Configuration des services de sécurité

Cette rubrique contient les sections suivantes :

Survol de la configuration des services de sécurité

Secure Web Appliance utilise des composants de sécurité pour protéger les utilisateurs finaux contre un éventail de programmes malveillants. Vous pouvez configurer les paramètres de protection contre les programmes malveillants et de réputation de sites Web pour chaque groupe de politiques. Lorsque vous configurez des politiques d'accès, AsyncOS pour le Web peut également choisir une combinaison d'analyses de protection contre les programmes malveillants et d'évaluation de réputation Web à utiliser pour déterminer le contenu à bloquer.

Pour protéger les utilisateurs finaux contre les programmes malveillants, vous activez ces fonctionnalités sur l'appliance, puis configurez les paramètres de protection contre les programmes malveillants et de réputation Web conformément à la politique.

Option	Description	Lien
Anti-malware scanning (Analyse de protection contre les programmes malveillants)	Fonctionne avec plusieurs moteurs d'analyse de protection contre les programmes malveillants intégrés à l'appliance pour bloquer les programmes malveillants	Survol de l'analyse à la recherche de programmes malveillants , on page 5

Option	Description	Lien
Web Reputation Filters (Filtres de réputation Web)	Analyse le comportement du serveur Web et détermine si l'URL contient un programme malveillant basé sur l'URL	Survol des filtres de réputation Web , on page 2
Cisco Secure Endpoint	Protection contre les menaces dans les fichiers téléchargés en évaluant la réputation des fichiers et en analysant les caractéristiques des fichiers.	Survol du filtrage de réputation de fichiers et de l'analyse de fichiers

Thèmes connexes

- Activation des filtres contre les programmes malveillants et de réputation, on page 8
- Interprétation de l'analyse adaptative, on page 7

Survol des filtres de réputation Web

Les filtres de réputation Web attribuent un score de réputation Web (WBRS) à une URL pour déterminer la probabilité qu'elle contienne des programmes malveillants basés sur l'URL. Le Secure Web Appliance utilise les scores de réputation Web pour identifier et arrêter les attaques de programmes malveillants avant qu'elles ne se produisent. Vous pouvez utiliser des filtres de réputation Web avec les politiques d'accès, de déchiffrement et de sécurité des données de Cisco.

Score de réputation Web

Les filtres de réputation Web utilisent des données pour évaluer la fiabilité des domaines Internet et la réputation des URL. Le calcul de la réputation Web associe une URL à des paramètres réseau pour déterminer la probabilité que des programmes malveillants soient présents. La probabilité agrégée de la présence de programmes malveillants est ensuite mappée sur un indice de réputation Web compris entre -10 et +10, +10 étant la valeur la moins susceptible de contenir des programmes malveillants.

Voici des exemples de paramètres :

- Données de catégorisation d'URL
- Présence d'un code téléchargeable
- Présence de contrats de licence d'utilisateur final (CLUF) longs et brouillés
- Volume global et variations de volume
- Renseignements sur le propriétaire du réseau
- Historique d'une URL
- Âge d'une URL
- Présence sur toutes les listes de blocage
- Présence sur toutes les listes d'autorisation
- Fautes de frappe d'URL de domaines populaires
- Informations sur le bureau d'enregistrement de domaine
- Informations sur l'adresse IP

Note Cisco ne recueille pas de renseignements permettant d'identifier les clients, comme les noms d'utilisateur, les phrases secrètes ou les adresses IP des clients.

Comprendre le fonctionnement du filtrage de réputation Web

Les scores de réputation Web sont associés à une action à effectuer sur une demande d'URL. Vous pouvez configurer chaque groupe de politiques pour corréler une action à un score de réputation Web particulier. Les actions disponibles dépendent du type de groupe de politiques affecté à la demande d'URL :

Type de politique	Action
Politiques d'accès	Vous pouvez choisir de bloquer, d'analyser ou d'autoriser
Politiques de déchiffrement	Vous pouvez choisir d'abandonner, de déchiffrer ou de transmettre
Politiques de sécurité des données de Cisco	Vous pouvez choisir de bloquer ou de surveiller

Réputation Web dans les politiques d'accès

Lorsque vous configurez les paramètres de réputation Web dans les politiques d'accès, vous pouvez choisir de les configurer manuellement ou de laisser AsyncOS pour le Web choisir les meilleures options à l'aide de l'analyse adaptative. Lorsque l'analyse adaptative est activée, vous pouvez activer ou désactiver le filtrage de réputation Web dans chaque politique d'accès, mais vous ne pouvez pas modifier les scores de réputation Web.

Résultat	Action	Description	Exemple
-10 à -6,0	Block (Bloquer)	Mauvais site. La demande est bloquée et aucune autre analyse contre les programmes malveillants ne se produit.	• L'URL télécharge des informations sans l'autorisation de l'utilisateur. • Pointe subite du volume d'URL. • L'URL correspond à un domaine populaire avec une faute de frappe.
-5,9 à 5,9	Analyser	Site indéterminé. La demande est transmise au moteur DVS pour une analyse plus poussée des programmes malveillants. Le moteur DVS analyse le contenu de la demande et de la réponse du serveur.	• URL créée récemment qui a une adresse IP dynamique et qui contient du contenu téléchargeable. • Adresse IP de propriétaire du réseau ayant un score de réputation Web positif.

Résultat	Action	Description	Exemple
6,0 à 10,0	Allow (Autoriser)	Bon site. La demande est autorisée. Aucune analyse des programmes malveillants requise.	• L'URL ne comporte aucun contenu téléchargeable. • Domaine réputé, à volume élevé, existant depuis longtemps. • Domaine présent sur plusieurs listes d'autorisation. • Aucun lien vers des URL de mauvaise réputation.

Par défaut, les URL d'une requête HTTP auxquelles un score de réputation de sites Web supérieur ou égal à 7 est attribué sont autorisées et ne nécessitent pas d'analyse supplémentaire. Cependant, un score plus faible pour une demande HTTP, tel que 3 ou plus, est automatiquement transféré au moteur Cisco DVS où il est analysé afin de détecter les programmes malveillants. Toute URL dans une demande HTTP qui a une mauvaise réputation est bloquée.

Thèmes connexes

- Interprétation de l'analyse adaptative, on page 7

Réputation Web dans les politiques de déchiffrement

Résultat	Action	Description
-10 à -9,0	Abandonner	Mauvais site. La demande est abandonnée sans avis envoyé à l'utilisateur final. Utilisez ce paramètre avec prudence.
-8,9 à 5,9	Déchiffrer	Site indéterminé. La demande est autorisée, mais la connexion est déchiffrée, et des politiques d'accès sont appliquées au trafic déchiffré.
6,0 à 10,0	Intercommunication	Bon site. La demande est transmise sans inspection ni déchiffrement.

Réputation Web dans les politiques de sécurité des données de Cisco

Résultat	Action	Description
-10 à -6,0	Block (Bloquer)	Mauvais site. La transaction est bloquée et aucune autre analyse n'est effectuée.
-5,9 à 0,0	Monitor (Surperviser)	La transaction ne sera pas bloquée en fonction de la réputation Web et fera l'objet d'une vérification de contenu (type et taille de fichier). **Note** Les sites sans score de réputation sont surveillés.

Survol de l'analyse à la recherche de programmes malveillants

La fonction de protection contre les programmes malveillants Secure Web Appliance utilise le moteur Cisco DVS™ en combinaison avec des moteurs d'analyse de protection contre les programmes malveillants pour bloquer les menaces contre les programmes malveillants sur le Web. Le moteur DVS fonctionne avec les moteurs d'analyse de protection contre les programmes malveillants Webroot™, McAfee et Sophos.

Les moteurs d'analyse inspectent les transactions pour déterminer un verdict d'analyse des programmes malveillants à transmettre au moteur DVS. Le moteur DVS détermine s'il faut surveiller ou bloquer la demande en fonction des verdicts de l'analyse des programmes malveillants. Pour utiliser le composant de protection contre les programmes malveillants de l'appliance, vous devez activer l'analyse contre les programmes malveillants et configurer les paramètres globaux, puis appliquer des paramètres spécifiques à différentes politiques.

Thèmes connexes

- Activation des filtres contre les programmes malveillants et de réputation, on page 8
- Interprétation de l'analyse adaptative, on page 7
- Analyse McAfee, on page 6

Comprendre le fonctionnement du moteur DVS

Le moteur DVS effectue une analyse de protection contre les programmes malveillants sur les transactions URL transférées à partir des filtres de réputation Web. Les filtres de réputation Web calculent la probabilité qu'une URL particulière contienne un programme malveillant et attribuent un score d'URL associé à une action pour bloquer, analyser ou autoriser la transaction.

Lorsque le score de réputation attribué indique d'analyser la transaction, le moteur DVS reçoit la demande d'URL et le contenu de la réponse du serveur. Le moteur DVS, en combinaison avec les moteurs d'analyse Webroot et/ou Sophos ou McAfee, renvoie un verdict d'analyse de programmes malveillants. Le moteur DVS utilise les informations des verdicts de recherche de programmes malveillants et des paramètres de politique d'accès pour déterminer s'il faut bloquer ou transmettre le contenu au client.

Utilisation de plusieurs verdicts de programmes malveillants

Le moteur DVS peut déterminer plusieurs verdicts de programmes malveillants pour une seule URL. Plusieurs verdicts peuvent émaner d'un des moteurs d'analyse activés ou des deux :

- **Différents verdicts émanant de différents moteurs d'analyse.** Lorsque vous activez Webroot et Sophos ou McAfee, chaque moteur d'analyse peut renvoyer différents verdicts de programmes malveillants pour le même objet. Lorsqu'une URL entraîne plusieurs verdicts de la part des deux moteurs d'analyse activés, l'appliance effectue l'action la plus restrictive. Par exemple, si un moteur d'analyse renvoie un verdict de blocage et l'autre un verdict de supervision, le moteur DVS bloque toujours la demande.
- **Différents verdicts émanant du même moteur d'analyse.** Un moteur d'analyse peut renvoyer plusieurs verdicts pour un seul objet lorsque ce dernier contient plusieurs infections. Lorsqu'une URL entraîne plusieurs verdicts de la part du même moteur d'analyse, l'appliance prend des mesures en fonction du verdict ayant la priorité la plus élevée. Le texte suivant répertorie les verdicts possibles d'analyse de programmes malveillants, de la priorité la plus élevée à la plus faible.
- Virus

- Outil de téléchargement de chevaux de Troie
- Cheval de Troie
- Cheval de Troie pour hameçonnage
- Détournement d'identité
- Supervision du système
- Supervision de système commercial
- Composeur automatique
- Vers
- Objet de l'assistant du navigateur
- URL d'hameçonnage
- Logiciels publicitaires
- Fichier chiffré
- Impossible à analyser
- Autres programmes malveillants

Analyse Webroot

Le moteur d'analyse Webroot inspecte les objets pour déterminer le verdict de l'analyse des programmes malveillants à envoyer au moteur DVS. Le moteur d'analyse Webroot inspecte les objets suivants :

- **Demande d'URL.** Webroot évalue une demande d'URL pour déterminer si l'URL pourrait être malveillante. Si Webroot soupçonne que la réponse à partir de cette URL peut contenir un programme malveillant, l'appliance surveille ou bloque la demande, selon la configuration de l'appliance. Si l'évaluation Webroot efface la demande, l'appliance récupère l'URL et analyse la réponse du serveur.
- **Réponse du serveur.** Lorsque l'appliance récupère une URL, Webroot analyse le contenu de la réponse du serveur et le compare à la base de données de signatures Webroot.

Analyse McAfee

Le moteur d'analyse McAfee inspecte les objets téléchargés à partir d'un serveur Web dans les réponses HTTP. Après avoir inspecté l'objet, il transmet un verdict d'analyse de programmes malveillants au moteur DVS pour que ce dernier puisse déterminer s'il faut surveiller ou bloquer la demande.

Le moteur d'analyse McAfee utilise les méthodes suivantes pour déterminer le verdict de l'analyse contre les programmes malveillants :

- Correspondance des schémas de signature de virus
- Analyse heuristique

Correspondance des schémas de signature de virus

McAfee utilise les définitions de virus dans sa base de données avec son moteur d'analyse pour détecter des virus, des types de virus ou d'autres logiciels potentiellement indésirables. Il recherche les signatures de virus dans les fichiers. Lorsque vous activez McAfee, le moteur d'analyse McAfee utilise cette méthode pour analyser le contenu de la réponse du serveur.

Analyse heuristique

L'analyse heuristique est une technique qui utilise des règles générales plutôt que des règles spécifiques pour détecter les nouveaux virus et programmes malveillants. Lorsque le moteur d'analyse McAfee utilise l'analyse

heuristique, il examine le code d'un objet, applique des règles génériques et détermine la probabilité que l'objet ressemble à un virus.

L'utilisation de l'analyse heuristique augmente le risque de signalement de faux positifs (contenu sain désigné comme virus) et pourrait avoir un impact sur les performances de l'appliance. Lorsque vous activez McAfee, vous pouvez choisir d'activer ou non l'analyse heuristique lors de l'analyse d'objets.

Catégories McAfee

Verdit McAfee	Catégorie du verdict de l'analyse contre les programmes malveillants
Virus connus	Virus
Cheval de Troie	Cheval de Troie
Fichier de recommandation	Logiciels publicitaires
Fichier de test	Virus
Candidats	Virus
Tué	Virus
Application commerciale	Supervision de système commercial
Objet potentiellement indésirable	Logiciels publicitaires
Progiciel potentiellement indésirable	Logiciels publicitaires
Fichier chiffré	Fichier chiffré

Analyse Sophos

Le moteur d'analyse Sophos inspecte les objets téléchargés à partir d'un serveur Web dans les réponses HTTP. Après avoir inspecté l'objet, il transmet un verdict d'analyse de programmes malveillants au moteur DVS pour que ce dernier puisse déterminer s'il faut surveiller ou bloquer la demande. Vous pourriez souhaiter activer le moteur d'analyse Sophos au lieu du moteur d'analyse McAfee si le logiciel antiprogramme malveillant McAfee est installé.

Interprétation de l'analyse adaptative

L'analyse adaptative décide quel moteur d'analyse de protection contre les programmes malveillants (y compris l'analyse Cisco Secure Endpoint pour les fichiers téléchargés) traitera la demande Web.

L'analyse adaptative applique la catégorie de programmes malveillants « Outbreak Heuristics » aux transactions qu'elle considère comme des programmes malveillants avant d'exécuter un moteur d'analyse. Vous pouvez choisir de bloquer ou non ces transactions lorsque vous configurez les paramètres de la protection contre les programmes malveillants sur l'appliance.

Analyse adaptative et politiques d'accès

Lorsque l'analyse adaptative est activée, certains paramètres de protection contre les programmes malveillants et de réputation que vous pouvez configurer dans les politiques d'accès sont légèrement différents :

- Vous pouvez activer ou désactiver le filtrage de réputation de sites Web dans chaque politique d'accès, mais vous ne pouvez pas modifier les scores de réputation Web.
- Vous pouvez activer l'analyse de protection contre les programmes malveillants dans chaque politique d'accès, mais vous ne pouvez pas choisir le moteur d'analyse de protection contre les programmes malveillants à activer. L'analyse adaptative choisit le moteur le plus approprié pour chaque demande Web.

Note Si l'analyse adaptative n'est pas activée et que des paramètres de réputation Web et de protection contre les programmes malveillants particuliers sont configurés pour une politique d'accès, tous les paramètres de réputation Web et de protection contre les programmes malveillants existants sont alors remplacés.

Les paramètres Cisco Secure Endpoint de chaque politique sont les mêmes, que l'analyse adaptative soit activée ou non.

Activation des filtres contre les programmes malveillants et de réputation

Before you begin

Vérifiez que les filtres de réputation des sites Web, le moteur DVS et les moteurs d'analyse Webroot, McAfee et Sophos sont activés. Par défaut, ils doivent être activés lors de la configuration du système.

Étape 1 Choisissez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants réputation).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Configurez les paramètres selon vos besoins.

Paramètres	Description
Filtrage de réputation Web	Choisissez d'activer ou non le filtrage de réputation Web.
Analyse adaptative	Choisissez d'activer ou non l'analyse adaptative. Vous pouvez uniquement activer l'analyse adaptative lorsque le filtrage de réputation Web est activé.
Filtrage de réputation de fichiers et analyse de fichiers	Voir Activation et configuration des services d'analyse et de réputation des fichiers.

Paramètres	Description
Intégration de la console Cisco Secure Endpoint [**Advanced** > **Advanced Settings for File Reputation** (Avancé > Paramètres avancés pour la réputation des fichiers)]	Cliquez sur **Register the Appliance with** Secure Endpoint to integrate your appliance with Secure Endpoint (Enregistrer l'appliance auprès de Cisco Secure Endpoint AMP for Endpoints) pour intégrer votre appliance à la console Cisco Secure Endpoint AMP for Endpoints). Pour plus d'informations sur les instructions, consultez Intégration de l'appliance à la console Secure Endpoint AMP for Endpoints, on page 15.
Limites d'analyse des objets du moteur DVS	Indiquez une pour l'analyse. La valeur de la taille maximale de l'objet que vous spécifiez s'applique à la taille complète des demandes et des réponses qui peuvent être analysées par tous les moteurs d'analyse de programmes malveillants et de virus et parCisco Secure Endpoint les fonctionnalités. Elle indique également la taille maximale d'une archive pouvant être inspectée pour l'inspection des archives; voir Politiques d'accès : blocage d'objets pour en savoir plus sur l'inspection des archives. Lorsqu'une taille de chargement ou de téléchargement dépasse cette taille, le composant de sécurité peut interrompre l'analyse en cours et peut ne pas fournir de verdict d'analyse au proxy Web. Si une archive pouvant être inspectée dépasse cette taille, elle est marquée « Not Scanned » (Non analysée).
Sophos	Choisissez d'activer ou non le moteur d'analyse Sophos.
McAfee	Choisissez d'activer ou non le moteur d'analyse McAfee. Lorsque vous activez le moteur d'analyse McAfee, vous pouvez choisir d'activer ou non l'analyse heuristique. **Note** L'analyse heuristique augmente la protection de la sécurité, mais peut entraîner de faux positifs et réduire les performances.
Webroot	Choisissez d'activer ou non le moteur d'analyse Webroot. Lorsque vous activez le moteur d'analyse Webroot, vous pouvez configurer le seuil de risque pour les menaces (TRT). Le seuil de risque pour les menaces attribue une valeur numérique à la probabilité que des programmes malveillants existent. Des algorithmes exclusifs évaluent le résultat d'une séquence de correspondance d'URL et attribuent une évaluation de risque de menace (TRR). Cette valeur est associée au paramètre de seuil de menace. Si la valeur TRR est supérieure ou égale à la valeur TRT, l'URL est considérée comme un programme malveillant et est transmise pour traitement ultérieur. **Note** La définition du seuil de risque de menace sur une valeur inférieure à 90 augmente considérablement le taux de blocage d'URL et rejette les demandes légitimes. Cisco recommande fortement de maintenir la valeur par défaut du TRT à 90. La valeur minimale d'un paramètre TRT est 51.

Étape 4 Envoyez et validez les modifications.

What to do next

- Interprétation de l'analyse adaptative, on page 7
- Analyse McAfee, on page 6

Effacement du cache des services Cisco Secure Endpoint

La fonctionnalité d'effacement du cache Cisco Secure Endpoint efface les dispositions de réputation des fichiers sains, malveillants et inconnus.

Remarque Le cache Cisco Secure Endpoint est utilisé pour augmenter les performances. En utilisant la commande **Clear Cache** (Effacer le cache), vous pourriez observer une dégradation temporaire des performances pendant le remplissage du cache.

Étape 1 Choisissez **Security Services** > **Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation).

Étape 2 Dans la section Cisco Secure Endpoint Services, cliquez sur **Clear Cache** (Effacer le cache) et confirmez votre action.

Configuration des politiques de protection contre les programmes malveillants et de réputation

Lorsque les filtres de protection contre les programmes malveillants et de réputation sont activés sur l'appliance, vous pouvez configurer différents paramètres dans les groupes de politiques. Vous pouvez activer la supervision ou le blocage des catégories de programmes malveillants en fonction des verdicts de l'analyse des programmes malveillants.

Vous pouvez configurer les paramètres de la protection contre les programmes malveillants dans les groupes de politiques suivants :

Type de politique	Lien vers la tâche
Politiques d'accès	Paramètres de protection contre les programmes malveillants et de réputation dans les politiques d'accès, on page 11
Politiques d'analyse des programmes malveillants sortants	Contrôle des demandes de téléchargement à l'aide des politiques d'analyse des programmes malveillants sortants

Vous pouvez configurer les paramètres de réputation Web dans les groupes de politiques suivants :

Type de politique	Lien vers la tâche
Politiques d'accès	Paramètres de protection contre les programmes malveillants et de réputation dans les politiques d'accès, on page 11
Politiques de déchiffrement	Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de déchiffrement, on page 14

Type de politique	Lien vers la tâche
Politiques de sécurité des données de Cisco	Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de déchiffrement, on page 14

Vous pouvez configurer les paramètres Cisco Secure Endpoint uniquement dans les politiques d'accès. Voir la section Configuration des fonctionnalités d'analyse et de réputation de fichiers.

Paramètres de protection contre les programmes malveillants et de réputation dans les politiques d'accès

Lorsque l'analyse adaptative est activée, les paramètres de réputation Web et de protection contre les programmes malveillants que vous pouvez configurer pour les politiques d'accès sont légèrement différents de ceux que vous pouvez définir lorsque l'analyse adaptative est désactivée.

Note Si votre déploiement comprend une appliance de gestion de la sécurité et que vous configurez cette fonctionnalité dans un fichier de configuration principal, les options disponibles dans cette page dépendent de l'activation de la sécurité adaptative pour la configuration principale concernée ou non. Vérifiez le paramètre sur l'appliance de gestion de la sécurité, sur la page **Web > Utilities > Security Services Display** (Web > Utilitaires > Affichage des services de sécurité).

- Interprétation de l'analyse adaptative, on page 7

Configuration des paramètres de protection contre les programmes malveillants et de réputation avec l'analyse adaptative activée

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien **Anti-Malware and Reputation** (Antiprogrammes malveillants et réputation) pour la politique d'accès que vous souhaitez configurer.

Étape 3 Dans la section **Web Reputation and Anti-Malware Settings** (Paramètres de réputation Web et de protection contre les programmes malveillants), choisissez **Define Web Reputation and Anti-Malware Custom Settings** (Définir les paramètres personnalisés de réputation Web et de protection contre les programmes malveillants).

Cela vous permet de configurer les paramètres de réputation Web et de protection contre les programmes malveillants pour cette politique d'accès qui sont différents de la politique globale.

Étape 4 Dans la section **Web Reputation Settings** (Paramètres de réputation Web), choisissez d'activer ou non le filtrage de réputation Web. L'analyse adaptative choisit les seuils de score de réputation Web les plus appropriés pour chaque demande Web.

Étape 5 Configurez les paramètres dans la section Cisco Secure Endpoint **Settings** (Paramètres).

Étape 6 Faites défiler la liste jusqu'à la section des paramètres de Cisco DVS Anti-Malware.

Étape 7 Configurez les paramètres de protection contre les programmes malveillants pour la politique au besoin.

Activer l'analyse des agents utilisateur suspects	Choisissez si vous souhaitez analyser ou non le trafic en fonction du champ user-agent spécifié dans l'en-tête de la demande HTTP. Lorsque vous cochez cette case, vous pouvez choisir de surveiller ou de bloquer les agents utilisateur suspects dans la section Additional Scanning (Analyse supplémentaire) au bas de la page. **Note** Les navigateurs Chrome n'incluent pas de chaîne user-agent dans les demandes FTP-sur-HTTP ; par conséquent, Chrome ne peut pas être détecté en tant qu'agent utilisateur dans ces demandes.
Activer l'analyse des programmes malveillants	Choisissez si vous souhaitez utiliser ou non le moteur DVS pour analyser le trafic à la recherche de programmes malveillants. L'analyse adaptative choisit le moteur le plus approprié pour chaque demande Web.
Malware Categories (Catégorie de programmes malveillants)	Choisissez de surveiller ou de bloquer les différentes catégories de programmes malveillants en fonction du verdict de l'analyse.
Autres catégories	Choisissez si vous souhaitez surveiller ou bloquer les types d'objets et les réponses répertoriés dans cette section. **Note** La catégorie Outbreak Heuristics (Heuristique des épidémies) s'applique aux transactions identifiées comme malveillantes par l'analyse adaptative avant l'exécution de tout moteur d'analyse. **Note** Les transactions URL sont classées comme non analysables lorsque le paramètre de durée maximale configuré est atteint ou lorsque le système éprouve une condition d'erreur transitoire. Par exemple, les transactions peuvent être classées comme non analysables lors des mises à jour du moteur d'analyse ou des mises à niveau d'AsyncOS. Les verdicts d'analyse des programmes malveillants SV_TIMEOUT et SV_ERROR sont considérés comme des transactions non analysables.

Étape 8 Envoyez et validez les modifications.

What to do next

- Interprétation de l'analyse adaptative, on page 7

Configuration des paramètres de protection contre les programmes malveillants et de réputation avec l'analyse adaptative désactivée

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien **Anti-Malware and Reputation** (Antiprogrammes malveillants et réputation) pour la politique d'accès que vous souhaitez configurer.

Étape 3 Dans la section **Web Reputation and Anti-Malware Settings** (Paramètres de réputation Web et de protection contre les programmes malveillants), choisissez **Define Web Reputation and Anti-Malware Custom Settings** (Définir les paramètres personnalisés de réputation Web et de protection contre les programmes malveillants).

Cela vous permet de configurer les paramètres de réputation Web et de protection contre les programmes malveillants pour cette politique d'accès qui sont différents de la politique globale.

Étape 4 Configurez les paramètres dans la section **Web Reputation Settings** (Paramètres de réputation Web).

Étape 5 Configurez les paramètres dans la section Cisco Secure Endpoint **Settings** (Paramètres).

Étape 6 Faites défiler la liste jusqu'à la section des paramètres de Cisco DVS Anti-Malware.

Étape 7 Configurez les paramètres de protection contre les programmes malveillants pour la politique au besoin.

Note Lorsque vous activez le contrôle Webroot, Sophos ou McAfee, vous pouvez choisir de surveiller ou de bloquer certaines catégories supplémentaires dans les catégories de programmes malveillants sur cette page.

Paramètres	Description
Activer l'analyse des agents utilisateur suspects	Choisissez d'activer ou non l'appliance pour analyser le trafic en fonction du champ user-agent spécifié dans l'en-tête de la demande HTTP. Lorsque vous cochez cette case, vous pouvez choisir de surveiller ou de bloquer les agents utilisateur suspects dans la section Additional Scanning (Analyse supplémentaire) au bas de la page. **Note** Les navigateurs Chrome n'incluent pas de chaîne user-agent dans les demandes FTP-sur-HTTP ; par conséquent, Chrome ne peut pas être détecté en tant qu'agent utilisateur dans ces demandes.
Activer Webroot	Choisissez si vous souhaitez permettre à l'appliance d'utiliser le moteur d'analyse Webroot lors de l'analyse du trafic.
Activer Sophos ou McAfee	Choisissez d'activer ou non l'appliance pour utiliser le moteur d'analyse Sophos ou McAfee lors de l'analyse du trafic.
Malware Categories (Catégorie de programmes malveillants)	Choisissez de surveiller ou de bloquer les différentes catégories de programmes malveillants en fonction du verdict de l'analyse. Les catégories répertoriées dans cette section dépendent des moteurs d'analyse que vous avez activés ci-dessus.
Autres catégories	Choisissez si vous souhaitez surveiller ou bloquer les types d'objets et les réponses répertoriés dans cette section. **Note** Les transactions URL sont classées comme non analysables lorsque le paramètre de durée maximale configuré est atteint ou lorsque le système éprouve une condition d'erreur transitoire. Par exemple, les transactions peuvent être classées comme non analysables lors des mises à jour du moteur d'analyse ou des mises à niveau d'AsyncOS. Les verdicts d'analyse des programmes malveillants SV_TIMEOUT et SV_ERROR sont considérés comme des transactions non analysables.

Étape 8 Envoyez et validez les modifications.

What to do next

- Configuration des seuils de score de réputation Web pour les politiques d'accès, on page 14

• Descriptions des catégories de programmes malveillants, on page 19

Configuration des scores de réputation Web

Lorsque vous installez et configurez Secure Web Appliance, les paramètres par défaut pour les scores de réputation de sites Web sont appliqués. Toutefois, vous pouvez modifier les paramètres de seuil pour l'évaluation de la réputation Web selon les besoins de votre organisation. Vous configurez les paramètres de filtre de réputation Web pour chaque groupe de politiques.

Configuration des seuils de score de réputation Web pour les politiques d'accès

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien sous la colonne **Anti-Malware and Reputation** (Protection contre les programmes malveillants et réputation) du groupe de politiques d'accès que vous souhaitez modifier.

Étape 3 Dans la section **Web Reputation and Anti-Malware Settings** (Paramètres de réputation Web et de protection contre les programmes malveillants), choisissez **Define Web Reputation and Anti-Malware Custom Settings** (Définir les paramètres personnalisés de réputation Web et de protection contre les programmes malveillants).

Cela vous permet de configurer les paramètres de réputation Web et de protection contre les programmes malveillants pour cette politique d'accès qui sont différents de la politique globale.

Étape 4 Vérifiez que le champ **Enable Web Reputation Filtering** (Activer le filtrage de réputation Web) est activé.

Étape 5 Déplacez les marqueurs pour modifier la plage des actions de blocage, d'analyse et d'autorisation d'URL.

Étape 6 Envoyez et validez les modifications.

Note Vous pouvez modifier les seuils de score de réputation Web dans les politiques d'accès lorsque l'analyse adaptative est désactivée.

Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de déchiffrement

Étape 1 Choisissez **Web Security Manager > Decryption Policies** (Web Security Manager > Politiques de déchiffrement).

Étape 2 Cliquez sur le lien sous la colonne Web Reputation (Réputation Web) pour le groupe de politiques de déchiffrement que vous souhaitez modifier.

Étape 3 Dans la section **Web Reputation Settings** (Paramètres de réputation Web), choisissez **Define Web Reputation Custom Settings** (Définir les paramètres personnalisés de réputation Web). Cela vous permet de remplacer les paramètres de réputation Web du groupe de politiques globales.

Étape 4 Vérifiez que le champ **Enable Web Reputation Filtering** (Activer le filtrage de réputation Web) est coché.

Étape 5 Déplacez les repères pour modifier la plage des actions de suppression, de déchiffrement et de transmission d'URL.

Étape 6 Dans le champ **Sites with No Score** (Sites sans score de réputation), choisissez l'action à entreprendre sur la demande pour les sites auxquels aucun score de réputation Web n'est affecté.

Étape 7 Envoyez et validez les modifications.

Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de sécurité des données

Étape 1 Choisissez **Web Security Manager > Cisco Data Security** (Web Security Manager > Politiques de sécurité des données de Cisco).

Étape 2 Cliquez sur le lien sous la colonne de réputation Web pour le groupe de politiques de sécurité des données que vous souhaitez modifier.

Étape 3 Dans la section **Web Reputation Settings** (Paramètres de réputation Web), choisissez **Define Web Reputation Custom Settings** (Définir les paramètres personnalisés de réputation Web).

Cela vous permet de remplacer les paramètres de réputation Web du groupe de politiques globales.

Étape 4 Déplacez le marqueur pour modifier la plage de blocage d'URL et surveiller les actions.

Étape 5 Envoyez et validez les modifications.

Note Seules des valeurs négatives et nulles peuvent être configurées pour les paramètres de seuil de réputation de sites Web pour les politiques de sécurité des données de Cisco. Par définition, toutes les évaluations positives sont surveillées

Intégration de l'appliance à la console Secure Endpoint AMP for Endpoints

Vous pouvez intégrer votre appliance à la console Secure Endpoint et effectuer les actions suivantes dans la console de Secure Endpoint :

- Créez une liste de détection personnalisée simple.
- Ajoutez de nouvelles informations SHA de fichiers malveillants à la liste de détection personnalisée simple.
- Créez une liste des applications autorisées.
- Ajoutez de nouvelles informations SHA de fichiers à la liste des applications autorisées.
- Créez une politique personnalisée.
- Associez la liste de détection personnalisée simple et la liste des applications autorisées à la politique personnalisée.
- Créez un groupe personnalisé.
- Associez la politique personnalisée au groupe personnalisé.
- Déplacez votre appliance enregistrée du groupe par défaut vers le groupe personnalisé.
- Affichez les détails de la trajectoire de fichier des informations SHA d'un fichier particulier.

Pour intégrer votre appliance à la console Secure Endpoint, vous devez enregistrer votre appliance auprès de la console.

Après l'intégration, quand les informations SHA du fichier sont envoyées au serveur de réputation des fichiers, le verdict obtenu pour les informations SHA du fichier à partir du serveur de réputation des fichiers est remplacé par le verdict déjà disponible pour les mêmes informations SHA du fichier dans la console Cisco Secure Endpoint.

Si un fichier SHA est déjà marqué comme malveillant dans le monde et si le même SHA de fichier est ajouté à la liste de blocage dans la console Secure Endpoint, la disposition du fichier est malveillante.

La page de rapport Cisco Secure Endpoint comprend une nouvelle section **Incoming Malware Files by Category** (Fichiers malveillants entrants par catégorie) pour afficher le pourcentage d'informations SHA du fichier de la liste de blocage reçues de la console Secure Endpoint qui sont affichés comme **Custom Detection** (Détection personnalisée). Le nom de menace d'informations SHA du fichier de la liste de blocage est affiché comme **Simple Custom Detection** (Détection personnalisée simple) dans la section des fichiers de programmes malveillants entrants du rapport. Vous pouvez cliquer sur le lien dans la section More Details (Plus de détails) du rapport pour afficher les détails de la trajectoire des informations SHA d'un fichier de la liste de blocage dans la console Secure Endpoint.

La page de rapport Cisco Secure Endpoint comprend une nouvelle section **Incoming Malicious Files by Category** (Fichiers malveillants entrants par catégorie) pour afficher le pourcentage d'informations SHA du fichier de la liste de blocage reçues de la console de la console Secure Endpoint qui sont affichées comme **Custom Detection** (Détection personnalisée). Le nom de menace des informations SHA d'un fichier de la liste de blocage s'affiche comme **Détection personnalisée** dans la section Malicious Threat Files (Fichiers de programmes malveillants) du rapport. Pour afficher les détails de la trajectoire des informations SHA d'un fichier de la liste de blocage dans la console Secure Endpoint, consultez #unique_459.

Avant de commencer

Assurez-vous d'avoir un compte d'utilisateur dans la console Cisco Secure Endpoint avec des droits d'accès admin. Pour en savoir plus sur la création d'un compte d'utilisateur sur la console Cisco Secure Endpoint, communiquez avec le service d'assistance technique de Cisco.

[Pour une configuration en grappe] Dans une configuration en grappe, vous pouvez uniquement enregistrer l'appliance connectée auprès de la console Secure Endpoint. Si vous avez déjà enregistré votre appliance auprès de la console Secure Endpoint en mode autonome, veillez à annuler l'enregistrement de l'appliance manuellement avant de l'associer à une grappe.

Assurez-vous d'avoir activé et configuré le filtrage de réputation des fichiers. Consultez la section Activation et configuration des services de réputation et d'analyse des fichiers pour savoir comment activer et configurer le filtrage de réputation des fichiers.

Étape 1 Sélectionnez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Cliquez sur **Register Appliance with** Secure Endpoint (Enregistrer l'appliance auprès de Secure Endpoint) pour obtenir la réputation du fichier dans la page File Reputation and File Analysis (Réputation des fichiers et analyse des fichiers) de l'interface Web.

Lorsque vous avez cliqué sur Register Appliance with Secure Endpoint (Enregistrer l'appliance auprès de Secure Endpoint), la page de connexion de la console Secure Endpoint s'affiche.

Étape 4 Cliquez sur **Register Appliance with** Secure Endpoint (Enregistrer l'appliance auprès de Cisco Secure Endpoint) dans le volet Advanced Settings (Paramètres avancés) pour la réputation des fichiers sur la page Anti-Malware and Reputation (Protection contre les programmes malveillants et réputation) de l'interface Web.

Lorsque vous avez cliqué sur Register Appliance with Secure Endpoint (Enregistrer l'appliance auprès de Secure Endpoint), la page de connexion de la console Secure Endpoint s'affiche.

Remarque Vous devez activer et configurer le filtrage de réputation de fichiers avant d'enregistrer l'appliance auprès de Secure Endpoint. Consultez la section sur l'activation et la configuration des services de réputation et d'analyse des fichiers pour savoir comment activer et configurer le filtrage de réputation des fichiers.

Étape 5 Connectez-vous à la console Cisco Secure Endpoint avec vos informations d'identification utilisateur.

Étape 6 Cliquez sur **Allow** (Autoriser) dans la page d'autorisation de Secure Endpoint pour enregistrer votre appliance.

Une fois que vous avez cliqué sur Allow (Autoriser), l'enregistrement est terminé et vous êtes redirigé vers la page de réputation de la protection contre les programmes malveillants de votre appliance. Le nom de votre appliance s'affiche dans le champ d'intégration de la console Cisco Secure Endpoint. Vous pouvez utiliser le nom de l'appliance pour personnaliser les paramètres de votre appliance dans la page de la console Secure Endpoint.

Prochaine étape

Prochaines étapes :

- Vous pouvez accéder à la section Accounts > Applications (Comptes > Applications) de la page de la console Cisco Secure Endpoint afin de vérifier si votre appliance est enregistrée auprès de la console Cisco Secure Endpoint. Le nom de votre appliance s'affiche dans la section Applications de la page de la console Cisco Secure Endpoint.
- Après l'enregistrement, votre appliance est ajouté au groupe par défaut (Groupe d'audit) auquel une politique par défaut (Politique réseau) est attachée. La politique par défaut contient les informations SHA du fichier qui sont ajoutées à la liste de blocage ou à la liste des autorisations. Si vous souhaitez personnaliser les paramètres de Cisco Secure Endpoint pour votre appliance et ajouter vos propres informations SHA du fichier qui sont ajoutées à la liste des blocages ou à la liste des autorisations, consultez la documentation de l'utilisateur Cisco Secure Endpoint dans https://console.amp.cisco.com/docs.
- Pour annuler l'enregistrement de la connexion de votre appliance auprès de la console Cisco Secure Endpoint, vous pouvez cliquer sur **Deregister** (Annuler l'enregistrement) dans la section Advanced Settings for File Reputation (Paramètres avancés de réputation des fichiers) de votre appliance ou vous devez vous rendre à la page de la console Cisco Secure Endpoint à l'adresse https://console.amp.cisco.com/ . Pour en savoir plus, consultez la documentation utilisateur de Secure Endpoint à l'adresse https://console.amp.cisco.com/docs.

Remarque Lorsque vous changez votre serveur de réputation des fichiers dans un autre centre de données, l'enregistrement de votre appliance est automatiquement annulé dans la console Secure Endpoint. Vous devez réenregistrer votre appliance auprès de la console Secure Endpoint avec le même centre de données que celui qui a été sélectionné pour le serveur de réputation des fichiers.

Remarque Si les informations SHA d'un fichier malveillant obtient un verdict sain, vérifiez si les mêmes informations SHA du fichier sont ajouté à la liste des autorisations dans la console Secure Endpoint.

Gestion des tableaux de base de données

Les bases de données de réputation de sites Web, Webroot, Sophos et McAfee reçoivent régulièrement des mises à jour du serveur de mise à jour Cisco. Les mises à jour du serveur sont automatisées et l'intervalle des mises à jour est défini par le serveur.

Base de données sur la réputation Web

Secure Web Appliance gère une base de données de filtrage qui contient des statistiques et des renseignements sur le traitement des différents types de demandes. L'appliance peut également être configurée pour envoyer des statistiques de réputation Web à un serveur du réseau Cisco SensorBase. Les informations du serveur SensorBase sont exploitées avec des flux de données du réseau SensorBase et les informations sont utilisées pour produire un score de réputation Web.

Journalisation de l'activité de filtrage de la réputation Web et de l'analyse DVS

Le fichier journal des accès enregistre les informations renvoyées par les filtres de réputation Web et le moteur DVS pour chaque transaction. La section des renseignements sur le verdict d'analyse dans les journaux d'accès comprend de nombreux champs pour aider à comprendre la cause de l'action appliquée à une transaction. Par exemple, certains champs affichent le score de réputation Web ou le verdict de recherche de programmes malveillants transmis par Sophos au moteur DVS.

Journalisation de l'analyse adaptative

Champ personnalisé dans les journaux d'accès	Champ personnalisé dans les journaux W3C	Description
%X6	x-as-malware-threat-name	Le nom de la solution antiprogramme malveillant renvoyé par l'analyse adaptative. Si la transaction n'est pas bloquée, ce champ renvoie un tiret (« - »). Cette variable est incluse dans les informations sur le verdict de l'analyse (entre les crochets à la fin de chaque entrée du journal des accès).

Les transactions bloquées et surveillées par le moteur d'analyse adaptative utilisent les balises de décision d'ACL :

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

Caching (Mise en mémoire cache)

Les directives suivantes expliquent comment AsyncOS utilise le cache lors de la recherche de programmes malveillants :

- AsyncOS ne met en cache les objets que si l'objet entier est téléchargé. Si le programme malveillant est bloqué pendant l'analyse, l'objet entier n'est pas téléchargé et, par conséquent, n'est pas mis en cache.
- AsyncOS analyse le contenu, qu'il soit récupéré depuis le serveur ou le cache Web.
- La durée pendant laquelle le contenu est mis en cache varie en fonction de nombreux facteurs. Il n'y a pas de valeur par défaut.
- AsyncOS analyse de nouveau le contenu lorsque les signatures sont mises à jour.

Descriptions des catégories de programmes malveillants

Type de maliciel	Description
Logiciels publicitaires	Les logiciels publicitaires englobent tous les exécutables logiciels et les modules d'extension qui dirigent les utilisateurs vers les produits à vendre. Ces programmes peuvent également modifier les paramètres de sécurité, en empêchant les utilisateurs de modifier les paramètres système.
Objet de l'assistant du navigateur	Un objet assistant de navigateur est un module d'extension de navigateur qui peut remplir diverses fonctions liées à la diffusion de publicités ou au détournement de paramètres utilisateur.
Supervision de système commercial	Un moniteur système commercial est un logiciel ayant les caractéristiques d'un moniteur système qui peut être obtenu avec une licence légitime par des moyens légaux.
Composeur automatique	Un composeur est un programme qui utilise votre modem ou un autre type d'accès Internet pour vous connecter à une ligne téléphonique ou à un site qui vous fait accumuler des frais d'interurbain pour lesquels vous n'avez pas donné votre plein consentement.
Logiciel espion générique	Un logiciel espion est un type de programme malveillant installé sur les ordinateurs qui recueille de petits éléments d'information sur les utilisateurs à l'insu des utilisateurs.
Détournement d'identité	Un pirate modifie les paramètres système ou toutes les modifications indésirables apportées au système d'un utilisateur qui peut le diriger vers un site Web ou exécuter un programme sans le consentement de l'utilisateur.
Fichiers malveillants ou à risque élevé connus	Il s'agit de fichiers qui ont été identifiés comme des menaces par le service de réputation de fichiers Cisco Secure Endpoint.
Autres programmes malveillants	Cette catégorie est utilisée pour détecter tous les autres programmes malveillants et comportements suspects qui n'entrent pas exactement dans l'une des autres catégories définies.

Type de maliciel	Description
URL d'hameçonnage	Une URL d'hameçonnage s'affiche dans la barre d'adresse du navigateur. Dans certains cas, elle implique l'utilisation de noms de domaine et ressemble à celle de domaines légitimes.
API (applications potentiellement indésirables)	Application potentiellement indésirable. Un PUA est une application qui n'est pas malveillante, mais qui peut être considérée comme indésirable.
Moniteur système	Un moniteur système englobe tout logiciel qui effectue l'une des opérations suivantes : • Enregistre ouvertement ou secrètement les processus du système et/ou les actions de l'utilisateur; • Rend ces enregistrements disponibles pour la récupération et l'examen ultérieurement.
Outil de téléchargement de chevaux de Troie	Un logiciel de téléchargement de chevaux de Troie désigne un cheval de Troie qui, après son installation, communique avec un hôte ou un site distant et installe des paquets ou des sociétés affiliées à partir de l'hôte distant.
Cheval de Troie	Un cheval de Troie est un programme destructeur qui se fait passer pour une application inoffensive. Contrairement aux virus, les chevaux de Troie ne se reproduisent pas.
Cheval de Troie pour hameçonnage	Un cheval de Troie pour hameçonnage peut rester sur un ordinateur infecté en attendant la visite d'une page Web spécifique ou peut analyser l'ordinateur infecté à la recherche de noms d'utilisateur et de phrases secrètes.
Virus	Un virus est un programme ou un élément de code qui est chargé sur votre ordinateur à votre insu.
Vers	Un ver est un programme ou un algorithme qui se reproduit sur un réseau informatique et qui effectue des actions malveillantes.

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.