Protection contre les programmes malveillants de réseau et politiques relatives aux fichiers

Les rubriques suivantes fournissent une présentation du contrôle de fichier, des politiques de fichiers, des règles de fichier, de la protection avancée contre les programmes malveillants (AMP), des connexions au nuage et des connexions d'analyse dynamique.

À propos de la protection contre les programmes malveillants de réseau et des politiques de fichiers

Pour détecter et bloquer les programmes malveillants, utilisez les politiques de fichiers. Vous pouvez également utiliser les politiques de fichiers pour détecter et contrôler le trafic par type de fichier.

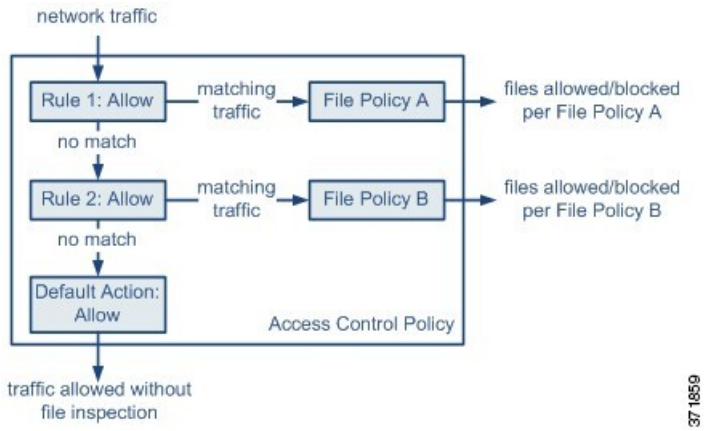
Advanced Malware Protection (AMP) pour Firepower peut détecter, capturer, suivre, analyser, consigner et éventuellement bloquer la transmission de programmes malveillants dans le trafic réseau. Dans l'interface Web Cisco Secure Firewall Management Center, cette fonctionnalité est appelée *Défense contre les programmes malveillants* , anciennement *AMP pour Firepower*. La protection avancée contre les programmes malveillants identifie les programmes malveillants à l'aide de périphériques gérés déployés en ligne et des données sur les menaces du nuage de Cisco.

Vous associez les politiques de fichiers à des règles de contrôle d'accès qui gèrent le trafic réseau dans le cadre de votre configuration globale de contrôle d'accès.

Lorsque le système détecte un programme malveillant sur votre réseau, il génère des événements liés aux fichiers et aux programmes malveillants. Pour analyser les données d'événements liés aux fichiers et aux programmes malveillants, consultez le chapitre *Événements liés aux fichiers et aux programmes malveillants et trajectoire des fichiers sur le réseau* dans Guide d'administration Cisco Secure Firewall Management Center .

Politique de fichiers

Une politique de fichiers est un ensemble de configurations que le système utilise pour assurer la protection contre les programmes malveillants et le contrôle des fichiers, dans le cadre de votre configuration globale de contrôle d'accès. Cette association fait en sorte qu'avant que le système passe un fichier dans le trafic correspondant aux conditions de la règle de contrôle d'accès, le fichier est d'abord inspecté. Examinez le diagramme suivant d'une politique de contrôle d'accès simple dans un déploiement en ligne.



La politique a deux règles de contrôle d'accès, qui utilisent l'action Allow (autoriser) et sont associées aux politiques de fichier. L'action par défaut de la politique consiste également à autoriser le trafic, mais sans inspection par la politique de fichiers. Dans ce scénario, le trafic est géré comme suit :

- Le trafic qui correspond à `la règle 1` est inspecté par `la politique de fichiers A`.
- Le trafic qui ne correspond pas à `la règle 1` est évalué en fonction de `la règle 2`. Le trafic qui correspond à `la règle 2` est inspecté par `la politique de fichiers B`.
- Le trafic qui ne correspond à aucune des règles est autorisé; vous ne pouvez pas associer de politique de fichiers à l'action par défaut.

En associant différentes politiques de fichiers à différentes règles de contrôle d'accès, vous avez un contrôle précis sur la façon dont vous identifiez et bloquez les fichiers transmis sur votre réseau.

Exigences et conditions préalables pour les politiques relatives aux fichiers

Prise en charge des modèles

N’importe lequel

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Administrateur d’accès

Exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants

Pour faire ceci	Licence requise	Action découlant d’une règle sur un fichier
Bloquer ou autoriser tous les fichiers d’un type particulier (par exemple, bloquer tous les fichiers .exe)	IPS (pour les périphériques défense contre les menaces) Protection (pour les périphériques classiques)	Autoriser, bloquer, bloquer avec réinitialisation
Autoriser ou bloquer sélectivement des fichiers en fonction du fait qu'ils contiennent ou sont susceptibles de contenir des programmes malveillants.	IPS (pour les périphériques défense contre les menaces) Protection (pour les périphériques classiques) Défense contre les programmes malveillants	Recherche dans le nuage de programmes malveillants, blocage des programmes malveillants

Pour faire ceci	Licence requise	Action découlant d'une règle sur un fichier
Stocker les fichiers	IPS (pour les périphériques défense contre les menaces) Protection (pour les périphériques classiques) Défense contre les programmes malveillants	Toute action de règle de fichier avec l'option **Store files** (Stocker les fichiers) sélectionnée

Pour en savoir plus sur les licences Défense contre les programmes malveillants, consultez :

- *Licences Malware Defense* dans Guide d'administration Cisco Secure Firewall Management Center

Bonnes pratiques pour les politiques de fichiers et la détection des programmes malveillants

En plus des éléments décrits ci-dessous, suivez les étapes dans Configurer la protection contre les programmes malveillants, à la page 7 et les rubriques référencées.

Bonnes pratiques en matière de règles de fichier

Tenez compte des consignes et limites suivantes lors de la configuration des règles de fichier :

- Une règle configurée pour bloquer des fichiers dans un déploiement passif ne bloque pas les fichiers correspondants. Puisque la connexion continue de transmettre le fichier, si vous configurez la règle pour consigner le début de la connexion, vous pouvez voir plusieurs événements journalisés pour cette connexion.
- Une politique peut inclure plusieurs règles. Lorsque vous créez les règles, vérifiez qu'aucune règle n'est « obscurcie » par une règle précédente.
- Les types de fichiers pris en charge pour l'analyse dynamique constituent un sous-ensemble des types de fichiers pris en charge pour d'autres types d'analyse. Pour afficher les types de fichiers pris en charge pour chaque type d'analyse, accédez à la page de configuration des règles de fichier, sélectionnez l'action **Block Malware** (Bloquer les programmes malveillants), puis cochez les cases qui vous intéressent.

  Pour vous assurer que le système examine tous les types de fichiers, créez des règles distinctes (dans la même politique) pour l'analyse dynamique et pour les autres types d'analyse.
- Si une règle de fichier est configurée avec une action **Rechercher** ou **Bloquer** les programmes malveillants dans le nuage et que centre de gestion ne peut pas établir la connectivité avec le nuage AMP, le système ne peut effectuer aucune option d'action basée sur une règle configurée tant que la connectivité n'est pas restaurée.
- Cisco vous recommande d'activer la **réinitialisation de la connexion** pour les actions **Bloquer les fichiers** et **Bloquer les programmes malveillants** afin d'éviter que les sessions d'application bloquées

restent ouvertes jusqu'à ce que la connexion TCP soit réinitialisée. Si vous ne réinitialisez pas les connexions, la session client restera ouverte jusqu'à ce que la connexion TCP se réinitialise.

- Si vous surveillez des volumes élevés de trafic, ne stockez **pas** tous les fichiers capturés ou ne soumettez pas tous les fichiers capturés pour une analyse dynamique. Cela peut avoir un impact négatif sur les performances du système.
- Vous ne pouvez pas effectuer d'analyse des programmes malveillants sur tous les types de fichiers détectés par le système. Après avoir sélectionné des valeurs dans les listes déroulantes **Application Protocol** (Protocole applicatif), **Direction of Transfer** (Direction du transfert) et **Action**, le système restreint la liste des types de fichiers.

Bonnes pratiques pour la détection de fichiers

Tenez compte des remarques et limitations suivantes concernant la détection de fichier :

- Si le profilage adaptatif n'est pas activé, les règles de contrôle d'accès ne peuvent pas effectuer de contrôle de fichier, y compris AMP.
- Si une règle et une condition de protocole d'application correspondent à un fichier, la génération d'événements de fichier se produit une fois que le système a réussi à identifier le protocole d'application d'un fichier. Les fichiers non identifiés ne génèrent pas d'événements de fichier.
- FTP transfère les commandes et les données sur différents canaux. Dans un déploiement en mode TAP passif ou en ligne, le trafic d'une session de données FTP et de sa session de contrôle peut ne pas être équilibré vers la même ressource interne.
- Si le nombre total d'octets pour tous les noms de fichiers dans une session POP3, POP, SMTP ou IMAP dépasse 1024, les événements de fichiers de la session peuvent ne pas refléter les noms de fichiers exacts pour les fichiers qui ont été détectés après le remplissage de la mémoire tampon de noms de fichiers.
- Lors de la transmission de fichiers texte par SMTP, certains clients de messagerie convertissent les retours à la ligne au caractère standard de retour à la ligne CRLF. Étant donné que les hôtes basés sur Mac utilisent le caractère de retour à la ligne (CR) et que les hôtes basés sur Unix/Linux utilisent le caractère de saut de ligne (LF), la conversion de nouvelle ligne par le client de messagerie peut modifier la taille du fichier. Notez que certains clients de messagerie utilisent par défaut la conversion de retour à la ligne lorsqu'ils traitent un type de fichier non reconnaissable.
- Pour détecter les fichiers ISO, définissez l'option « Limit the number of bytes inspected when doing file type detection » (Limiter le nombre d'octets inspectés lors de la découverte du type de fichier) à une valeur supérieure à 36870, comme décrit dans Options de rendement et de stockage pour l'inspection des fichiers et des logiciels malveillants, à la page 34.
- Les fichiers .exe contenus dans certaines archives .rar ne peuvent pas être détectés, y compris peut-être rar5.

Bonnes pratiques en matière de blocage de fichiers

Tenez compte des remarques et limitations suivantes concernant le blocage de fichiers :

- Si un marqueur de fin de fichier n'est pas détecté pour un fichier, quel que soit le protocole de transfert, le fichier ne sera pas bloqué par une règle **Block Malware** (Bloquer les programmes malveillants) ou la liste de détection personnalisée. Le système attend pour bloquer le fichier jusqu'à ce que le fichier entier

ait été reçu, comme indiqué par le marqueur de fin de fichier, et bloque le fichier après la détection du marqueur.

- Si le marqueur de fin de fichier pour un transfert de fichier FTP est transmis séparément du segment de données final, le marqueur sera bloqué et le client FTP indiquera que le transfert de fichier a échoué, mais le fichier sera en fait complètement transféré sur le disque.
- Les règles de fichiers avec les actions **Bloquer les fichiers** et **Bloquer les programmes malveillants** bloquent la reprise automatique du téléchargement de fichiers via HTTP en bloquant les nouvelles sessions avec le même fichier, l'URL, le serveur et l'application client détectés pendant 24 heures après la tentative initiale de transfert de fichiers.
- Dans de rares cas, si le trafic d'une session de téléchargement HTTP est en panne, le système ne peut pas rassembler le trafic correctement et, par conséquent, ne le bloquera pas ou ne générera pas d'événement de fichier.
- Si vous transférez un fichier sur NetBIOS-ssn (comme un transfert de fichier SMB) qui est bloqué par une règle de **blocage de fichiers**, vous pourriez voir un fichier sur l'hôte de destination. Cependant, le fichier est in utilisable, car il est bloqué après le début du téléchargement, ce qui entraîne un transfert de fichier incomplet.
- Si vous créez des règles de fichiers pour détecter ou bloquer les fichiers transférés sur NetBIOS-ssn (comme un transfert de fichier SMB), le système n'inspecte pas les transferts de fichiers en cours. Cependant, le système inspecte les nouveaux fichiers transférés après le déploiement d'une politique de contrôle d'accès en appelant la politique de fichiers.
- SMB possède une fonctionnalité appelée multicanal qui crée plusieurs sessions parallèles avec la même adresse IP et des ports différents. Pour une transaction donnée sur plusieurs canaux, le téléchargement de fichier est multiplexé sur ces sessions qui ne sont pas inspectés par le système en tant que fichier unique.
- Les fichiers transférés simultanément au cours d'une seule session TCP ou SMB ne sont pas inspectés.
- Dans un environnement de grappe, si une session SMB existante est déplacée vers un nouveau périphérique en raison d'un changement de rôle dans la grappe ou d'une défaillance d'appareil, les fichiers de tout transfert de fichiers en cours peuvent ne pas être inspectés.
- Certains transferts de fichiers SMB entre systèmes Microsoft Windows utilisent une fenêtre TCP très élevée pour les transferts de fichiers rapides. Pour détecter ou bloquer de tels transferts de fichiers, il est recommandé d'augmenter la valeur du nombre **maximal d'octets en file d'attente** et du **nombre maximal de segments en file d'attente** dans **Options de dépannage** > **Politique d'analyse de réseau** > **TCP Stream**.
- Si vous configurez la haute disponibilité de Firepower Threat Defense et que le basculement se produit pendant que le périphérique actif d'origine identifie le fichier, le type de fichier n'est pas synchronisé. Même si votre politique de fichiers bloque ce type de fichier, le nouveau périphérique actif télécharge le fichier.

Bonnes pratiques en matière de politique de fichiers

Notez les consignes générales et restrictions suivantes lors de la configuration des politiques de fichiers.

- Vous pouvez associer une politique de fichier unique à une règle de contrôle d'accès dont l'action est **Autoriser**, **Blocage interactif ou Blocage interactif avec réinitialisation**.

- Vous **ne pouvez pas** utiliser une politique de fichier pour inspecter le trafic géré par l'action de contrôle d'accès par défaut.
- Dans le cas d'une nouvelle politique, l'interface Web indique que la politique n'est pas utilisée. Si vous modifiez une politique de fichier en cours d'utilisation, l'interface Web vous indique combien de politiques de contrôle d'accès utilisent la politique de fichiers. Dans les deux cas, vous pouvez cliquer sur le texte pour passer à la page Access Control Policies (politiques de contrôle d'accès).
- Pour que le blocage de fichiers fonctionne, la Politique d'analyse de réseau (NAP) que vous appliquez à la politique de contrôle d'accès doit fonctionner en mode de protection, également appelé mode en ligne.
- Selon votre configuration, vous pouvez inspecter un fichier la première fois que le système le détecte et attendre un résultat de recherche dans le nuage, ou transmettre le fichier lors de cette première détection sans attendre le résultat de la recherche dans le nuage.
- Par défaut, l'inspection des fichiers des charges utiles chiffrées est désactivée. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès pour laquelle l'inspection de fichiers est configurée.

Attention Le préprocesseur d'inspection de fichiers avec les ID de générateur (GID) suivants est activé par défaut pour la politique sur les fichiers et les programmes malveillants : GID : 146 et GID : 147.

Configurer la protection contre les programmes malveillants

Cette rubrique résume les étapes à suivre pour configurer votre système de manière à protéger votre réseau contre les programmes malveillants.

Procédure

Étape 1 Planifier et préparer la protection contre les logiciels malveillants, à la page 8

Étape 2 Configurer les politiques relatives aux fichiers, à la page 9

Étape 3 Ajouter des politiques de fichiers à votre configuration de contrôle d'accès, à la page 9

Étape 4 Configurez les politiques de découverte de réseau pour associer les événements liés aux fichiers et aux programmes malveillants aux hôtes de votre réseau.

(N'activez pas simplement la découverte de réseau, vous devez la configurer pour découvrir les hôtes sur votre réseau afin de créer une cartographie du réseau de votre entreprise.)

Consultez Politiques de découverte du réseau et les sous-sections.

Étape 5 Déployer des politiques sur les périphériques gérés.

Consultez Déployer les modifications de configuration.

Étape 6 Testez votre système pour vous assurer qu'il traite les fichiers malveillants comme vous le souhaitez.

Étape 7 Configurer la maintenance et la surveillance de la protection contre les programmes malveillants, à la page 11

Prochaine étape

- (Facultatif) Pour améliorer encore la détection des programmes malveillants dans votre réseau, déployez et intégrez le produit AMP pour les points terminaux de Cisco. Consultez (Facultatif) Protection contre les programmes malveillants avec AMP pour les points terminaux, à la page 37 et les sous-sections.

Planifier et préparer la protection contre les logiciels malveillants

Cette procédure est la première série d'étapes du processus complet de configuration de votre système pour fournir une protection contre les programmes malveillants.

Procédure

Étape 1 Achetez et installez les licences.

Consultez les sections *Licences* Exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants, à la page 3 et dans Guide d'administration Cisco Secure Firewall Management Center.

Étape 2 Découvrez comment les politiques de fichiers et la protection contre les programmes malveillants s'intègrent dans votre plan de contrôle d'accès.

Voir le chapitre Aperçu du contrôle d'accès.

Étape 3 Comprendre les outils d'analyse de fichiers et de protection contre les programmes malveillants.

Consultez Actions de la règle de fichier, à la page 23 et les sous-sections.

Consultez également Options avancées et options d'inspection de fichier d'archive, à la page 17.

Étape 4 Déterminez si vous utiliserez des nuages publics ou privés (sur site) pour la protection contre les programmes malveillants (analyse de fichiers et analyse dynamique).

Consultez Connexions en nuage pour la protection contre les programmes malveillants, à la page 12 et les sous-sections.

Étape 5 Si vous utilisez des nuages privés (sur site) pour la protection contre les programmes malveillants : Achetez, déployez et testez ces produits.

Pour de plus amples renseignements, communiquez avec votre responsable de compte Cisco local ou avec votre revendeur agréé Cisco.

Étape 6 Configurez votre pare-feu pour autoriser les communications avec les nuages de votre choix.

Consultez les rubriques *Sécurité, accès à l'internet et ports de communication* du Guide d'administration Cisco Secure Firewall Management Center.

Étape 7 Configurez les connexions entre Firepower et les nuages de protection contre les programmes malveillants (publics ou privés, selon les besoins).

Prochaine étape

Passez à l'étape suivante du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 7.

Configurer les politiques relatives aux fichiers

Avant de commencer

Effectuez les tâches jusqu'à ce stade du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 7.

Procédure

Étape 1 Passez en revue la politique de fichiers et les restrictions liées aux règles de fichier.

Consultez Bonnes pratiques pour les politiques de fichiers et la détection des programmes malveillants , à la page 4 et les sous-sections.

Étape 2 Créer une politique de gestion des fichiers

Consultez Créer ou modifier une politique de fichiers, à la page 16.

Étape 3 Créez des règles dans votre politique de fichiers.

Consultez Règles de fichier, à la page 21 et les sous-sections.

Étape 4 Configurer les options avancées.

Consultez Options avancées et options d'inspection de fichier d'archive, à la page 17.

Prochaine étape

Passez à l'étape suivante du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 7.

Ajouter des politiques de fichiers à votre configuration de contrôle d'accès

Une politique de contrôle d'accès peut avoir plusieurs règles de contrôle d'accès associées aux politiques de fichiers. Vous pouvez configurer l'inspection de fichiers pour n'importe quelle règle de contrôle d'accès Allow (autorisation) ou Interactive Block (blocage interactif), ce qui vous permet de faire correspondre différents profils d'inspection de fichiers et de programmes malveillants avec différents types de trafic sur votre réseau avant qu'ils n'atteignent sa destination finale.

Avant de commencer

Effectuez les tâches jusqu'à ce stade du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 7.

Procédure

Étape 1 Consulter les directives relatives aux politiques de fichiers dans les politiques de contrôle d'accès. (Elles sont différentes de la règle de fichier et des directives de politique de fichier que vous avez examinées précédemment.)

Passer en revue Ordre d'inspection de fichier et d'intrusion.

Étape 2 Associer la politique de fichier à une politique de contrôle d'accès.

Voir la section Configuration d'une règle de contrôle d'accès pour la protection contre les programmes malveillants, à la page 10.

Étape 3 Attribuez la politique de contrôle d'accès aux périphériques gérés.

Consultez Définition des périphériques cibles pour une politique de contrôle d'accès.

Prochaine étape

Passez à l'étape suivante du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 7.

Configuration d'une règle de contrôle d'accès pour la protection contre les programmes malveillants

Mise en garde Ajoutez la première ou supprimez la dernière règle de fichier active qui combine l'action de règle de recherche de programmes malveillants dans le nuage (Malware Cloud Lookup) ou de blocage de programmes malveillants (**Block Malware**) avec une option d'analyse (**Spero Analysis ou MSEXE**, **Dynamic Analysis**, ou encore **Local Malware Analysis**) ou une option de stockage de fichiers (**Malware** pour les programmes malveillants, **Unknown** pour les fichiers inconnus**, Clean** pour les fichiers fiables ou **Custom** pour un stockage personnalisé). redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Remarque La normalisation en ligne est activée automatiquement lorsqu'une politique de fichier est incluse dans une règle de contrôle d'accès. Pour en savoir plus, consultez Le préprocesseur de normalisation en ligne.

Avant de commencer

- Le profilage adaptatif **doit** être activé (son état par défaut) comme décrit dans Configuration des profils adaptatifs pour que les règles de contrôle d'accès effectuent le contrôle de fichiers, y compris AMP.
- Vous devez être un administrateur, un administrateur de l'accès ou un administrateur réseau pour effectuer cette tâche.

Procédure

Étape 1 Dans l'éditeur de règles de contrôle d'accès (à partir de **Policies > Access Control)** (Politiques > Contrôle d'accès) choisissez l'**actionAllow** (autorisation), **Interactive Block** (blocage interactif) ou **Interactive Block with reset** (blocage interactif avec réinitialisation).

Étape 2 Choisissez une **politique de fichiers** pour inspecter le trafic qui correspond à la règle de contrôle d'accès, ou choisissez **Aucune** pour désactiver l'inspection de fichiers pour le trafic correspondant.

Étape 3 (Facultatif) Désactivez la journalisation des événements liés aux fichiers ou aux programmes malveillants pour les connexions correspondantes en cliquant sur **Logging** (Journalisation) et en décochant la case **Log files** (Fichiers journaux).

Remarque Cisco vous recommande de laisser activée la journalisation des événements liés aux fichiers et aux programmes malveillants.

Étape 4 Enregistrer la règle

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

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Créer ou modifier une politique de fichiers, à la page 16
Scénarios de redémarrage de Snort

Configurer la maintenance et la surveillance de la protection contre les programmes malveillants

Une maintenance permanente est essentielle pour la protection de votre réseau.

Avant de commencer

Configurez votre système pour protéger votre réseau contre les programmes malveillants.

Voir Configurer la protection contre les programmes malveillants, à la page 7 et les procédures référencées.

Procédure

Étape 1 Assurez-vous que votre système dispose toujours de la protection la plus à jour et la plus efficace.

Consultez Maintenance de votre système : mise à jour des types de fichiers admissibles pour l'analyse dynamique, à la page 15.

Étape 2 Configurez des alertes pour les événements liés aux programmes malveillants et la surveillance de l'intégrité.

Consultez le Guide d'administration Cisco Secure Firewall Management Center pour obtenir des renseignements sur la *configuration des alertes Défense contre les programmes malveillants* et pour des renseignements sur les modules suivants :

- Analyse locale des programmes malveillants
- Renseignements de sécurité
- Mises à jour des périphériques à propos des données sur les menaces
- Taux d'événements d'intrusion et de fichier
- AMP pour l'état de FirePower
- État de AMP for Endpoints

Prochaine étape

Passez en revue les prochaines étapes du processus de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 7.

Connexions en nuage pour la protection contre les programmes malveillants

Des connexions à des nuages publics ou privés sont nécessaires pour protéger votre réseau contre les programmes malveillants.

Nuages AMP

Le serveur en nuage Advanced Malware Protection (AMP) est un serveur hébergé par Cisco qui utilise l'analyse du mégadonnées et une analyse en continu pour fournir des renseignements que le système utilise pour détecter et bloquer les programmes malveillants sur votre réseau.

La solution AMP en nuage fournit des dispositions pour les programmes malveillants détectés dans le trafic réseau par les périphériques gérés, ainsi que des mises à jour des données pour l'analyse des programmes malveillants locaux et la préclassification des fichiers.

Si votre entreprise a déployé AMP pour les points terminaux et configuré Firepower pour importer ses données, le système importe ces données depuis le nuage AMP, y compris les enregistrements d'analyse, les détections de programmes malveillants, les quarantaines et les indications de compromission (IOC).

Cisco offre les options suivantes pour obtenir des données du nuage Cisco sur les menaces de programmes malveillants connues :

- **Nuage public AMP**

  Votre Cisco Secure Firewall Management Center communique directement avec le nuage public de Cisco. Il existe trois nuages AMP publics, aux États-Unis, en Europe et en Asie.

Nuage d'analyse dynamique

- **Nuage Cisco Secure Malware Analytics**

Nuage public qui traite les fichiers admissibles que vous envoyez pour une analyse dynamique, et fournit des évaluations de menace et des rapports d'analyse dynamique. Firepower prend en charge 200 échantillons par jour pour l'analyse Cisco Secure Malware Analytics.

Configurations de la connexion au nuage AMP

Exigences et bonnes pratiques pour les connexions au nuage d'AMP

Exigences relatives aux connexions au nuage d'AMP

Vous devez être un utilisateur administrateur pour configurer le nuage AMP.

Pour vous assurer que votre centre de gestion peut communiquer avec le nuage AMP, consultez les rubriques sous *Sécurité, accès Internet et ports de communication* dans le fichier Guide d'administration Cisco Secure Firewall Management Center.

Pour utiliser le port existant pour les communications AMP, consultez *Exigences en matière de ports* de communication dans le Guide d'administration Cisco Secure Firewall Management Center .

AMP et haute disponibilité

Bien qu'ils partagent les politiques de fichiers et les configurations associées, les centre de gestion d'une paire à haute disponibilité ne partagent ni les connexions au nuage, ni les fichiers capturés, ni les événements de fichiers et de programmes malveillants. Pour assurer la continuité des opérations et pour s'assurer que les dispositions des fichiers détectés aux programmes malveillants sont les mêmes sur les deux centre de gestion, les centre de gestion] actifs et en veille doivent avoir accès au nuage.

Dans les configurations à haute disponibilité, vous devez configurer les connexions cloud AMP indépendamment sur les instances Active et Standby du Firepower Management Center; ces configurations ne sont pas synchronisées.

Modifier les options AMP (de protection avancée contre les logiciels malveillants)

Procédure

Étape 1 Choisissez **Intégration** > **Autres intégrations**.

Étape 2 Cliquez sur **Services infonuagiques**.

Étape 3 Sélectionnez des options :

Tableau 1 : Options AMP pour les réseaux

Option	Description
Activer les mises à jour automatiques de la détection locale de programmes malveillants.	Le moteur de détection local des programmes malveillants analyse et préclassifie de manière statique les fichiers à l'aide des signatures fournies par Cisco. Si vous activez cette option, le Cisco Secure Firewall Management Center vérifie les mises à jour de signature une fois toutes les 30 minutes.

Option	Description
Partager l'URI des événements de logiciels malveillants avec Cisco	Le système peut envoyer des informations sur les fichiers détectés dans le trafic réseau vers le nuage AMP. Ces informations comprennent les informations d'URI associées aux fichiers détectés et leurs valeurs de hachage SHA-256. Bien que le partage soit obligatoire, la transmission de ces informations à Cisco contribue aux efforts futurs pour identifier et suivre les programmes malveillants.

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

Connexions d'analyse dynamique

Exigences en matière d'analyse dynamique

Vous devez être un administrateur, un administrateur d'accès ou un utilisateur réseau et faire partie du domaine global pour utiliser l'analyse dynamique.

Avec la licence appropriée, le système a automatiquement accès au nuage Cisco Secure Malware Analytics.

L'analyse dynamique exige que les périphériques gérés aient un accès direct ou un accès par serveur mandataire au nuage Cisco Secure Malware Analytics ou à un appareil Cisco Secure Malware Analytics sur site sur le port 443.

Consultez aussi Quels fichiers sont admissibles pour l'analyse dynamique?, à la page 29.

Affichage de la connexion d'analyse dynamique par défaut

Par défaut, Cisco Secure Firewall Management Center peut se connecter au nuage Cisco Secure Malware Analytics public pour la soumission de fichiers et la récupération de rapports. Vous ne pouvez ni configurer ni supprimer cette connexion.

Procédure

Étape 1 Choisissez **intégration** > **AMP** > **Connexions d'analyse dynamique**.

Étape 2 Vous pouvez afficher le nuage utilisé sur la connexion d'analyse dynamique par défaut. Pour associer le périphérique, cliquez sur **Associé** ( ). Pour en savoir plus, consultez Activation de l'accès aux résultats de l'analyse dynamique dans le nuage public, à la page 14.

Activation de l'accès aux résultats de l'analyse dynamique dans le nuage public

Cisco Secure Malware Analytics offre des rapports sur les fichiers analysés plus détaillés que ceux disponibles dans centre de gestion. Si votre entreprise dispose d'un compte Cisco Secure Malware Analytics en nuage, vous pouvez accéder directement au portail Cisco Secure Malware Analytics pour afficher des détails supplémentaires sur les fichiers envoyés à des fins d'analyse à partir de vos périphériques gérés. Toutefois, pour des raisons de confidentialité, les détails de l'analyse des fichiers ne sont accessibles que pour

l'organisation qui a transmis les fichiers. Par conséquent, avant de pouvoir afficher ces informations, vous devez associer votre centre de gestion aux fichiers soumis par ses périphériques gérés.

Avant de commencer

Vous devez avoir un compte Cisco Secure Malware Analytics en nuage et avoir à portée de main les identifiants de votre compte.

Procédure

Étape 1 Sélectionnez **intégration** > **AMP** > **Connexions d'analyse dynamique**.

Étape 2 Cliquez sur **Associé** ( ) dans la ligne du tableau correspondant à l'icône Cisco Secure Malware Analytics.

Une fenêtre de portail Cisco Secure Malware Analytics s'ouvre.

Étape 3 Connectez-vous au Cisco Secure Malware Analytics en nuage.

Étape 4 Cliquez sur **Submit Query** (Envoyer la demande).

Remarque Ne modifiez pas la valeur par défaut dans le champ **Devices** (Périphériques).

Si vous rencontrez des difficultés avec ce processus, communiquez avec votre représentant Cisco Secure Malware Analytics chez Cisco TAC.

Cela peut prendre jusqu'à 24 heures pour que cette modification prenne effet.

Prochaine étape

Une fois l'association activée, consultez *Affichage des résultats de l'analyse dynamique dans le nuage Cisco* dans le Guide d'administration Cisco Secure Firewall Management Center.

Maintenance de votre système : mise à jour des types de fichiers admissibles pour l'analyse dynamique

La liste des types de fichiers admissibles à l'analyse dynamique est déterminée par la base de données de vulnérabilités (VDB), qui est mise à jour périodiquement (mais pas plus d'une fois par jour). Si vous êtes un utilisateur administrateur, vous pouvez mettre à jour les types de fichiers admissibles pour l'analyse dynamique.

Pour vous assurer que votre système dispose de la liste actuelle :

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- (Recommandé) Voir *Automatisation de la mise à jour de la base de données de vulnérabilités* comme indiqué dans le Guide d'administration Cisco Secure Firewall Management Center
- Vérifiez régulièrement les nouvelles mises à jour de VDB et *mettez à jour manuellement la VDB* comme indiqué dans le Guide d'administration Cisco Secure Firewall Management Center au besoin.

  Si vous choisissez cette option, nous vous recommandons de planifier des rappels réguliers à cet effet.

Étape 2 Si vos politiques de fichiers précisent des types de fichiers individuels au lieu de la catégorie de types de fichiers compatibles avec l' **analyse dynamique**, mettez à jour vos politiques de fichiers pour utiliser les nouveaux types de fichiers pris en charge.

Étape 3 Si la liste des types de fichiers admissibles change, procéder au déploiement sur les périphériques gérés.

Politiques relatives aux fichiers et règles de fichiers

Créer ou modifier une politique de fichiers

Avant de commencer

Si vous configurez des politiques de protection contre les programmes malveillants, consultez toutes les procédures requises dans Configurer les politiques relatives aux fichiers, à la page 9.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Malware & File (programme malveillant et fichier)** .

Étape 2 Créer une nouvelle politique ou modifier une politique existante

Si vous modifiez une politique existante : Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Astuces Pour faire une copie d'une politique de fichiers existante, cliquez sur **Copier** ( ), puis saisissez un nom unique pour la nouvelle politique dans la boîte de dialogue qui apparaît. Vous pouvez ensuite modifier la copie.

Étape 3 Ajoutez une ou plusieurs règles à la politique de fichier, comme décrit dans Création de règles de fichier, à la page 32.

Étape 4 Si vous le souhaitez, sélectionnez Avancé et configurez les options avancées comme décrit dans Options avancées et options d'inspection de fichier d'archive, à la page 17.

Étape 5 Enregistrez la politique de fichiers.

Prochaine étape

- Si vous configurez des politiques de protection contre les programmes malveillants, consultez les autres procédures obligatoires dans Configurer les politiques relatives aux fichiers, à la page 9.
- Sinon :
  - Ajoutez la politique de fichiers à une règle de contrôle d'accès, comme décrit dans Ajouter des politiques de fichiers à votre configuration de contrôle d'accès, à la page 9.
  - Déployer les changements de configuration.

Options avancées et options d'inspection de fichier d'archive

Les paramètres avancés de l'éditeur de politiques de fichiers proposent les options générales suivantes :

- **Première analyse du fichier** : Sélectionnez cette option pour analyser les fichiers vus pour la première fois pendant que la disposition AMP sur le nuage est en attente. Le fichier doit correspondre à une règle configurée pour effectuer une recherche dans le nuage de programmes malveillants et une analyse dynamique de Spéro, de logiciel malveillant local. Si vous désélectionnez cette option, les fichiers détectés pour la première fois sont marqués avec une disposition Inconnue
- **Activer la liste de détection personnalisée** : bloquez les fichiers sur la liste de détection personnalisée.
- **Activer la liste blanche** : si elle est activée, cette politique autorisera les fichiers sur la liste blanche des fichiers inoffensifs.
- **Si la disposition du nuage AMP est inconnue, remplacer la disposition en fonction de l'indice de menace** : sélectionnez une option :
  - Si vous sélectionnez **Désactivé**, le système ne remplacera pas la disposition fournie par AMP Cloud.
  - Si vous définissez un seuil de score de menace, les fichiers ayant un verdict AMP sur le nuage Inconnu sont considérés comme des programmes malveillants si leur score d'analyse dynamique est égal ou inférieur au seuil.
  - Si vous sélectionnez une valeur de seuil inférieure, vous augmentez le nombre de fichiers traités comme des programmes malveillants. Selon l'action sélectionnée dans votre politique de fichiers, cela peut entraîner une augmentation du nombre de fichiers bloqués.

Les paramètres avancés de l'éditeur de politiques de fichiers proposent les options d'inspection de fichier d'archive suivantes :

- **Inspecter les archives** : permet d'inspecter le contenu des fichiers d'archive, pour les fichiers d'archive aussi volumineux que le paramètre de contrôle d'accès avancé **Taille de fichier maximale pour stocker**.
- **Bloquer les archives chiffrées** : pour bloquer les archives protégées par mot de passe.
- **Bloquer les archives non inspectées** : bloque les fichiers d'archive dont le contenu ne peut être inspecté par le système pour des raisons autres que le chiffrement. Cela s'applique généralement aux fichiers corrompus ou à ceux qui dépassent la profondeur d'archivage maximale spécifiée.
- **Profondeur maximale des archives** : bloque les fichiers d'archives imbriqués qui dépassent la profondeur spécifiée. Le fichier d'archive de niveau supérieur n'est pas pris en compte dans ce décompte; La profondeur commence à 1 avec le premier fichier imbriqué.

Fichiers d'archive

Les fichiers d'archive sont des fichiers qui contiennent d'autres fichiers, tels que des fichiers `.zip` ou `.rar`.

Si un fichier individuel dans une archive correspond à une règle de fichier avec une action de blocage, le système bloque l'ensemble de l'archive, pas seulement le fichier individuel.

Pour en savoir plus sur les options d'inspection du fichier d'archive, consultez Options avancées et options d'inspection de fichier d'archive, à la page 17.

Fichiers d'archives pouvant être inspectés

- **Types de fichiers**

Une liste complète des types de fichiers d'archive inspectables s'affiche dans l'interface Web de FMC sur la page de configuration des règles de fichier. Pour afficher cette page, consultez Création de règles de fichier, à la page 32.

Les fichiers contenus qui peuvent être inspectés s'affichent dans la même page.

- **Taille du fichier**

  Vous pouvez inspecter des fichiers d'archive aussi volumineux que le paramètre de contrôle d'accès avancé de la politique d'archivage des fichiers (**Maximum file size to store**).

- **Archives imbriquées**

  Les fichiers d'archive peuvent contenir d'autres fichiers d'archive, qui peuvent à leur tour contenir des fichiers d'archive. Le niveau auquel un fichier est imbriqué correspond à la *profondeur de son fichier d'archive*. Notez que le fichier d'archive de niveau supérieur n'est pas inclus dans le décompte de profondeur; La profondeur commence à 1 avec le premier fichier imbriqué.

  Le système peut inspecter jusqu'à trois niveaux de fichiers imbriqués sous le fichier d'archive le plus externe (niveau 0). Vous pouvez configurer votre politique de fichiers pour bloquer les fichiers d'archive qui dépassent cette profondeur (ou une profondeur maximale inférieure que vous spécifiez).

  Si vous choisissez de ne pas bloquer les fichiers qui dépassent la profondeur maximale d'archive de 3, lorsque des fichiers d'archive qui contiennent du contenu amovible et certains contenus imbriqués à une profondeur de 3 ou plus apparaissent dans le trafic surveillé, le système examine et rapporte des données uniquement pour qu'il a pu inspecter.

  Toutes les fonctionnalités applicables aux fichiers non compressés (comme l'analyse dynamique et le stockage de fichiers) sont disponibles pour les fichiers imbriqués dans les fichiers d'archive.

- **Fichiers chiffrés**

  Vous pouvez configurer le système pour bloquer les archives dont le contenu est chiffré ou ne peut pas être inspecté.

- **Les archives qui ne sont pas inspectées**

  Si le trafic qui contient un fichier d'archive figure sur une liste de blocage de Security Intelligence ou une liste à ne pas bloquer, ou si la valeur SHA-256 du fichier d'archive de niveau supérieur figure sur la liste de détection personnalisée, le système n'inspecte pas le contenu du fichier d'archive.

  Si un fichier imbriqué est bloqué, l'archive entière est bloquée; cependant, si un fichier imbriqué est autorisé, l'archive n'est pas transmise automatiquement (selon les autres fichiers imbriqués et leurs caractéristiques).

  Les fichiers .exe contenus dans certaines archives .rar ne peuvent pas être détectés, y compris peut-être rar5.

Dispositions des fichiers d'archive

Les dispositions des fichiers d'archives sont basées sur les dispositions attribuées aux fichiers dans l'archive. **Toutes** les archives qui contiennent des fichiers de programmes malveillants identifiés reçoivent un classement `Programme malveillant`. Les archives qui ne contiennent pas de fichiers malveillants identifiés reçoivent un classement `Inconnu` si elles contiennent des fichiers inconnus, et un classement `Sain` si elles ne contiennent que des fichiers sains.

Tableau 2 : Disposition du fichier d'archive par contenu

Dispositions des fichiers d'archive	Nombre de fichiers inconnus	Nombre de fichiers propres	Nombre de fichiers de programmes malveillants
`Inconnu`	1 ou plus	N'importe lequel	0
`Sain`	0	1 ou plus	0
`Logiciels malveillants`	N'importe lequel	N'importe lequel	1 ou plus

Les fichiers d'archives, comme les autres fichiers, peuvent avoir un classement `Détection personnalisée` ou `Indisponible` si les conditions relatives à ces classements s'appliquent.

Affichage du contenu et des détails des archives

Si votre politique de fichiers est configurée pour inspecter le contenu du fichier d'archive, vous pouvez utiliser le menu contextuel dans un tableau dans les pages du menu Analyse > Fichiers et la visionneuse de trajectoire de fichier réseau pour afficher les informations sur les fichiers d'une archive lorsque le fichier d'archive s'affiche dans un événement de fichier, dans un événement malveillant ou comme fichier de capture.

Tout le contenu des fichiers d'archive est répertorié sous forme de tableau, avec un court résumé des informations pertinentes : nom, valeur de hachage SHA-256, type, catégorie et profondeur de l'archive. Une icône de trajectoire de fichier réseau se trouve à côté de chaque fichier, sur laquelle vous pouvez cliquer pour afficher plus d'informations sur ce fichier spécifique.

Remplacer la disposition du fichier à l'aide de listes personnalisées

Si un fichier a une disposition dans le nuage AMP que vous savez être incorrecte, vous pouvez ajouter la valeur SHA-256 du fichier à une liste de fichiers qui remplace la disposition du nuage :

- Pour traiter un dossier comme si le nuage AMP avait reçu une disposition sûre, ajoutez le dossier à la *liste sûre*.
- Pour traiter un fichier comme si le nuage AMP avait affecté une disposition de programmes malveillants, ajoutez le fichier à la *liste de détection personnalisée.*

Lors de la détection ultérieure, le périphérique autorise ou bloque le fichier sans réévaluer la disposition du fichier. Vous pouvez utiliser la politique de liste sûre ou de liste de détection personnalisée par fichier.

Remarque Pour calculer la valeur SHA-256 d'un fichier, vous devez configurer une règle dans la politique de fichiers pour effectuer une recherche de programme malveillant dans le nuage ou bloquer les programmes malveillants sur les fichiers correspondants.

Pour obtenir des renseignements complets sur l'utilisation des listes de fichiers dans Firepower, consultez Liste de fichiers.

Sinon, le cas échéant, utiliser Listes de fichiers centralisées d'AMP pour les points terminaux, à la page 20.

Listes de fichiers centralisées d'AMP pour les points terminaux

Si votre entreprise a déployé AMP pour les points terminaux, Firepower peut utiliser les listes de blocage et d'autorisation créées dans AMP pour les points terminaux lorsqu'elle interroge le nuage AMP pour obtenir les dispositions des fichiers.

Préalables :

- Votre entreprise doit utiliser le nuage public AMP.
- Votre entreprise a déployé AMP pour les points terminaux.
- Vous avez enregistré votre système Firepower auprès de AMP pour les points terminaux en utilisant la procédure décrite dans Intégrer Firepower et Cisco Secure Endpoint, à la page 39.

Pour créer et déployer ces listes, consultez la documentation ou l'aide en ligne d'AMP pour les points terminaux.

Remarque Les listes de fichiers créées dans Firepower remplacent les listes de fichiers créées dans AMP pour les points terminaux.

Gestion des politiques relatives aux fichiers

La page Politiques de fichiers affiche une liste des politiques de fichiers existantes ainsi que les dates de leur dernière modification. Vous pouvez utiliser cette page pour gérer vos politiques de fichiers.

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.

Remarque Le système vérifie les mises à jour de la liste des types de fichiers admissibles pour l'analyse dynamique (pas plus d'une fois par jour). Si la liste des types de fichiers admissibles change, cela constitue un changement de la politique de fichiers; toute politique de contrôle d'accès qui utilise la politique de fichier est marquée comme obsolète si elle est déployée sur des périphériques. Vous devez déployer des politiques avant que la politique de fichiers mise à jour puisse prendre effet sur le périphérique. Consultez Maintenance de votre système : mise à jour des types de fichiers admissibles pour l'analyse dynamique, à la page 15.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Malware & File (programme malveillant et fichier)** .

Étape 2 Gérez vos politiques de fichiers :

- Comparer : Cliquez sur **Comparer les politiques**; voir Comparer les politiques.
- Créer : pour créer une politique de fichiers, cliquez sur **Nouvelle politique de fichiers** et procédez comme décrit dans Créer ou modifier une politique de fichiers, à la page 16.

- Copier : pour copier une politique de fichiers, cliquez sur **Copier** ().

  Si **Afficher** () apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

- Supprimer : si vous souhaitez supprimer une politique de fichiers, cliquez sur **Supprimer** (), puis cliquez sur **Yes** (oui) et sur **OK** lorsque vous y êtes invité.

  Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

- Deploy—Choose (déployer, choisir) **Deploy (déployer)** > **Deployment (déploiement)**; voir Déployer les modifications de configuration.

- Modifier : si vous souhaitez modifier une politique de fichiers existante, cliquez sur **Edit** ().

- Rapporter : Cliquez sur **Rapport** (); voir Générer des rapports sur les politiques appliquées.

Règles de fichier

Une politique de fichier, tout comme sa politique de contrôle d'accès parente, contient des règles qui déterminent la façon dont le système gère les fichiers correspondant aux conditions de chaque règle. Vous pouvez configurer des règles de fichier distinctes pour effectuer différentes actions pour différents types de fichiers, protocoles d'application ou directions de transfert.

Par exemple, quand un fichier correspond à une règle, la règle peut :

- autoriser ou bloquer des fichiers en fonction d'une simple correspondance de type de fichier
- bloquer des fichiers en fonction de leur disposition (si l'évaluation indique ou non qu'il est malveillant)
- stocker des fichiers sur le périphérique (pour en savoir plus, consultez Fichiers capturés et stockage de fichiers, à la page 29)
- soumettre les fichiers stockés (capturés) aux programmes malveillants locaux, à Spéro ou pour une analyse dynamique

En outre, la politique de fichier peut :

- traiter automatiquement un fichier comme s'il était propre ou constituait un logiciel malveillant en fonction des entrées de la liste de nettoyage ou de la liste de détection personnalisée
- traiter un fichier comme s'il s'agissait d'un logiciel malveillant si le niveau de menace du fichier dépasse un seuil configurable
- inspecter le contenu des fichiers d'archive (comme `.zip` ou `.rar`)
- bloquer les fichiers d'archives dont le contenu est chiffré, imbriqué au-delà d'une profondeur d'archive maximale spécifiée ou pour d'autres raisons, non inspectable

Composants des règles de fichiers

Tableau 3 : Composants des règles de fichiers

Composant de règle de fichier	Description
Protocole d'application	Le système peut détecter et inspecter les fichiers transmis par FTP, HTTP, SMTP, IMAP, POP3 et NetBIOS-ssn (SMB). **Any**, la valeur par défaut, détecte les fichiers dans le trafic HTTP, SMTP, IMAP, POP3, FTP et NetBIOS-ssn (SMB). Pour améliorer les performances, vous pouvez restreindre la détection de fichiers à un seul de ces protocoles d'application par fichier.
Direction du transfert	Vous pouvez inspecter le trafic entrant FTP, HTTP, IMAP, POP3 et NetBIOS-ssn (SMB) pour repérer les fichiers téléchargés. vous pouvez inspecter le trafic sortant FTP, HTTP, SMTP et NetBIOS-ssn (SMB) pour repérer les fichiers téléchargés. **Astuces** Utilisez **Any** pour détecter les fichiers sur plusieurs protocoles d'application, que les utilisateurs envoient ou reçoivent.
Catégories de types de fichiers	Le système peut détecter différents types de fichiers. Ces types de fichiers sont regroupés en catégories de base, y compris les fichiers multimédias (SWF, mp3), les fichiers exécutables (exe, torrent) et les fichiers PDF. Vous pouvez configurer des règles de fichiers qui détectent des types de fichiers individuels ou sur des catégories entières de types de fichiers. Par exemple, vous pouvez bloquer tous les fichiers multimédias ou uniquement les fichiersshockWave Flash (SWF). Vous pouvez également configurer le système pour vous avertir lorsqu'un utilisateur télécharge un fichier BitTorrent (torrent). Notez que les exécutables comprennent des types de fichiers qui peuvent exécuter des macros et des scripts, car ils peuvent contenir des programmes malveillants. Pour obtenir la liste des types de fichiers que le système peut inspecter, sélectionnez **Policy (Contrôle d'accès) (Access Control) > Malware and File** (programmes malveillants et fichier) , créez une nouvelle politique de fichier temporaire, puis cliquez sur **Add Rule** (ajouter une règle). Sélectionnez une catégorie de type de fichier. Les types de fichiers que le système peut inspecter s'affichent dans la liste **Types de fichiers**. **Remarque** Les règles de fichier déclenchées fréquemment peuvent affecter les performances du système. Par exemple, la détection de fichiers multimédias dans le trafic HTTP (par exemple, YouTube transmet une quantité importante de contenu Flash) pourrait générer un nombre considérable d'événements.

Composant de règle de fichier	Description
Action découlant d'une règle sur un fichier	L'action d'une règle de fichier détermine la façon dont le système gère le trafic qui correspond aux conditions de la règle. Selon l'action sélectionnée, vous pouvez configurer si le système stocke le fichier ou effectue une analyse Spéro, un programme malveillant local ou une analyse dynamique d'un fichier. Si vous sélectionnez une action de blocage, vous pouvez également configurer si le système réinitialise également la connexion bloquée. Pour obtenir une description de ces actions et options, consultez Actions de la règle de fichier, à la page 23. Les règles de fichier sont évaluées dans l'ordre règle-action, et non numérique. Pour de plus amples renseignements, consultez la section Actions de règle de fichier : ordre d'évaluation, à la page 31.

Actions de la règle de fichier

Les règles de fichiers vous donnent un contrôle fin sur les types de fichiers que vous souhaitez consigner, bloquer ou analyser pour détecter les programmes malveillants. Chaque règle de fichier est associée à une action qui détermine la façon dont le système gère le trafic correspondant aux conditions de la règle. Pour être efficace, une politique de fichiers doit contenir une ou plusieurs règles. Vous pouvez utiliser des règles distinctes dans une politique de fichiers pour effectuer différentes actions pour différents types de fichiers, protocoles d'application ou directions de transfert.

Actions de la règle de fichier

- Les règles de *détection de fichiers* vous permettent d'enregistrer la détection de types de fichiers spécifiques dans la base de données, tout en autorisant leur transmission.
- Les règles de *blocage des fichiers* vous permettent de bloquer des types de fichiers spécifiques. Vous pouvez configurer des options pour réinitialiser la connexion lorsqu'un transfert de fichier est bloqué et stocker les fichiers capturés sur le périphérique géré.
- Les règles*Recherche dans le nuage de programmes malveillants* vous permettent d'obtenir et d'enregistrer la disposition des fichiers qui traversent votre réseau, tout en permettant leur transmission.
- Les règles de *blocage des programmes malveillants* vous permettent de calculer la valeur de hachage SHA-256 de types de fichiers spécifiques, d'interroger le nuage AMP pour déterminer si les fichiers qui traversent votre réseau contiennent des programmes malveillants, puis de bloquer les fichiers qui représentent des menaces.

Actions de la règle de fichier

Selon l'action que vous sélectionnez, vous avez différentes options :

Actions de la règle de fichier	Vous avez la capacité de bloquer les fichiers?	Capable de bloquer les programmes malveillants?	Capable de détecter les fichiers?	Capable de rechercher dans le nuage des programmes malveillants?
Analyse Spero pour MSEXE	non	oui, vous pouvez soumettre des fichiers exécutables.	non	oui, vous pouvez soumettre des fichiers exécutables.
Analyse dynamique*	non	oui, vous pouvez soumettre des fichiers exécutables avec des dispositions de fichier inconnues.	non	oui, vous pouvez soumettre des fichiers exécutables avec des dispositions de fichier inconnues.
Gestion de la capacité	Non	Oui	Non	oui
Analyse locale des programmes malveillants*	Non	Oui	Non	oui
Réinitialiser la connexion	oui (recommandée)	oui (recommandée)	Non	Non
Stocker les fichiers	oui, vous pouvez stocker tous les types de fichiers correspondants	oui, vous pouvez stocker les types de fichiers correspondant aux dispositions de fichiers que vous sélectionnez	oui, vous pouvez stocker tous les types de fichiers correspondants	oui, vous pouvez stocker les types de fichiers correspondant aux dispositions de fichiers que vous sélectionnez

* Pour des informations complètes sur ces options, consultez Options de protection contre les programmes malveillants (dans Actions de règle de fichier), à la page 25 et ses sous-sections.

Mise en garde Activer ou désactiver le **stockage des fichiers** dans une règle **Détecter les fichiers** ou **Bloquer les fichiers** , ou ajouter la première ou supprimer la dernière règle de fichier qui combine l'action de la règle **Recherche dans le nuage de programmes malveillants** ou **Blocage des programmes malveillants** avec une option **d'analyse (Analyse Spero ou MSEXE**, **Analyse dynamique**ou **Analyse locale des programmes malveillants**) ou une option de stockage des fichiers (Programmes**malveillants** , **Inconnu**, **Propre**ou **Personnalisé**), redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Options de protection contre les programmes malveillants (dans Actions de règle de fichier)

Le système applique plusieurs méthodes d'inspection et d'analyse de fichier pour déterminer si un fichier contient un programme malveillant.

Selon les options que vous activez dans une règle de fichier, le système inspecte les fichiers à l'aide des outils suivants, dans l'ordre :

1. Analyse Spero, à la page 27 et Recherche en nuage de la solution AMP, à la page 27
2. Analyse locale des programmes malveillants, à la page 28
3. Analyse dynamique, à la page 28

Pour une comparaison de ces outils, consultez Comparaison des options de protection contre les programmes malveillants, à la page 25.

(Vous pouvez également, si vous le souhaitez, bloquer tous les fichiers en fonction de leur type. Pour plus d'information, consultez la section Bloquer tous les fichiers par type, à la page 31.

Consultez également les renseignements sur le produit AMP pour les points terminaux de Cisco à l'adresse (Facultatif) Protection contre les programmes malveillants avec AMP pour les points terminaux, à la page 37 et les sous-sections.

Comparaison des options de protection contre les programmes malveillants

Le tableau suivant détaille les avantages et les désavantages de chaque type d'analyse de fichier, ainsi que la façon dont chaque méthode de protection contre les programmes malveillants détermine le classement d'un fichier.

Type d'analyse	Avantage	Restrictions	Identification des programmes malveillants
Analyse Spero	Analyse structurelle des fichiers exécutables, envoi de la signature Spero au nuage AMP pour analyse	Moins approfondie que l'analyse locale des programmes malveillants ou l'analyse dynamique, uniquement pour les fichiers exécutables	Le classement passe de Inconnu à Logiciel malveillant uniquement lors de l'identification définitive d'un logiciel malveillant.
Analyse locale des programmes malveillants	Utilise moins de ressources que l'analyse dynamique et renvoie les résultats plus rapidement, en particulier si les programmes malveillants détectés sont courants	Résultats moins approfondis que l'analyse dynamique	Le classement passe de Inconnu à Logiciel malveillant uniquement lors de l'identification définitive d'un logiciel malveillant.

Type d'analyse	Avantage	Restrictions	Identification des programmes malveillants
Analyse dynamique	Une analyse approfondie des fichiers inconnus à l'aide de Cisco Secure Malware Analytics	Les fichiers admissibles sont téléversés dans le nuage public ou dans un appareil sur place. L'analyse prend un certain temps.	Le niveau de menace détermine le caractère malveillant d'un fichier. Le classement peut être fondé sur le seuil de niveau de menace configuré dans la politique de fichiers.
Analyse Spéro et analyse des programmes malveillants locaux	Consomme moins de ressources que la configuration de l'analyse locale des programmes malveillants et de l'analyse dynamique, tout en utilisant les ressources en nuage AMP pour identifier les programmes malveillants	Moins approfondie que l'analyse dynamique, analyse de Spéro convient uniquement aux fichiers exécutables	Le classement passe de Inconnu à Logiciel malveillant uniquement lors de l'identification définitive d'un logiciel malveillant.
Analyse Spéro et analyse dynamique	Utilise toutes les capacités d'AMP en nuage pour envoyer des fichiers et des signatures Spéro	Résultats obtenus moins rapidement qu'avec l'analyse locale des programmes malveillants	La note de menace change en fonction des résultats de l'analyse dynamique pour les fichiers préclassifiés comme programmes malveillants possibles. Le classement change en fonction du seuil de note de menace configuré dans la politique de fichiers, et va d'Inconnu à Programme malveillant si l'analyse de Spéro identifie un logiciel malveillant.
Analyse des programmes malveillants locaux et analyse dynamique	Des résultats exhaustifs avec l'utilisation des deux types d'analyse de fichier	Consomme plus de ressources que l'une ou l'autre seule	La note de menace change en fonction des résultats de l'analyse dynamique pour les fichiers préclassifiés comme programmes malveillants possibles. Le classement passe de Inconnu à Logiciel malveillant si l'analyse locale des programmes malveillants identifie un programme malveillant, ou en fonction du seuil de niveau de menace configuré dans la politique de fichiers.

Type d'analyse	Avantage	Restrictions	Identification des programmes malveillants
Analyse de Spéro, analyse des programmes malveillants locaux et analyse dynamique	Les résultats les plus exhaustifs	Utilise la plupart des ressources pour exécuter les trois types d'analyses de fichiers	La note de menace change en fonction des résultats de l'analyse dynamique pour les fichiers préclassifiés comme programmes malveillants possibles. Le classement change de Inconnu à Programme malveillant si l'analyse de Spéro ou l'analyse locale de logiciel malveillant identifie un logiciel malveillant, ou en fonction du seuil de niveau de menace configuré dans la politique de fichiers.
(Bloquer la transmission de tous les fichiers d'un type de fichier précisé)	Ne nécessite pas de licence Défense contre les programmes malveillants (Techniquement, cette option n'est pas une option de protection contre les programmes malveillants.)	Des fichiers légitimes seront également bloqués	(Aucune analyse n'est effectuée.)

Remarque La préclassification ne détermine pas en elle-même la disposition d'un fichier; il s'agit simplement d'un des facteurs qui déterminent si un fichier est admissible pour l'analyse dynamique.

Analyse Spero

L'analyse de Spéro examine les caractéristiques structurelles telles que les métadonnées et les informations d'en-tête dans les fichiers exécutables. Après avoir généré une signature Spéro sur la base de ces informations, si le fichier est un fichier exécutable admissible, le périphérique la soumet au moteur heuristique Spéro dans le nuage AMP. En fonction de la signature Spéro, le moteur Spéro détermine si le fichier est un logiciel malveillant. Vous pouvez également configurer des règles pour soumettre des fichiers à l'analyse de Spéro sans les soumettre également au nuage AMP.

Notez que vous ne pouvez pas soumettre manuellement des fichiers pour analyse Spéro.

Recherche en nuage de la solution AMP

Pour les fichiers admissibles à une évaluation à l'aide de la protection avancée contre les programmes malveillants, centre de gestion effectue une *recherche dans le nuage des programmes malveillants* et interroge le nuage AMP sur la disposition du fichier en fonction de sa valeur de hachage SHA-256.

Pour améliorer les performances, le système met en cache les dispositions renvoyées par le nuage et utilise les dispositions mises en cache pour les fichiers connus plutôt que d'interroger le nuage AMP. Pour plus d'informations sur ce cache, consultez Longévité de la disposition en cache, à la page 28.

Analyse locale des programmes malveillants

L'analyse locale des programmes malveillants permet à un appareil géré d'inspecter localement les fichiers exécutables, les PDF, les documents bureautiques et d'autres types de fichiers à la recherche des types de programmes malveillants les plus courants, à l'aide d'un ensemble de règles de détection fourni par Talos Intelligence Group. Comme l'analyse locale n'interroge pas le nuage AMP et n'exécute pas le fichier, l'analyse locale des programmes malveillants permet de gagner du temps et des ressources système.

Si le système détecte un programme malveillant lors d'une analyse locale des programmes malveillants, il met à jour la disposition du fichier existant de Inconnu à Programme malveillant. Le système génère ensuite un nouvel événement de programme malveillant. Si le système ne détecte pas les programmes malveillants, il ne met pas à jour la disposition du fichier de Inconnu à Nettoyé. Après avoir exécuté l'analyse locale des programmes malveillants, le système met en cache les informations sur les fichiers telles que la valeur de hachage SHA-256, l'horodatage et la disposition de sorte que s'il est détecté à nouveau dans un certain délai, le système peut identifier les programmes malveillants sans analyse supplémentaire. Pour plus d'informations sur le cache, consultez Longévité de la disposition en cache, à la page 28.

L'analyse des programmes malveillants locaux ne nécessite pas l'établissement de communications avec le nuage Cisco Secure Malware Analytics. Cependant, vous devez configurer les communications avec le nuage pour soumettre des fichiers à une analyse dynamique et pour télécharger les mises à jour de l'ensemble de règles local d'analyse des programmes malveillants.

Longévité de la disposition en cache

Les classements renvoyés par une requête dans le nuage AMP, les scores de menace associés et les classements attribués par l'analyse locale des programmes malveillants ont une valeur de durée de vie (TTL). Lorsqu'un classement a été conservé sans mise à jour pendant la durée spécifiée dans la valeur TTL, le système purge les informations en cache. Les classements et les évaluations de menace associées ont les valeurs TTL suivantes :

- Propre : 4 heures
- Inconnu : 1 heure
- Programme malveillant : 1 heure

Si une interrogation du cache identifie une disposition en cache qui a expiré, le système interroge la base de données locale d'analyse de programmes malveillants et le nuage AMP pour une nouvelle disposition.

Analyse dynamique

Vous pouvez configurer votre politique de fichiers pour soumettre automatiquement les fichiers à une analyse dynamique à l'aide de Cisco Secure Malware Analytics (anciennement Threat Grid), la plateforme d'analyse de fichiers et d'informations sur les menaces de Cisco.

Les périphériques envoient des fichiers admissibles à Cisco Secure Malware Analytics (vers le nuage public ou vers un appareil sur site, selon vos spécifications), peu importe si le périphérique stocke le fichier.

Cisco Secure Malware Analytics exécute le fichier dans un environnement de bac à sable, analyse le comportement du fichier pour déterminer s'il est malveillant et renvoie un niveau de menace qui indique la probabilité qu'un fichier contient un programme malveillant. À partir du score de menace, vous pouvez afficher un rapport de synopsis d'analyse dynamique avec les motifs du score de menace attribué. Vous pouvez

également examiner Cisco Secure Malware Analytics pour afficher les rapports détaillés sur les fichiers que votre organisation a envoyés, ainsi que les rapports nettoyés avec des données limitées pour les fichiers que votre organisation n'a pas envoyés.

Pour en savoir plus sur l'ensemble des pratiques Cisco Secure Malware Analytics de Cisco, consultez https://www.cisco.com/c/en/us/products/security/threat-grid/index.html.

Pour configurer votre système afin d'effectuer une analyse dynamique, consultez les rubriques sous Connexions d'analyse dynamique, à la page 14.

Quels fichiers sont admissibles pour l'analyse dynamique?

L'admissibilité d'un fichier à l'analyse dynamique dépend des éléments suivants :

- le type de fichier
- la taille du fichier
- l'action de la règle de fichier

En outre :

- Le système transmet uniquement les fichiers qui correspondent aux règles de fichiers que vous configurez.
- Le fichier doit avoir une disposition de recherche dans le nuage avec programme malveillant Inconnu ou Indisponible au moment de l'envoi du fichier pour analyse.
- Le système doit préclassifier le fichier comme logiciel malveillant potentiel.

Analyse dynamique et gestion de la capacité

La gestion de la capacité vous permet de stocker temporairement des fichiers qui sont par ailleurs éligibles à l'analyse dynamique si le système est temporairement incapable d'envoyer des fichiers au nuage, soit parce que l'appareil ne peut pas communiquer avec le nuage, soit parce que le nombre maximum d'envois a été atteint. Le système transmet les fichiers stockés lorsque la condition d'empêchement est levée.

Certains périphériques peuvent stocker des fichiers sur le disque dur du périphérique ou dans un ensemble de stockage des programmes malveillants. Consultez aussi Ensemble de stockage de logiciels malveillants, à la page 30.

Fichiers capturés et stockage de fichiers

La fonction de stockage de fichiers vous permet de recueillir des fichiers sélectionnés détectés dans le trafic et d'en stocker automatiquement une copie temporaire sur le disque dur d'un périphérique ou, s'il est installé, dans le paquet de stockage de programmes malveillants.

Une fois que votre appareil a capturé les fichiers, vous pouvez :

- Stocker les fichiers capturés sur le disque dur du périphérique pour analyse ultérieure.
- Télécharger le fichier stocké sur un ordinateur local pour une analyse manuelle plus approfondie ou à des fins d'archivage.
- Soumettre manuellement les fichiers capturés admissibles à la recherche dans le nuage ou à l'analyse dynamique d'AMP.

Notez qu'une fois qu'un périphérique a stocké un fichier, il ne le recapturera pas si le fichier est détecté ultérieurement et que le périphérique a toujours ce fichier stocké.

Remarque Lorsqu'un fichier est détecté pour la première fois sur votre réseau, vous pouvez générer un événement de fichier qui représente la détection du fichier. Cependant, si votre règle de fichier effectue une recherche en nuage de programme malveillant, le système a besoin de plus de temps pour interroger le nuage AMP et renvoyer une décision de suppression ou non. En raison de ce délai, le système ne peut pas stocker ce fichier avant la deuxième fois qu'il est vu sur votre réseau, et le système peut immédiatement déterminer la suppression ou non du fichier.

Que le système capture ou stocke un fichier, vous pouvez :

- Passer en revue les informations sur le fichier capturé dans Analyse > Fichiers > Fichiers capturés, y compris si le fichier a été stocké ou soumis pour analyse dynamique, la disposition du fichier et le niveau de menace, ce qui vous permet d'examiner rapidement les menaces possibles détectées sur votre réseau.
- Afficher la trajectoire du fichier pour déterminer comment il a traversé votre réseau et quels hôtes en ont une copie.
- Ajouter le fichier à la liste des fichiers propres ou à la liste de détection personnalisée pour toujours traiter le fichier comme s'il était propre ou malveillant lors d'une future détection.

Configurer des règles de fichier dans une politique de fichier pour capturer et stocker des fichiers d'un type spécifique, ou avec une forme de fichier particulière, si elle est disponible. Après avoir associé la politique de fichiers à une politique de contrôle d'accès et l'avoir déployée sur vos périphériques, les fichiers correspondants dans le trafic sont capturés et stockés. Vous pouvez également limiter les tailles de fichier minimale et maximale à stocker.

Les fichiers stockés ne sont pas inclus dans les sauvegardes du système.

Vous pouvez afficher les informations sur les fichiers capturés sous Analysis > Files (analyses > Fichiers) » et télécharger une copie pour une analyse hors ligne.

Ensemble de stockage de logiciels malveillants

Selon la configuration de votre politique de fichiers, votre appareil pourrait stocker une quantité importante de données de fichiers sur le disque dur. Vous pouvez installer un ensemble de stockage de programmes malveillants dans le périphérique; Le système stocke les fichiers dans l'ensemble de stockage de programmes malveillants, ce qui laisse plus d'espace sur le disque dur principal pour stocker les événements et les fichiers de configuration. Le système supprime régulièrement les fichiers plus anciens. S'il n'y a pas suffisamment d'espace disponible sur le disque dur principal du périphérique et qu'une unité de stockage de programmes malveillants n'est pas installée, vous ne pouvez pas stocker de fichiers.

Mise en garde Ne tentez pas d'installer un disque dur non fourni par Cisco dans votre périphérique. L'installation d'un disque dur non pris en charge pourrait endommager ce dernier. Les ensembles de stockage de programmes malveillants sont disponibles à l'achat **uniquement** auprès de Cisco. Communiquez avec le service d'assistance si vous avez besoin d'aide avec l'ensemble de stockage contre les programmes malveillants.

Sans ensemble de stockage de logiciel malveillant installé, lorsque vous configurez un périphérique pour stocker des fichiers, il alloue une partie définie de l'espace du disque dur principal au stockage des fichiers capturés. Si vous configurez la gestion de la capacité pour stocker temporairement des fichiers en vue de l'analyse dynamique, le système utilise la même allocation de disque dur pour stocker ces fichiers jusqu'à ce qu'il puisse les soumettre de nouveau au nuage.

Lorsque vous installez un ensemble de stockage de programmes malveillants dans un périphérique et que vous configurez le stockage de fichiers ou la gestion de la capacité, le périphérique alloue l'ensemble de l'ensemble de stockage de programmes malveillants pour le stockage de ces fichiers. Le périphérique ne peut pas stocker d'autres informations dans l'ensemble de stockage du logiciel malveillant.

Lorsque l'espace alloué au stockage des fichiers capturés est plein, le système supprime les fichiers stockés les plus anciens jusqu'à ce que l'espace alloué atteigne un seuil défini par le système. En fonction du nombre de fichiers stockés, vous pourriez constater une baisse substantielle de l'utilisation du disque après la suppression des fichiers par le système.

Si un appareil contient déjà des fichiers lorsque vous installez un ensemble de stockage de programmes malveillants, au prochain redémarrage du périphérique , tous les fichiers capturés ou fichiers de gestion de capacité stockés sur le disque dur principal sont déplacés vers l'ensemble de stockage de logiciel malveillant. Tous les fichiers futurs que le périphérique stockera seront stockés dans l'ensemble de stockage des programmes malveillants.

Pour en savoir plus sur l'utilisation de MSP sur les périphériques Firepower, consultez le Guide d'installation du matériel Firepower pour votre périphérique.

Bloquer tous les fichiers par type

Si votre entreprise souhaite bloquer non seulement la transmission de fichiers malveillants, mais aussi de tous les fichiers d'un type spécifique, qu'ils contiennent ou non des programmes malveillants, vous pouvez le faire.

Le contrôle de fichiers est pris en charge pour tous les types de fichiers où le système peut détecter les programmes malveillants, ainsi que pour de nombreux types de fichiers supplémentaires. Ces types de fichiers sont regroupés en catégories de base, telles que les fichiers multimédias (SWF, mp3), les fichiers exécutables (exe, torrent) et les fichiers PDF.

Techniquement, le blocage de tous les fichiers en fonction de leur type n'est pas une fonctionnalité de protection contre les programmes malveillants; il ne nécessite pas de licence Défense contre les programmes malveillants et n'interroge pas le nuage AMP.

Actions de règle de fichier : ordre d'évaluation

Une politique de fichiers contient probablement plusieurs règles avec des actions différentes pour différentes situations. Si plusieurs règles peuvent s'appliquer à une situation particulière, l'ordre d'évaluation décrit dans cette rubrique s'applique. En général, le blocage simple prévaut sur l'inspection et le blocage des programmes malveillants, qui prévalent sur la détection et la journalisation simples.

L'ordre de préséance des actions File-rule (de règle relative aux fichiers) est le suivant :

- *Bloquer les fichiers*
- *Bloquer les maliciels*
- *Recherche de maliciels dans le nuage*
- *Détecter les fichiers*

Création de règles de fichier

Mise en garde Activer ou désactiver le **stockage des fichiers** dans une règle **Détecter les fichiers** ou **Bloquer les fichiers** , ou ajouter la première ou supprimer la dernière règle de fichier qui combine l'action de la règle **Recherche dans le nuage de programmes malveillants** ou **Blocage des programmes malveillants** avec une option **d'analyse (Analyse Spero ou MSEXE**, **Analyse dynamique**ou **Analyse locale des programmes malveillants**) ou une option de stockage des fichiers (Programmes**malveillants** , **Inconnu**, **Propre**ou **Personnalisé**), redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Avant de commencer

Si vous configurez des règles pour la protection contre les programmes malveillants, consultez Configurer les politiques relatives aux fichiers, à la page 9.

Procédure

Étape 1 Sélectionnez **Policies (politiques) > Access Control (contrôle d'accès) > Malware & File (programme malveillant et fichier)**.

Étape 2 Cliquez sur l'icône de modification pour modifier une politique de fichiers existante.

Étape 3 Dans l'éditeur de politiques de fichiers, cliquez sur **Add Rule** (ajouter une règle).

Étape 4 Sélectionnez un **protocole d'application** et une **direction de transfert**, comme décrit dans Composants des règles de fichiers, à la page 22.

Étape 5 Sélectionnez un ou plusieurs **types de fichiers**.

Les types de fichiers que vous voyez dépendent du protocole d'application sélectionné, de la direction du transfert et de l'action.

Vous pouvez filtrer la liste des types de fichiers comme suit :

- Sélectionnez une ou plusieurs **catégories de types de fichiers**, puis cliquez sur **Tous les types dans les catégories sélectionnées.**
- Recherchez un type de fichier par son nom ou sa description. Par exemple, saisissez `Windows` dans le champ **Rechercher le nom et la description** pour afficher une liste des fichiers propres à Microsoft Windows.

Astuces Passez votre curseur sur un type de fichier pour afficher sa description.

Étape 6 Sélectionner une **action** de règle de fichier comme décrit dans Actions de la règle de fichier, à la page 23, en tenant compte de Actions de règle de fichier : ordre d'évaluation, à la page 31.

Les actions à votre disposition dépendent des licences que vous avez installées. Consultez Exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants, à la page 3.

Étape 7 Selon l'action que vous avez sélectionnée, configurez les options :

- réinitialiser la connexion après le blocage du fichier

- stocker les fichiers qui correspondent à la règle
- activer l'analyse Spero*
- activer l'analyse locale des programmes malveillants*
- activer l'analyse dynamique* et la gestion de la capacité

* Pour en savoir plus sur ces options, consultez Actions de la règle de fichier, à la page 23 et Options de protection contre les programmes malveillants (dans Actions de règle de fichier), à la page 25 et leurs sous-sections.

Étape 8 Cliquez sur **Add** (ajouter).

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Si vous configurez des politiques de protection contre les programmes malveillants, retournez à Configurer les politiques relatives aux fichiers, à la page 9.
- Déployer les changements de configuration.

Journalisation des règles de contrôle d'accès pour la protection contre les programmes malveillants

Lorsque le système détecte un fichier interdit (y compris un logiciel malveillant) selon les paramètres de la politique de fichiers, il consigne automatiquement un événement dans la base de données Cisco Secure Firewall Management Center. Si vous ne souhaitez pas consigner les événements liés aux fichiers ou aux programmes malveillants, vous pouvez désactiver cette journalisation pour chaque règle de contrôle d'accès.

Le système enregistre également la fin de la connexion associée à la base de données Cisco Secure Firewall Management Center, quelle que soit la configuration de l'enregistrement de la règle de contrôle d'accès invoquée.

Modifications rétrospectives de disposition

Les dispositions des fichiers peuvent changer. Par exemple, à mesure que de nouvelles informations sont découvertes, le nuage AMP peut déterminer qu'un fichier qui était auparavant considéré comme sûr est maintenant identifié comme programme malveillant, ou inversement, qu'un fichier identifié comme programme malveillant est en fait sûr. Lorsque la disposition d'un fichier que vous avez interrogé au cours de la semaine passée change, le nuage AMP en informe le système afin qu'il puisse automatiquement prendre des mesures lors de la prochaine détection de ce fichier. Une disposition modifiée est appelée disposition *rétrospective*.

Options de rendement et de stockage pour l'inspection des fichiers et des logiciels malveillants

L’augmentation de la taille des fichiers peut affecter les performances du système.

Tableau 4 : Fichier de contrôle d’accès avancé et options Défense contre les programmes malveillants

Champ	Description	Directives et restrictions
Limiter le nombre d’octets inspectés lors de la détection du type de fichier	Limiter le nombre d’octets inspectés lors de la détection du type de fichier	0 - 4294967295 (4 Go) 0 supprime la restriction. La valeur par défaut est la taille maximale de segment d’un paquet TCP (1 460 octets). Dans la plupart des cas, le système peut identifier les types de fichiers courants à l’aide du premier paquet. Pour détecter les fichiers ISO, saisissez une valeur supérieure à 3 68 70.
Autoriser le fichier si la recherche dans le nuage pour le blocage des maliciels prend plus de (secondes)	Spécifie la durée pendant laquelle le système conserve le dernier octet d'un fichier qui correspond à une règle **Bloquer les programmes malveillants** et qui n'a pas de disposition en cache, pendant que la recherche de nuages de programmes malveillants s'effectue. Si le temps s’écoule sans que le système n’obtient de disposition, le fichier est transmis. Les dispositions de Non disponible ne sont pas mises en cache.	30 secondes Ne réglez *pas* cette option à 0 sans contacter le service d’assistance. Cisco vous recommande d’utiliser la valeur par défaut pour éviter de bloquer le trafic en raison d’échecs de connexion.
Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)	Empêche le système de stocker des fichiers dont la taille dépasse une certaine taille, d’effectuer une recherche dans le nuage de programmes malveillants ou de bloquer les fichiers s’ils sont ajoutés à la liste de détection personnalisée.	0 - 4294967295 (4 Go) 0 supprime la restriction. Cette valeur doit être supérieure ou égale à la **taille maximale du fichier à stocker (octets)** et à la **taille maximale du fichier pour les tests d'analyse dynamique (octets)**.

Champ	Description	Directives et restrictions

Taille minimale du fichier pour l'inspection et le stockage avancés des fichiers (octets)	Ces paramètres spécifient :
	• Taille de fichier que le système peut inspecter à l'aide des détecteurs suivants :
	  • Analyse Spero
	  • Utilisation en fonction bac à sable et préclassification
	  • Analyse locale des programmes malveillants / ClamAV
	  • Inspection d'archive
	• Taille de fichier que le système peut stocker à l'aide d'une règle de fichier.
		0 à 10487560 (10 Mo)
		0 désactive le stockage de fichiers.
		Doit être inférieur ou égal à **Taille maximale du fichier à stocker (octets)** et **Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)**.

Taille maximale du fichier pour l'inspection et le stockage avancés des fichiers (octets)		0 à 10487560 (10 Mo) 0 désactive le stockage de fichiers. Doit être supérieur ou égal à **Taille minimale du fichier à stocker (octets)**, et inférieur ou égal à **Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)**.
Taille de fichier minimale pour les tests d'analyse dynamique (octets)	Spécifie la taille de fichier minimale que le système peut soumettre au nuage AMP pour une analyse dynamique.	0 à 10487560 (10 Mo) Doit être inférieur ou égal à **Taille maximale du fichier pour le test d'analyse dynamique (octets)** et **Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)**. La taille de fichier pour l'analyse dynamique doit être dans les limites définies par les paramètres minimaux et maximaux pour l'analyse de fichier. Le système vérifie dans le nuage AMP les mises à jour de la taille de fichier minimale que vous pouvez envoyer (pas plus d'une fois par jour). Si la nouvelle taille minimale est supérieure à votre valeur actuelle, votre valeur actuelle est mise à jour avec la nouvelle taille minimale et votre politique est marquée comme obsolète.

Champ	Description	Directives et restrictions
Taille de fichier maximale pour les tests d'analyse dynamique (octets)	Spécifie la taille de fichier maximale que le système peut soumettre au nuage AMP pour une analyse dynamique.	0 à 10487560 (10 Mo) Doit être supérieur ou égal à **Taille minimale du fichier pour le test d'analyse dynamique (octets)**, et inférieur ou égal à **Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)**. La taille de fichier pour l'analyse dynamique doit être dans les limites définies par les paramètres minimaux et maximaux pour l'analyse de fichier. Le système vérifie le nuage AMP pour s'assurer que la taille de fichier maximale que vous pouvez envoyer est mise à jour (pas plus d'une fois par jour). Si la nouvelle taille maximale est inférieure à votre valeur actuelle, votre valeur actuelle est mise à jour avec la nouvelle taille maximale et votre politique est marquée comme obsolète.

Réglage du rendement et du stockage de l'inspection des fichiers et des logiciels malveillants

Vous devez être un administrateur, un administrateur de l'accès ou un administrateur réseau pour effectuer cette tâche.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Paramètres avancés**.

Étape 2 Cliquez sur **Edit** (✎) à côté de **Paramètres des fichiers et des programmes malveillants**.

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 l'une des options décrites dans Options de rendement et de stockage pour l'inspection des fichiers et des logiciels malveillants, à la page 34.

Étape 4 Cliquez sur **OK**.

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

Prochaine étape

- Déployer les changements de configuration.

(Facultatif) Protection contre les programmes malveillants avec AMP pour les points terminaux

AMP pour les points terminaux de Cisco est un produit de protection distinct contre les programmes malveillants qui peut compléter la protection contre les programmes malveillants fournie par le système Firepower et être intégré à votre déploiement Firepower.

AMP pour les points terminaux est la solution avancée de protection contre les programmes malveillants de Cisco pour grande entreprise qui fonctionne comme un connecteur léger sur les *points terminaux* des utilisateurs (ordinateurs et périphériques mobiles) pour découvrir, comprendre et bloquer les manifestations de programmes malveillants avancés, les menaces persistantes avancées et les attaques ciblées.

Avantages de la solution AMP pour les points terminaux :

- configurer des politiques et des profils de détection de programmes malveillants personnalisés pour l'ensemble de votre entreprise et effectuer des analyses flash et complètes des fichiers de vos utilisateurs.
- effectuer une analyse des programmes malveillants, y compris afficher les cartes thermiques, les informations détaillées sur les fichiers, la trajectoire du fichier réseau et les causes premières des menaces
- configurer plusieurs aspects du contrôle des épidémies, y compris les quarantaines automatiques, le blocage des applications pour empêcher l'exécution des fichiers exécutables non en quarantaine et les listes d'exclusion
- créer des protections personnalisées, bloquer l'exécution de certaines applications en fonction de la politique de groupe et créer des listes d'applications autorisées personnalisées
- utiliser la console de gestion AMP pour les points terminaux pour vous aider à atténuer les effets des programmes malveillants. La console de gestion offre une interface Web robuste et flexible dans laquelle vous contrôlez tous les aspects de votre déploiement d'AMP pour les points terminaux et gérez toutes les phases d'une épidémie.

Pour en savoir plus sur AMP pour les points terminaux, consultez :

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html.
- L'aide en ligne de la console de gestion AMP pour les points terminaux.
- La documentation AMP pour les points terminaux disponible à l'adresse : http://docs.amp.cisco.com.

Comparaison des protections contre les programmes malveillants : Firepower ou AMP pour les points terminaux

Tableau 5 : Différences dans la protection avancée contre les programmes malveillants par détection de produit

Fonctionnalités	Firepower Malware Protection (Défense contre les programmes malveillants)	AMP pour les points terminaux
Détection du type de fichier et méthode de blocage (contrôle des fichiers)	Dans le trafic réseau, en utilisant le contrôle d'accès et les politiques de fichiers	Non pris en charge

Fonctionnalités	Firepower Malware Protection (Défense contre les programmes malveillants)	AMP pour les points terminaux
Détection et blocage de programmes malveillants	Dans le trafic réseau, en utilisant le contrôle d'accès et les politiques de fichiers	Sur les points d'accès individuels (ordinateurs des utilisateurs finaux et périphériques mobiles), à l'aide d'un connecteur qui communique avec le nuage AMP
Trafic réseau inspecté	Trafic passant par un périphérique géré	Aucun; les connecteurs installés sur les terminaux inspectent directement les fichiers
Source de données sur les programmes malveillants	Nuage AMP (public ou privé)	Nuage AMP (public ou privé)
Force de détection des programmes malveillants	Types de fichiers limités	Tous les types de fichiers
Choix d'analyse des programmes malveillants	Analyse basée sur le centre de gestion, plus dans le nuage AMP	Basée sur centre de gestion, plus options supplémentaires dans la console de gestion AMP pour les points terminaux
Atténuation du risque des programmes malveillants	Blocage des programmes malveillants dans le trafic réseau, corrections initiées par centre de gestion	Options de quarantaine et de contrôle des épidémies basées sur AMP pour les points terminaux, -remédiations à l'initiative de centre de gestion
Événements générés	Événements de fichiers, fichiers capturés, événements de programmes malveillants et événements rétrospectifs de programmes malveillants	Événements de programmes malveillants
Informations contenues dans les événements de programmes malveillants	Informations de base sur les programmes malveillants, ainsi que données de connexion (adresse IP, port et protocole d'application)	des informations détaillées sur les événements malveillants associés aux programmes malveillants; aucune donnée de connexion
Trajectoire des fichiers de réseau	Basé sur centre de gestion	centre de gestion et la console de gestion AMP pour les points terminaux ont chacun une trajectoire de fichier réseau. Les deux sont utiles.
Licences ou abonnements requis	Licences requises pour le contrôle des fichiers et Défense contre les programmes malveillants	Abonnement AMP pour points terminaux Aucune licence n'est requise pour importer les données AMP pour points terminaux dans FMC.

À propos de l'intégration de Firepower et d'AMP pour les points terminaux

Si votre entreprise a déployé AMP pour les points terminaux, vous pouvez éventuellement intégrer ce produit à votre déploiement Firepower.

L'intégration d'AMP pour les points terminaux ne nécessite pas de licence Firepower dédiée.

Avantages de l'intégration de Firepower et d'AMP pour les points terminaux

L'intégration de votre déploiement AMP pour les points terminaux à votre système offre les avantages suivants :

- Les listes centralisées d'applications bloquées et d'applications autorisées configurées dans AMP pour points terminaux peuvent déterminer les résultats des analyses SHA des fichiers envoyés par Firepower au nuage AMP en vue de leur élimination.

  Consultez Listes de fichiers centralisées d'AMP pour les points terminaux, à la page 20.

- Le système peut importer dans Cisco Secure Firewall Management Center les événements de programmes malveillants détectés par Cisco Advanced Malware Protection afin que vous puissiez gérer ces événements avec les événements de programmes malveillants générés par le système. Les données importées pour ces événements comprennent les analyses, les détections de programmes malveillants, les quarantaines, les exécutions bloquées et les rappels dans le nuage, ainsi que les indications de compromission (IOC) que centre de gestion affichent pour les hôtes qu'il surveille.
- Vous pouvez afficher la trajectoire du fichier et d'autres détails dans la console AMP pour les points terminaux.

Important Si vous utilisez un nuage privé Cisco AMP, consultez les limites à l'adresse AMP pour les points terminaux et nuage privé AMP, à la page 39.

AMP pour les points terminaux et nuage privé AMP

Si vous configurez un nuage privé Cisco AMP pour collecter les données de point terminal AMP sur votre réseau, tous les connecteurs AMP pour les points terminaux envoient des données au nuage privé, qui les transmet à Cisco Secure Firewall Management Center. Le nuage privé ne partage aucune de vos données de point terminal sur une connexion externe.

Si votre entreprise a déployé un nuage privé AMP, toutes les connexions au nuage AMP passent par le nuage privé, qui agit comme un serveur mandataire anonymisé pour assurer la sécurité et la confidentialité de votre réseau surveillé. Cela inclut l'importation des données AMP pour les points terminaux. Le nuage privé ne partage aucune de vos données de point terminal sur une connexion externe.

Les fonctionnalités d'intégration suivantes ne sont pas disponibles si vous utilisez un nuage privé AMP :

- L'utilisation des listes d'applications bloquées et d'applications autorisées configurées dans AMP pour les points terminaux. (Ces listes sont utilisées pour bloquer ou autoriser des fichiers.)
- Visibilité dans AMP pour les points terminaux des événements malveillants générés par Firepower.

Vous pouvez configurer plusieurs nuages privés pour prendre en charge la capacité dont vous avez besoin.

Intégrer Firepower et Cisco Secure Endpoint

Si votre entreprise a déployé le produit Cisco Secure Endpoint de Cisco, vous pouvez intégrer cette application à Firepower pour profiter des avantages décrits dans Avantages de l'intégration de Firepower et d'AMP pour les points terminaux, à la page 39.

Lorsque vous intégrez Cisco Secure Endpoint, vous devez configurer la connexion Cisco Secure Endpoint même si les connexions Défense contre les programmes malveillants (AMP pour Firepower) sont déjà configurées. Vous pouvez configurer plusieurs connexions Cisco Secure Endpoint au nuage.

Mise en garde Dans un déploiement multidomaine, configurez les connexions Cisco Secure Endpoint au niveau feuille uniquement, en particulier si l'espace IP de vos domaines feuilles se chevauche. Si plusieurs sous-domaines ont des hôtes avec la même paire d'adresses IP-MAC, le système pourrait enregistrer les événements de programmes malveillants générés par Cisco Secure Endpoint dans le domaine descendant incorrect ou associer les IOC aux hôtes incorrects.

Cependant, vous pouvez configurer des connexions Cisco Secure Endpoint à n'importe quel niveau de domaine, à condition d'utiliser un compte Cisco Secure Endpoint distinct pour chaque connexion. Par exemple, chaque client d'un MSSP peut avoir son propre déploiement Cisco Secure Endpoint.

Remarque Les connexions Cisco Secure Endpoint qui ne se sont pas enregistrées avec succès n'affectent pas Défense contre les programmes malveillants .

Avant de commencer

- Vous devez être un utilisateur administrateur pour effectuer cette tâche.
- Si votre déploiement utilise le nuage privé Cisco AMP, consultez les limites à l'adresse AMP pour les points terminaux et nuage privé AMP, à la page 39.
- Cisco Secure Endpoint doivent être configurés et fonctionner correctement sur votre réseau.
- Le centre de gestion doit avoir un accès direct à Internet.
- Vérifiez que vos centre de gestion et Cisco Secure Endpoint peuvent communiquer entre eux. Consultez les rubriques sous *Sécurité, accès à l'internet et ports de communication* de Guide d'administration Cisco Secure Firewall Management Center.
- Si vous vous connectez au nuage AMP après avoir restauré vos Cisco Secure Firewall Management Center aux valeurs par défaut ou être revenu à une version précédente, utilisez la console de gestion AMP pour les points terminaux pour supprimer la connexion précédente.
- Vous aurez besoin de vos informations d'authentification Cisco Secure Endpoint pour vous connecter à la console Cisco Secure Endpoint au cours de cette procédure.

Procédure

Étape 1 Choisissez **intégration** > **AMP** > **Gestion AMP**.

Étape 2 Cliquez sur **Add AMP Cloud Connection** (Ajouter une connexion AMP en nuage).

Étape 3 Dans la liste déroulante **Cloud Name** (nom du nuage), choisissez le nuage que vous souhaitez utiliser :

- Le nuage AMP le plus proche de l'emplacement géographique de votre Cisco Secure Firewall Management Center.

  APJC correspond à Asie/Pacifique/Japon/Chine.

Étape 4 Si vous souhaitez utiliser ce nuage pour Défense contre les programmes malveillants et Cisco Secure Endpoint, cochez la case **Use for AMP for Firepower**.

Si vous avez configuré un autre nuage pour gérer les communications Défense contre les programmes malveillants (AMP pour Firepower), vous pouvez décocher cette case; s'il s'agit de votre seule connexion au nuage AMP, vous ne pouvez pas.

Dans un déploiement multidomaine, cette case à cocher s'affiche uniquement dans le domaine global. Chaque Cisco Secure Firewall Management Center ne peut avoir qu'une seule connexion Défense contre les programmes malveillants .

Étape 5 Cliquez sur **Register** (Inscrire).

Une icône d'état en rotation indique qu'une connexion est en attente, par exemple, après avoir configuré une connexion sur Cisco Secure Firewall Management Center, mais avant de l'autoriser à l'aide de la console de gestion Cisco Secure Endpoint. Un **Refus** ( ) indique que le nuage a refusé la connexion ou que la connexion a échoué pour une autre raison.

Étape 6 Confirmez que vous souhaitez continuer avec la console de gestion Cisco Secure Endpoint, puis connectez-vous à cette dernière.

Étape 7 À l'aide de la console de gestion, autorisez le nuage AMP à envoyer des données à Cisco Secure Endpointcentre de gestion.

Étape 8 Si vous souhaitez restreindre les données que centre de gestion reçoit, sélectionnez les groupes spécifiques de votre organisation pour lesquels vous souhaitez recevoir des informations.

Par défaut, le nuage AMP envoie des données pour tous les groupes. Pour gérer les groupes, choisissez **Management** > **Groups** dans la console de gestion Cisco Secure Endpoint. Pour des informations détaillées, consultez l'aide en ligne de la console de gestion.

Étape 9 Cliquez sur **Allow** (autoriser) pour activer la connexion et lancer le transfert des données.

Cliquez sur **Deny** (Refuser) pour revenir à Cisco Secure Firewall Management Center, où la connexion est marquée comme refusée. Si vous quittez la page des applications de la console de gestion Cisco Secure Endpoint et que vous ne refusez ni n'autorisez la connexion, la connexion est marquée comme en attente sur l'interface Web de Cisco Secure Firewall Management Center. Le moniteur d'intégrité ne vous alerte **pas** en cas d'échec de connexion dans ces situations. Si vous souhaitez vous connecter au nuage AMP ultérieurement, supprimez la connexion ayant échoué ou en attente, puis recréez-la.

Un enregistrement incomplet de la connexion Cisco Secure Endpoint ne désactive pas la connexion Défense contre les programmes malveillants .

Étape 10 Pour vérifier que la connexion est correctement configurée :

a) Sur la page **intégration** > **AMP** > **Gestion AMP**, cliquez sur le nom du nuage qui inclut **`AMP pour les points terminaux`** dans la colonne **Type de solution Cisco AMP**.
b) Dans la fenêtre de console AMP pour les points terminaux qui s'affiche, choisissez **Accounts (Comptes)** > **Applications**.
c) Vérifiez que votre centre de gestion figure dans la liste.
d) Dans la fenêtre de la console AMP pour les points terminaux, choisissez **Manage**(gestion)
e) Vérifiez que votre centre de gestion figure dans la liste.

Prochaine étape

- Dans la fenêtre de console AMP pour les points terminaux, configurez les paramètres selon vos besoins. Par exemple, définissez l'appartenance à un groupe pour votre centre de gestion et attribuez des politiques.

Pour obtenir des renseignements, consultez l'aide en ligne de Cisco Advanced Malware Protection pour les points terminaux ou consultez d'autres documents.

- Dans les configurations à haute disponibilité, vous devez configurer les connexions cloud AMP indépendamment sur les instances Active et Standby du Firepower Management Center; ces configurations ne sont pas synchronisées.
- La politique d'intégrité par défaut vous avertit si centre de gestion ne peut pas se connecter au portail AMP pour les points terminaux après une connexion initiale réussie, ou si la connexion est désenregistrée à l'aide du portail AMP.

  Vérifiez que le moniteur **d'état de Cisco Advanced Malware Protection pourles points terminaux** est activé sous **System > Intégrité > Politique**

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.