Bloquer le trafic de téléchargement dans l'appliance Web sécurisée

Table des matières

Introduction

Ce document décrit le processus de blocage du trafic de téléchargement vers certains sites Web dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès à l'interface utilisateur graphique (GUI) de SWA
- Accès administratif au SWA.

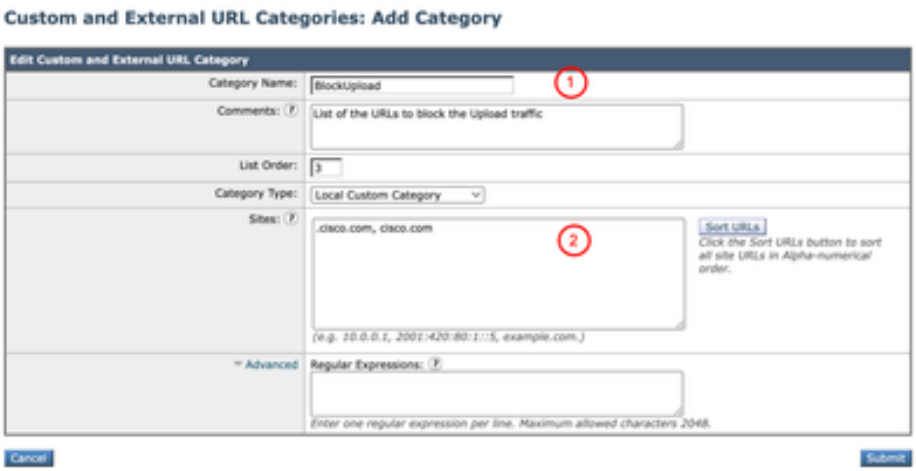
Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration Steps

Étape 1 : création d'une catégorie d'URL personnalisée	Étape 1.1. Dans l’interface graphique, accédez à Web Security Manager et sélectionnez Custom and External URL Categories.

pour le site Web	Étape 1.2. Cliquez sur Ajouter une catégorie pour créer une nouvelle catégorie d'URL personnalisée. Étape 1.3. Saisissez le nom de la nouvelle catégorie. Étape 1.4. Définissez le domaine et/ou les sous-domaines du site Web que vous essayez de bloquer le trafic de téléchargement (dans cet exemple, cisco.com et tous ses sous-domaines). Étape 1.5.Envoyer les modifications  Image - Créer une catégorie d'URL personnalisée Conseil : Pour plus d'informations sur la configuration des catégories d'URL personnalisées, consultez le site : https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html
Étape 2 : décryptage du trafic pour l'URL	Étape 2.1. À partir de l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Decryption Policies Étape 2.2. Cliquez sur Add Policy. Étape 2.3. Entrez le nom de la nouvelle stratégie. Étape 2.4. (Facultatif) Sélectionnez le profil d'identification auquel s'applique cette stratégie. Étape 2.5. Dans la section Définition de membre de stratégie, cliquez sur les liens Catégories d'URL pour ajouter la catégorie d'URL personnalisée. Étape 2.6. Sélectionnez la catégorie d'URL créée à l'étape 1.

Étape 2.7. Cliquez sur Submit.

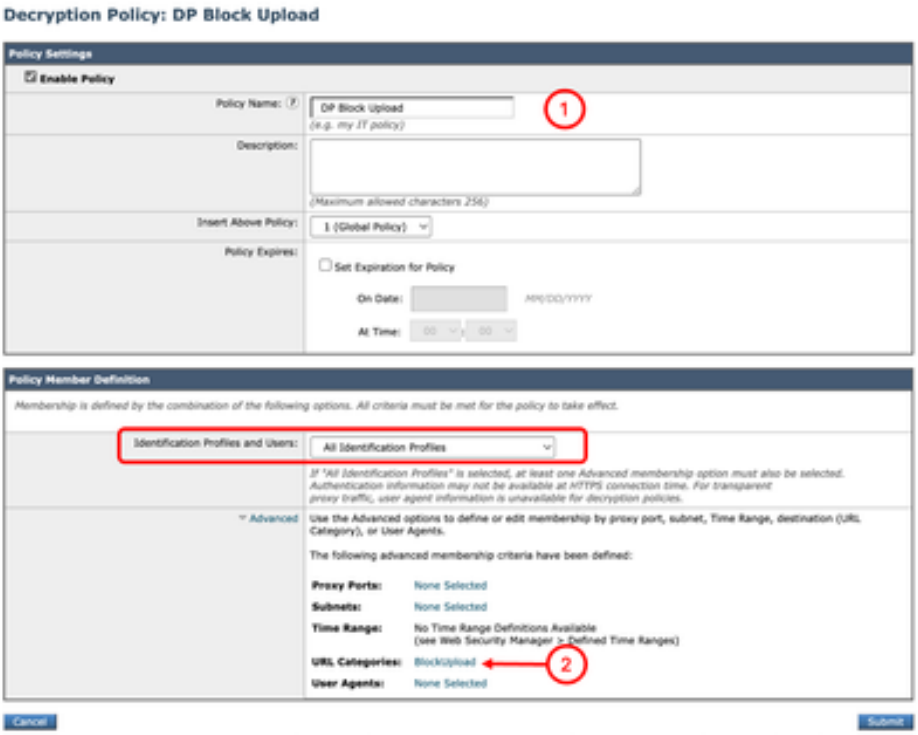


Image - Créer une stratégie de déchiffrement

Étape 2.8. Dans la page Stratégies de décodage, cliquez sur le lien du filtrage des URL pour la nouvelle stratégie.

Image : sélectionnez le filtrage des URL.

Étape 2.9. Choisissez Décrypter comme action pour la catégorie d'URL personnalisée.

Étape 2.10. Cliquez sur Submit.

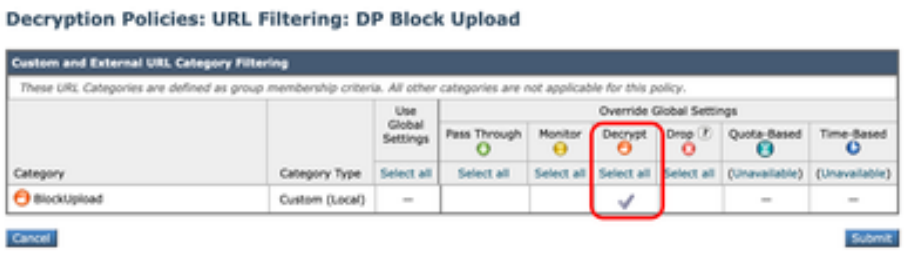


Image - Définir le déchiffrement comme action

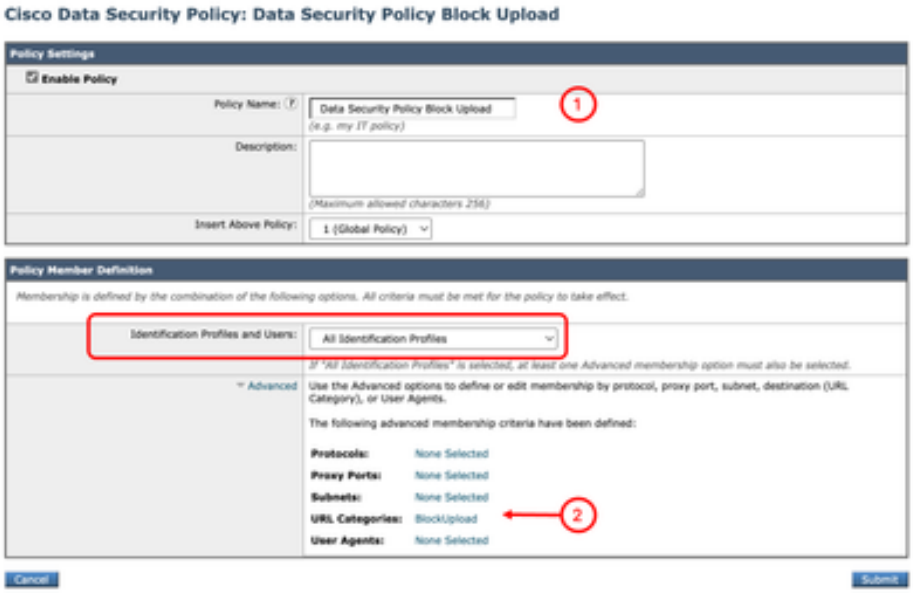
Étape 3 : blocage du trafic de téléchargement	Étape 3.1. Dans l'interface graphique utilisateur, accédez à Web Security Manager et sélectionnez Cisco Data Security. Étape 3.2. Cliquez sur Add Policy. Étape 3.3. Entrez le nom de la nouvelle stratégie. Étape 3.4. (Facultatif) Sélectionnez le profil d'identification auquel s'applique cette stratégie. Étape 3.5. Dans la section Définition de membre de stratégie, cliquez sur les liens Catégories d'URL pour ajouter la catégorie d'URL personnalisée. Étape 3.6. Sélectionnez la catégorie d'URL créée à l'étape 1. Étape 3.7. Cliquez sur Submit.  Image - Politique de sécurité des données Cisco Conseil : Pour les besoins du reporting, il est préférable de choisir un nom différent des autres politiques d'accès/décodage. Étape 3.8. Dans la page Cisco Date Security Policy, cliquez sur le lien du filtrage des URL pour la nouvelle stratégie. 

	Image : sélectionnez le filtrage des URL. Étape 3.9. Choisissez Block comme action pour Custom URL Category. Étape 3.10. Cliquez sur Submit.  Image - Bloquer le téléchargement Étape 3.11. Valider les modifications

Rapports et journaux

Journaux

Vous pouvez afficher les journaux associés au trafic de téléchargement à partir de l'interface de ligne de commande en choisissant idsdataloss_logs qui est le nom de journalisation par défaut pour les journaux de sécurité des données.

Pour accéder aux journaux, procédez comme suit :

Étape 1 : connexion à l'interface de ligne de commande

Étape 2. Tapez grep et appuyez sur Entrée.

Étape 3. Recherchez et tapez le numéro associé à idsdataloss_logs :

- type : "Journaux de sécurité des données"
- Récupération : Sondage FTP et appuyez sur Entrée.

Étape 4. (Facultatif) Entrez l'expression régulière pour grep vous ventilateur filtrer par mots clés, ou vous pouvez appuyer sur Entrée, pour afficher tous les journaux

Étape 5. (Facultatif) Voulez-vous que cette recherche ne respecte pas la casse ? [Y]> Si vous sélectionnez un mot-clé à l'étape 4, vous pouvez choisir que le filtre ne respecte pas la casse ou ne le respecte pas.

Étape 6. (Facultatif) Voulez-vous rechercher les lignes qui ne correspondent pas ? [N]> Si vous devez filtrer tous les journaux, à l'exception des mots-clés sélectionnés définis à l'étape 4, vous pouvez utiliser cette section. Sinon, vous pouvez appuyer sur Entrée.

Étape 7. (Facultatif) Voulez-vous suivre les journaux ? [N]> Si vous devez afficher les journaux en direct, tapez Y et appuyez sur Entrée. Sinon, appuyez sur Entrée pour afficher tous les journaux disponibles.

Étape 8. (Facultatif) Voulez-vous paginer le résultat ? [N]> Si vous devez afficher les résultats par page, vous pouvez taper Y et appuyer sur Entrée, sinon appuyez sur Entrée pour utiliser la valeur par défaut [N].

Rapports

Vous pouvez générer un rapport de suivi Web pour afficher les rapports du trafic de chargement bloqué par le nom de la stratégie de sécurité des données Cisco.

Pour générer les rapports, procédez comme suit :

Étape 1. Dans l'interface utilisateur graphique, sélectionnez Reporting et choisissez Web Tracking.

Étape 2. Choisissez la plage horaire souhaitée.

Étape 3. Cliquez sur le lien Avancé pour rechercher des transactions à l'aide de critères avancés.

Étape 4. Dans la section Stratégie, sélectionnez Filtrer par stratégie et tapez le nom de la sécurité des données Cisco qui a été créée précédemment.

Étape 5. Cliquez sur Rechercher pour consulter le rapport.

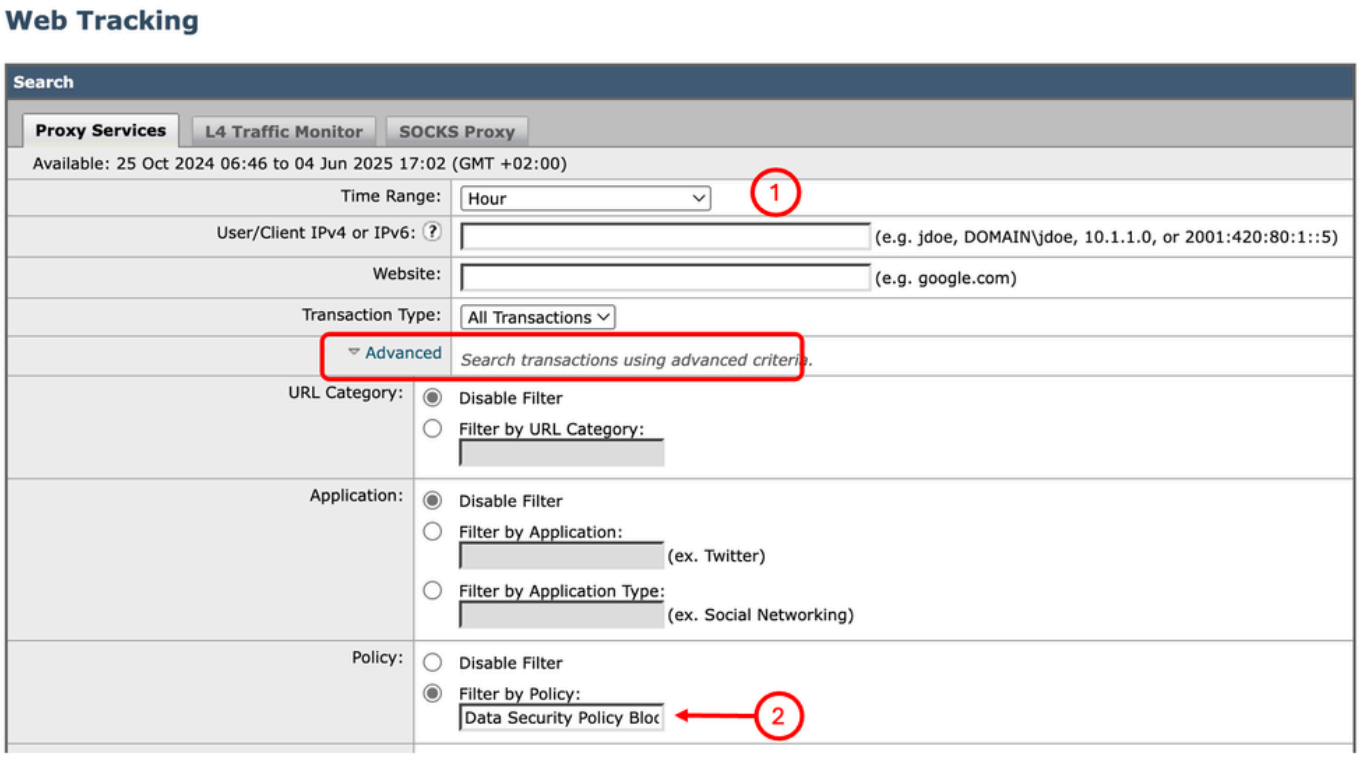


Image - Filtrage des rapports de suivi Web

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance
- Guide d'installation de l'appliance virtuelle Cisco Secure Email and Web
- Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco
- Utilisation des meilleures pratiques de sécurisation des appliances Web
- Configurer le pare-feu pour l'appliance Web sécurisée
- Configurer le certificat de déchiffrement dans l'appareil Web sécurisé
- Configuration et dépannage du protocole SNMP dans SWA
- Configuration des journaux de transmission SCP dans l'appliance Web sécurisée avec Microsoft Server
- Activer une chaîne/vidéo YouTube spécifique et bloquer le reste de YouTube dans SWA
- Comprendre le format de journal d'accès HTTPS dans l'appliance Web sécurisée
- Accéder aux journaux de l'appliance Web sécurisée
- Contourner l'authentification dans l'appliance Web sécurisée
- Bloquer le trafic dans l'appliance Web sécurisée
- Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.