest 5 (MD5) ou la fonction de hachage Secure Hash Algorithm (SHA) pour chiffrer ce mot de passe, selon la configuration. Si vous spécifiez un mot de passe d'authentification, l'authentification est activée.
Mot de passe privé	La clé SNMP pour la confidentialité. SNMPv3 utilise le chiffrement par bloc Data Encryption Standard (DES) pour chiffrer ce mot de passe. Lorsque vous saisissez un mot de passe pour le protocole SNMP v3, il s'affiche en texte brut lors de la configuration initiale, mais il est enregistré sous forme chiffrée. Si vous spécifiez un mot de passe privé, la confidentialité est activée et vous devez également spécifier un mot de passe d'authentification.
Nom d'utilisateur	Votre nom d'utilisateur SNMP

Configuration des alertes Syslog pour les incidents d'intrusion

Après avoir activé les alertes du journal système dans une politique de prévention des intrusions, le système envoie tous les incidents d'intrusion au journal système, soit sur le périphérique géré lui-même, soit à un ou plusieurs hôtes externes. Si vous spécifiez un hôte externe, des alertes syslog sont envoyées à partir du périphérique géré.

Procédure

Étape 1 Dans le volet de navigation de l'éditeur de politique de prévention des intrusions, cliquez sur **Advanced Settings** (Paramètres avancés).

Étape 2 Assurez-vous que **les alertes du journal système** sont **activées**, puis cliquez sur **Edit** (modifier).
Un message au bas de la page identifie la couche de politique de prévention des intrusions qui contient la configuration. La page **Syslog Alerting** (Alertes Syslog) est ajoutée sous **Advanced Settings** (Paramètres avancés).

Étape 3 Saisissez les adresses IP des **hôtes de journalisation** auxquels vous souhaitez envoyer des alertes syslog.

Si vous laissez le champ **Logging Hosts** (Hôtes de journalisation) vide, les détails des hôtes de journalisation sont tirés de la section Journalisation de la politique de contrôle d'accès associée.

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.

Étape 4 Choisissez les niveaux d'**Installation** et de **gravité**de comme décrit dans Installations et gravités pour les alertes de prévention des intrusions Syslog, à la page 5.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, sélectionnez **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Installations et gravités pour les alertes de prévention des intrusions Syslog

Les périphériques gérés peuvent envoyer des incidents d'intrusion sous forme d'alertes syslog en utilisant une fonction particulière et un niveau de **gravité**, afin que l'hôte de journalisation puisse classer les alertes. La *fonction* précise le sous-système qui l'a générée. Ces valeurs de facilité et de **gravité** ne s'affichent pas dans les messages du journal système.

Choisissez des valeurs qui ont du sens en fonction de votre environnement. Les fichiers de configuration locaux (comme syslog.conf sur les hôtes de journalisation UNIX) peuvent indiquer quelles installations sont enregistrées dans quels fichiers journaux.

Fonctions d'alertes Syslog

Facility (ressource)	Description
AUTH	Un message associé à la sécurité et à l'autorisation.
AUTHPRIV	Un message d'accès restreint associé à la sécurité et à l'autorisation. Sur de nombreux systèmes, ces messages sont transférés vers un fichier sécurisé.
CONSOLE	Un message d'alerte.
CRON	Un message généré par le daemon clock.
DÉMON	Un message généré par un daemon du système.
FTP	Un message généré par le daemon FTP.
KERN	Un message généré par le noyau. Sur de nombreux systèmes, ces messages sont imprimés sur la console lorsqu'ils s'affichent.
LOCAL0-LOCAL7	Un message généré par un processus interne.
LPR	Un message généré par le sous-système d'impression.
MESSAGERIE	Message généré par un système de messagerie.

Facility (ressource)	Description
ACTUALITÉS	Un message généré par le sous-système de nouvelles du réseau.
JOURNAL SYSTÈME	Un message généré par le daemon syslog.
Webex	Un message généré par un processus au niveau utilisateur.
UUCP	Un message généré par le sous-système UUCP.

Gravité des alertes Syslog

Niveau	Description
EMERG	Un état d'urgence diffusé à tous les utilisateurs
ALERTE	Une condition qui doit être corrigée immédiatement
CRIT	Une condition critique.
ERR	Une condition d'erreur
AVERTISSEMENT	Des message d'avertissement.
AVIS	Des conditions qui ne sont pas des conditions d'erreur, mais nécessitent votre attention
INFO	Des messages informatifs.
DÉBOGAGE	Des messages contenant des informations de débogage

Configuration des alertes par courriel pour les incidents d'intrusion

Si vous activez les alertes par courriel en cas de prévention des intrusions, le système peut envoyer un courriel lorsqu'il génère un incident d'intrusion, quel que soit le périphérique géré ou la politique de prévention des intrusions qui a détecté l'intrusion. Ces alertes sont envoyées à partir de Cisco Secure Firewall Management Center.

Avant de commencer

- Assurez-vous que Cisco Secure Firewall Management Center peut effectuer la résolution inversée comme propre adresse IP.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Cliquez sur **Intrusion Email** (Courriel d'intrusion).

Étape 3 Choisissez les options d'alerte, y compris les règles ou les groupes de règles de prévention des intrusions pour lesquels vous souhaitez envoyer des alertes, comme décrit dans Options d'alerte de prévention des intrusions par courriel, à la page 7.

Étape 4 Cliquez sur **Save** (enregistrer).

Options d'alerte de prévention des intrusions par courriel

Marche/Arrêt

Active ou désactive les alertes par courriel de prévention des intrusions.

Remarque Son activation activera les alertes pour toutes les règles, sauf si des règles individuelles sont sélectionnées.

Adresses de provenance et de destination

L'expéditeur et les destinataires du courriel. Vous pouvez spécifier une liste de destinataires séparés par des virgules.

Maximum et fréquence des alertes

Le nombre maximal d'alertes par courriel (**Max Alerts**) que Cisco Secure Firewall Management Center enverra par intervalle de temps (**Fréquence**).

Alertes de fusion

Réduit le nombre d'alertes envoyées en regroupant les alertes qui ont la même adresse IP source et le même ID de règle.

Résultats sommaires

Active de brèves alertes, convenant aux périphériques à texte limité. Les alertes brèves contiennent :

- Horodatage
- Protocole
- Adresses IP et ports de la source et de la destination
- Message
- Le nombre d'incidents d'intrusion générés pour la même adresse IP source

Par exemple : `. (116:108)`

Si vous activez la **sortie du résumé**, pensez à activer également la **fusion des alertes**. Vous pouvez également réduire le **nombre maximum d'alertes** pour éviter de dépasser les limites de messages texte.

Fuseau horaire

Fuseau horaire pour les horodatages des alertes.

Alertes par courriel concernant la configuration de règles spécifiques

Vous permet de choisir les règles selon lesquelles vous souhaitez définir des alertes par courriel.

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.