Analyser le trafic sortant à la recherche d'infections existantes

Cette rubrique contient les sections suivantes :

Survol de l'analyse du trafic sortant

Pour empêcher des données malveillantes de quitter le réseau, le Secure Web Appliance fournit la fonctionnalité d'analyse des programmes malveillants sortants. Les groupes de politiques vous permettent de définir quels téléchargements sont analysés à la recherche de programmes malveillants, quels moteurs d'analyse utiliser pour l'analyse et quels types de programmes malveillants bloquer.

Le moteur de conversion en flux continu et vecteur dynamique de Cisco (DVS) analyse les demandes de transaction dès qu'elles quittent le réseau. En fonctionnant avec le moteur Cisco DVS, le Secure Web Appliance vous permet d'empêcher les utilisateurs de charger involontairement des données malveillantes.

Vous pouvez effectuer les tâches suivantes:

Tâche	Lien vers la tâche
Créer des politiques pour bloquer les programmes malveillants	Création de politiques d'analyse à la recherche de programmes malveillants sortants, on page 3
Affecter des demandes de téléchargement aux groupes de politiques sur les programmes malveillants sortants	Contrôle des demandes de chargement , on page 5

Expérience de l'utilisateur lorsque les demandes sont bloquées par le moteur DVS

Lorsque le moteur Cisco DVS bloque une demande de chargement, le proxy Web envoie une page de blocage à l'utilisateur final. Cependant, tous les sites Web n'affichent pas la page de blocage à l'utilisateur final. Certains sites Web 2.0 affichent du contenu dynamique en utilisant Javascript au lieu d'une page Web statique et il est peu probable qu'ils affichent la page de blocage. Les utilisateurs sont toujours correctement empêchés de charger des données malveillantes, mais ils ne sont pas toujours informés par le site Web.

Interprétation des demandes de chargement

Les politiques d'analyse des programmes malveillants sortants définissent si le proxy Web bloque les requêtes HTTP et les connexions HTTPS déchiffrées pour les transactions qui téléchargent des données vers un serveur (demandes de téléchargement). Une demande de téléchargement est une demande HTTP ou HTTPS déchiffré dont le corps a du contenu.

Lorsque le proxy Web reçoit une demande de téléchargement, il la compare aux groupes de politiques des groupes de politiques d'analyse des programmes malveillants sortants afin de déterminer le groupe de politiques à appliquer. Après avoir affecté la demande à un groupe de politiques, il compare la demande aux paramètres de contrôle configurés du groupe de politiques pour déterminer s'il faut bloquer la demande ou surveiller la demande. Lorsqu'une politique d'analyse des programmes malveillants sortants détermine la supervision d'une demande, celle-ci est évaluée par rapport aux politiques d'accès, et l'action finale implémentée par le proxy Web sur la demande est déterminée par la politique d'accès.

Note Les demandes de téléchargement qui tentent de charger des fichiers d'une taille de zéro (0) octet ne sont pas évaluées par rapport aux politiques d'analyse des programmes malveillants sortants.

Critères d'appartenance à un groupe

Chaque demande client est affectée à une identité et est ensuite évaluée par rapport aux autres types de politiques afin de déterminer à quel groupe de politiques elle appartient pour chaque type. Le proxy Web applique les paramètres de contrôle de politiques configurés à une demande d'un client en fonction de l'appartenance au groupe de politiques de la demande.

Le proxy Web suit un processus précis pour correspondre aux critères d'appartenance au groupe. Il prend en compte les facteurs suivants pour l'appartenance à un groupe :

Critère	Description
Identification Profile (Profil d'identification)	Chaque demande de client correspond à un **profil d'identification**, échoue à l'authentification et obtient l'accès invité, ou échoue à l'authentification et est terminée.

Critère	Description
Authorized users (Utilisateurs autorisés).	Si le **profil d'identification** attribué nécessite une authentification, l'utilisateur doit être dans la liste des utilisateurs autorisés dans le groupe de politiques de l'analyse des programmes malveillants sortants pour correspondre au groupe de politiques. La liste d'utilisateurs autorisés peut comprendre n'importe quel groupe ou utilisateur précisé ou peut être des utilisateurs invités si le **profil d'identification** permet l'accès comme invité.
Advanced options (Options avancées)	Vous pouvez configurer plusieurs options avancées pour l'appartenance au groupe de politiques d'analyse des programmes malveillants sortants. Certaines options, telles que le port proxy et la catégorie d'URL, peuvent également être définies dans le **profil d'identification**. Lorsqu'une option avancée est configurée dans le **profil d'identification**, elle n'est pas configurable au niveau de groupe de la Politique d'analyse des programmes malveillants sortants.

Mise en correspondance des demandes des clients et des groupes de politiques d'analyse à la recherche de programmes malveillants sortants

Le proxy Web compare l'état de la demande de chargement aux critères d'appartenance au premier groupe de politiques. S'ils correspondent, le proxy Web applique les paramètres de politique de ce groupe de politiques.

S'ils ne correspondent pas, le proxy Web compare la demande de chargement au groupe de politiques suivant. Il poursuit ce processus jusqu'à ce qu'il fasse correspondre la demande de chargement à un groupe de politiques défini par l'utilisateur. S'il ne correspond pas à un groupe de politiques défini par l'utilisateur, il correspond au groupe de politiques global. Lorsque le proxy Web fait correspondre la demande de chargement à un groupe de politiques ou au groupe de politiques global, il applique les paramètres de politiques de ce groupe de politiques.

Création de politiques d'analyse à la recherche de programmes malveillants sortants

Vous pouvez créer des groupes de politiques d'analyse des programmes malveillants sortants en fonction de combinaisons de plusieurs critères, comme une ou plusieurs identités ou la catégorie d'URL du site de destination. Vous devez définir au moins un critère d'appartenance à un groupe de politiques. Lorsque vous définissez plusieurs critères, la demande de chargement doit satisfaire à tous les critères pour correspondre au groupe de politiques. Cependant, la demande de chargement ne doit correspondre qu'à l'une des identités configurées.

Étape 1 Choisissez **Web Security Manager > Outbound Malware Scanning** (Web Security Manager > Analyse des programmes malveillants sortants).

Étape 2 Cliquez sur **Add Policy** (Ajouter une politique).

Étape 3 Saisissez un nom et une description facultative pour le groupe de politiques.

Note Chaque nom de groupe de politiques doit être unique et contenir uniquement des caractères alphanumériques ou un espace.

Étape 4 Dans le champ Insert Above Policy (Insérer au-dessus de la politique), sélectionnez l'emplacement dans le tableau des politiques où insérer le groupe de politiques.

Lors de la configuration de plusieurs groupes de politiques, vous devez préciser un ordre logique pour chaque groupe.

Étape 5 Dans la section **Identification Profiles and Users** (Profils d'identification et utilisateurs), sélectionnez un ou plusieurs groupes d'identité à appliquer à ce groupe de politiques.

Étape 6 (Facultatif) Développez la section « Advanced » (Avancé) pour définir les exigences d'appartenance supplémentaires.

Étape 7 Pour définir l'appartenance à un groupe de politiques en fonction des options avancées, cliquez sur le lien de l'option avancée et configurez l'option dans la page qui s'affiche.

Option avancée	Description
Protocols (Protocoles)	Choisissez de définir ou non l'appartenance au groupe de politiques par le protocole utilisé dans la demande du client. Sélectionnez les protocoles à inclure. « All others » (Tous les autres) désigne tout protocole non répertorié au-dessus de cette option. **Note** Lorsque le proxy HTTPS est activé, seules les politiques de déchiffrement s'appliquent aux transactions HTTPS. Vous ne pouvez pas définir l'appartenance aux politiques à l'aide du protocole HTTPS pour les politiques d'accès, de routage, d'analyse des programmes malveillants sortants, de sécurité des données ou DLP externes.
Proxy Ports (Ports du proxy)	Choisissez de définir ou non l'appartenance au groupe de politiques par le port de proxy utilisé pour accéder au proxy Web. Entrez un ou plusieurs numéros de port dans le champ Proxy Ports (Ports du proxy). Séparez les valeurs de ports multiples par des virgules. Pour les connexions de transfert explicite, il s'agit du port configuré dans le navigateur. Pour les connexions transparentes, il s'agit du même port de destination. Si vous définissez l'appartenance à un groupe de politiques par le port proxy lorsque les demandes des clients sont redirigées de manière transparente vers l'appliance, certaines demandes peuvent être refusées. **Note** Si l'identité associée à ce groupe de politiques définit l'appartenance à l'identité par ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques autre que l'identité.
Subnets (Sous-réseaux)	Choisissez de définir ou non l'appartenance au groupe de politiques par sous-réseau ou autres adresses. Vous pouvez choisir d'utiliser les adresses qui peuvent être définies avec l'identité associée ou vous pouvez entrer des adresses spécifiques ici. **Note** Si l'identité associée à ce groupe de politiques définit ses membres par des adresses, alors vous devez saisir dans ce groupe de politiques des adresses qui sont un sous-ensemble des adresses définies dans l'identité. L'ajout d'adresses dans le groupe de politiques réduit davantage la liste des transactions qui correspondent à ce groupe de politiques.
URL Categories (Catégories d'URL)	Choisissez de définir ou non l'appartenance au groupe de politiques par catégories d'URL. Sélectionnez les catégories d'URL prédéfinies ou définies par l'utilisateur. **Note** Si l'identité associée à ce groupe de politiques définit l'appartenance à l'identité par ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques autre que l'identité.

Option avancée	Description
User Agents (Agents utilisateur)	Choisissez si vous souhaitez définir l'appartenance au groupe de politiques en fonction des agents utilisateur (applications clientes telles que les programmes de mise à jour et les navigateurs Web) utilisés dans la demande du client. Vous pouvez sélectionner des agents utilisateur couramment définis ou définir les vôtres à l'aide d'expressions régulières. Indique si la définition d'appartenance inclut uniquement les agents utilisateur sélectionnés ou exclut expressément les agents utilisateur sélectionnés. **Note** Si le **profil d'identification** associé à ce groupe de politiques définit l'appartenance au **profil d'identification** en fonction de ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques sans **profil d'identification**.
User Location (Emplacement de l'utilisateur)	Choisissez de définir ou non l'appartenance au groupe de politiques par emplacement d'utilisateur, distant ou local.

Étape 8 Envoyez vos modifications.

Étape 9 Configurez les paramètres de contrôle de groupe de la politique d'analyse des programmes malveillants sortants pour définir la façon dont le proxy Web gère les transactions.

Le nouveau groupe de politiques d'analyse des programmes malveillants sortants hérite automatiquement des paramètres globaux du groupe de politiques jusqu'à ce que vous configuriez des options pour chaque paramètre de contrôle.

Étape 10 Envoyez et validez les modifications.

Contrôle des demandes de chargement

Chaque demande de téléchargement est affectée à un groupe de politiques d'analyse des programmes malveillants sortants et hérite des paramètres de contrôle de ce groupe de politiques. Une fois que le proxy Web a reçu les en-têtes de la demande de chargement, il dispose des informations nécessaires pour décider s'il doit analyser le corps de la demande. Le moteur DVS analyse la demande et renvoie un verdict au proxy Web. La page de blocage s'affiche pour l'utilisateur final, le cas échéant.

Étape 1 Choisissez **Web Security Manager > Outbound Malware Scanning** (Web Security Manager > Analyse des programmes malveillants sortants).

Étape 2 Dans la colonne **Destinations**, cliquez sur le lien correspondant au groupe de politiques que vous souhaitez configurer.

Étape 3 Dans la section **Edit Destination Settings** (Modifier les paramètres de destination), sélectionnez **Define Destinations Scanning Custom Settings** (Définir les paramètres personnalisés d'analyse de destination) dans le menu déroulant.

Étape 4 Dans la section **Destinations to Scan** (Destinations à analyser), sélectionnez l'une des options suivantes :

Option	Description
Do not scan any uploads (Ne pas analyser les téléchargements)	Le moteur DVS n'analyse aucune demande de téléchargement. Toutes les demandes de téléchargement sont évaluées par rapport aux politiques d'accès

Option	Description
Scan all uploads (Analyser tous les chargements)	Le moteur DVS analyse toutes les demandes de téléchargement. La demande de téléchargement est bloquée ou évaluée par rapport aux politiques d'accès, selon le verdict d'analyse du moteur DVS
Scan uploads to specified custom URL categories (Analyser les téléchargements vers des catégories d'URL personnalisées précisées)	Le moteur DVS analyse les demandes de chargement qui appartiennent à des catégories d'URL personnalisées spécifiques. La demande de téléchargement est bloquée ou évaluée par rapport aux politiques d'accès, selon le verdict d'analyse du moteur DVS. Cliquer sur **Edit custom categories list** (Modifier la liste des catégories personnalisées) pour sélectionner les catégories d'URL à analyser.

Étape 5 Envoyez vos modifications.

Étape 6 Dans la colonne **Anti-Malware Filtering** (Filtrage des programmes malveillants), cliquez sur le lien du groupe de politiques.

Étape 7 Dans la section **Anti-Malware Settings** (Paramètres de protection contre les programmes malveillants), sélectionnez **Define Anti-Malware Custom Settings** (Définir les paramètres personnalisés de la protection contre les programmes malveillants).

Étape 8 Dans la section **Cisco DVS Anti-Malware Settings** (Paramètres de protection contre les programmes malveillants Cisco DVS), sélectionnez les moteurs d'analyse de protection contre les programmes malveillants à activer pour ce groupe de politiques.

Étape 9 Dans la section **Malware Catégories** (Catégories de programmes malveillants), sélectionnez si vous souhaitez surveiller ou bloquer les différentes catégories de programmes malveillants.

Les catégories répertoriées dans cette section dépendent des moteurs d'analyse que vous activez.

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 10 Envoyez et validez les modifications.

Journalisation de l'analyse DVS

Les journaux d'accès indiquent si le moteur DVS a analysé ou non une demande de téléchargement à la recherche de programmes malveillants. La section du verdict d'analyse de chaque entrée du journal des accès comprend des valeurs pour l'activité du moteur DVS pour les téléchargements analysés. Vous pouvez également ajouter l'un des champs aux journaux d'accès ou W3C pour trouver plus facilement l'activité de ce moteur DVS :

Table 1: Champs de journalisation dans les journaux W3C et spécificateurs de format dans les journaux d'accès

Champ de journalisation W3C	Spécificateur de format dans les journaux d'accès
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4

Champ de journalisation W3C	Spécificateur de format dans les journaux d'accès
x-req-dvs-verdictname	%X3

Lorsque le moteur DVS marque une demande de téléchargement comme étant un programme malveillant et qu'il est configuré pour bloquer les téléchargements de programmes malveillants, la balise de décision ACL dans les journaux d'accès est BLOCK_AMW_REQ.

Cependant, lorsque le moteur DVS marque une demande de téléchargement comme étant un programme malveillant et qu'il est configuré pour *surveiller* les téléchargements de programmes malveillants, la balise de décision dans les journaux d'accès est en fait déterminée par la politique d'accès appliquée à la transaction.

Pour déterminer si le moteur DVS a analysé une demande de téléchargement à la recherche de programmes malveillants, affichez les résultats de l'activité du moteur DVS dans la section des renseignements sur le verdict d'analyse de chaque entrée du journal des accès.

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.