Comment bloquer des applications inconnues sur un dispositif Web sécurisé

Contenu

Introduction

Ce document décrit plusieurs méthodes pour bloquer des applications inconnues sur Cisco Secure Web Appliance.

Méthodes de blocage des applications inconnues

Vous pouvez utiliser l'une de ces méthodes seule ou en combinaison.

> **Note**: Cet article de la base de connaissances se rapporte à un logiciel qui n'est pas mis à jour ou pris en charge par Cisco. Les informations sont fournies comme courtoisie pour votre commodité. Pour plus d'assistance, communiquez avec le fournisseur du logiciel.

Bloquer les applications en fonction des chaînes d'agents utilisateur

La première défense consiste à utiliser des chaînes d'agent utilisateur pour bloquer les applications inconnues.

- Ajouter l'agent utilisateur sous **Web Security Manager** > **Access Policies** > **Protocols and User Agents** colonne <pour la stratégie d'accès requise>.
- Ajouter la chaîne Agent utilisateur sous **Block Custom User Agents** (un par ligne).

> **Note**: Vous pouvez utiliser les liens fournis sous Référence pour rechercher des agents utilisateur.

Bloquer les applications en fonction des contrôles de visibilité des applications

Si les contrôles de visibilité sur les applications (AVC) sont activés (sous **GUI > Security Services > Web Reputation and Anti-Malware**), vous pouvez ensuite bloquer l'accès en fonction des types d'applications tels que les serveurs proxy, le partage de fichiers, les utilitaires Internet, etc. Vous pouvez faire ceci sous **Web Security Manager > Access Policies > Applications** colonne <pour la stratégie d'accès requise>.

Bloquer les applications en fonction du type MIME

Si l'agent utilisateur n'existe pas, vous pouvez essayer d'ajouter le type MIME (Multipurpose Internet Mail Extensions) :

- Ajouter des types MIME sous **Web Security Manager** > **Web Access Policies** > **Objects** colonne <pour la stratégie d'accès requise>.
- Ajoutez le type d'objet/MIME dans la **Block Custom MIME Types** (une par ligne). Par exemple, pour bloquer les applications BitTorrent, saisissez application/x-bittorrent.

  Note: Vous pouvez utiliser les liens fournis sous Référence pour rechercher des types MIME.

Bloquer les catégories d'URL dans les stratégies d'accès

Assurez-vous que les catégories telles que l'évitement des filtres, les activités illégales, les téléchargements illégaux, etc., sont bloquées dans les stratégies d'accès. Si certaines applications utilisent des URL ou des adresses IP connues pour leurs connexions, vous pouvez bloquer leurs catégories d'URL prédéfinies associées ou les configurer dans une catégorie d'URL personnalisée bloquée à l'aide de leur adresse IP, de leur nom de domaine complet (FQDN) ou d'un regex correspondant aux domaines. Vous pouvez faire ceci sous **Web Security Manager > Access Policies > URL Categories** colonne.

Restreindre la configuration des ports HTTP CONNECT dans la stratégie d'accès

Certaines applications peuvent utiliser la méthode HTTP CONNECT pour se connecter à différents ports. Autorisez uniquement les ports connus ou les ports spécifiques requis dans votre environnement dans les domaines de configuration des ports HTTP CONNECT :

- HTTP CONNECT peut être configuré sous **Web Security Manager** > **Access Policies** > **Protocols and User Agents** colonne <pour la stratégie d'accès requise>.
- Ajouter les ports autorisés sous **HTTP CONNECT Ports**.

Bloquer l'accès pour des adresses IP spécifiques

Pour les applications dont vous ne connaissez que les adresses IP de destination auxquelles vous accédez, vous pouvez utiliser la fonctionnalité Moniteur du trafic de couche 4 pour bloquer l'accès à ces adresses IP spécifiques. Vous pouvez ajouter les adresses IP de destination sous **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses**.

Comment trouver l'agent utilisateur ou le type MIME utilisé par une application

Si vous ne savez pas quel agent utilisateur ou quel type MIME est utilisé par certaines applications, vous pouvez effectuer l'une des étapes suivantes pour rechercher ces informations :

- Exécuter une capture de paquets avec WireShark (Ethereal) sur la machine du client et filtrer le protocole 'http'.
- Exécuter la capture sur Secure Web Appliance (sous **Support and Help** > **Packet Capture**), filtrée sur l'adresse IP du client.

Référence

> **Note**: Les sites Web externes répertoriés ici sont fournis à titre de référence uniquement. Les liens et le contenu ne sont pas contrôlés par Cisco et peuvent être modifiés.

Liste des agents utilisateur

User Agent String.Com (sur useragentstring.com)

Liste des types MIME

- Types MIME courants (sur mozilla.org)
- Types MIME : Liste complète des types MIME (sur w3cub.com)
- Liste complète des types MIME (sur site.com)