Bloquer le téléchargement de fichiers exécutables dans SWA

Table des matières

Introduction

Ce document décrit le processus de configuration de Secure Web Appliance (SWA) pour bloquer le téléchargement de fichiers exécutables.

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.

Avant de commencer

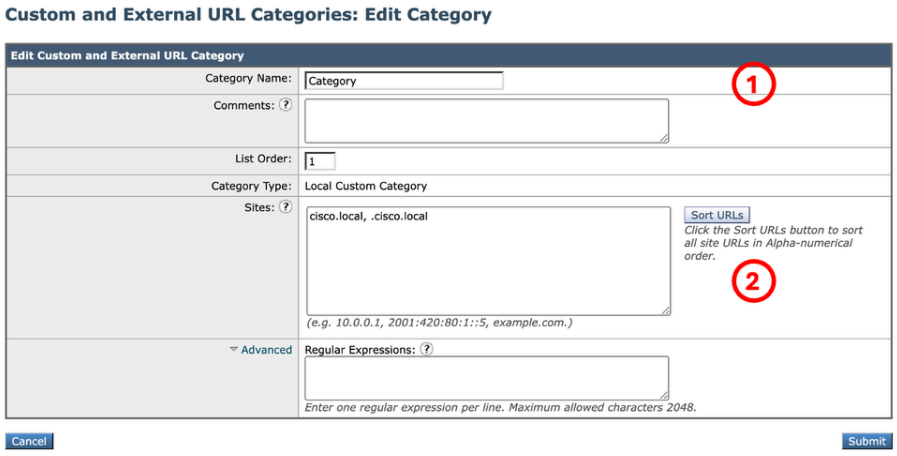
Cisco SWA peut bloquer efficacement le téléchargement de fichiers exécutables en inspectant le type de contenu Web MIME (Multipurpose Internet Mail Extensions). En identifiant des types de fichiers tels que application/x-msdownload, application/x-msi et d'autres types MIME associés, SWA applique des politiques qui empêchent l'exécution de fichiers exécutables aux utilisateurs.

En plus de la détection de type MIME, SWA peut tirer parti du filtrage des extensions de fichiers, de l'analyse basée sur la réputation et des règles de stratégie personnalisées pour renforcer la protection contre les téléchargements indésirables ou risqués. Ces fonctionnalités aident les entreprises à maintenir un environnement de navigation sécurisé et à réduire les risques d'infection par des programmes malveillants.

Conseil : SWA ne peut pas identifier le type MIME du fichier, sauf si le trafic est déchiffré.

application/octet-stream est un type MIME générique utilisé pour indiquer qu'un fichier contient des données binaires. Il ne spécifie pas la nature du fichier, il peut donc être utilisé pour n'importe quel fichier qui ne correspond pas à un type MIME plus spécifique. Ce type est généralement attribué aux fichiers exécutables, aux programmes d'installation et à d'autres fichiers non textuels lorsque le serveur Web ne peut pas déterminer un type plus précis.

Configuration Steps

Étape 1.Créez une catégorie d'URL personnalisée pour le site Web.	Étape 1.1.Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Custom and External URL Categories. Étape 1.2.Cliquez sur Ajouter une catégorie pour créer une nouvelle catégorie d'URL personnalisée. Étape 1.3.EnterName pour 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.local et tous ses sous-domaines). Étape 1.5.Envoyez 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-cu...
Étape 2.Déchiffrez le trafic de l'URL	Mise en garde : Le déchiffrement d'un grand nombre d'URL peut entraîner une dégradation des performances. Étape 2.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Decryption Policies Étape 2.2.Cliquez sur Add Policy. Étape 2.3.EnterName pour la nouvelle stratégie. Étape 2.4.(Facultatif) Sélectionnez le profil d'identification auquel s'applique cette stratégie. Conseil : (Facultatif) Si vous souhaitez appliquer la stratégie à tous les utilisateurs, même s'ils ne sont pas authentifiés, sélectionnez Tous les utilisateurs (utilisateurs authentifiés et non authentifiés). Étape 2.5.Dans la section Définition de membre de stratégie, cliquez sur le lien 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 Envoyer.

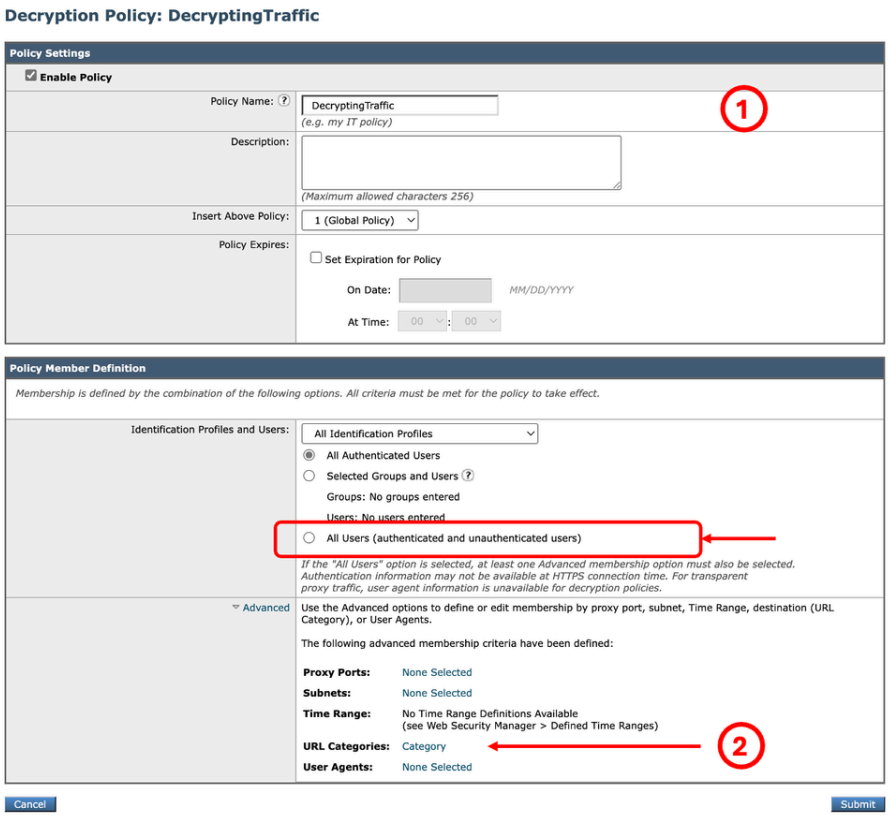


Image - Créer une stratégie de déchiffrement

Étape 2.8.InDecryption Policies page, cliquez sur le lien fromURL Filtering pour la nouvelle stratégie.

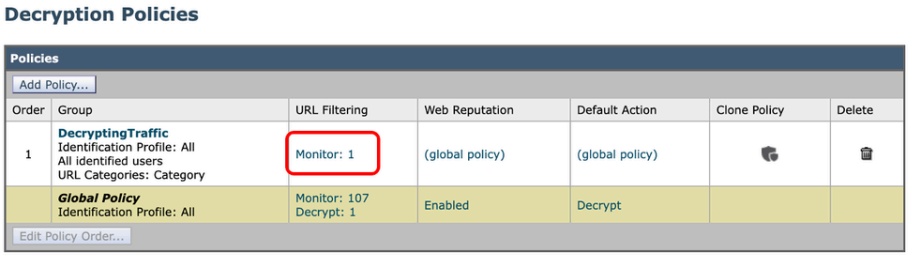


Image : sélectionnez le filtrage des URL.

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

Étape 2.10.Cliquez sur Envoyer.

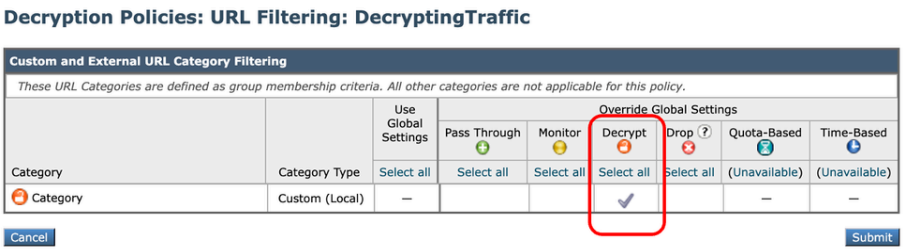


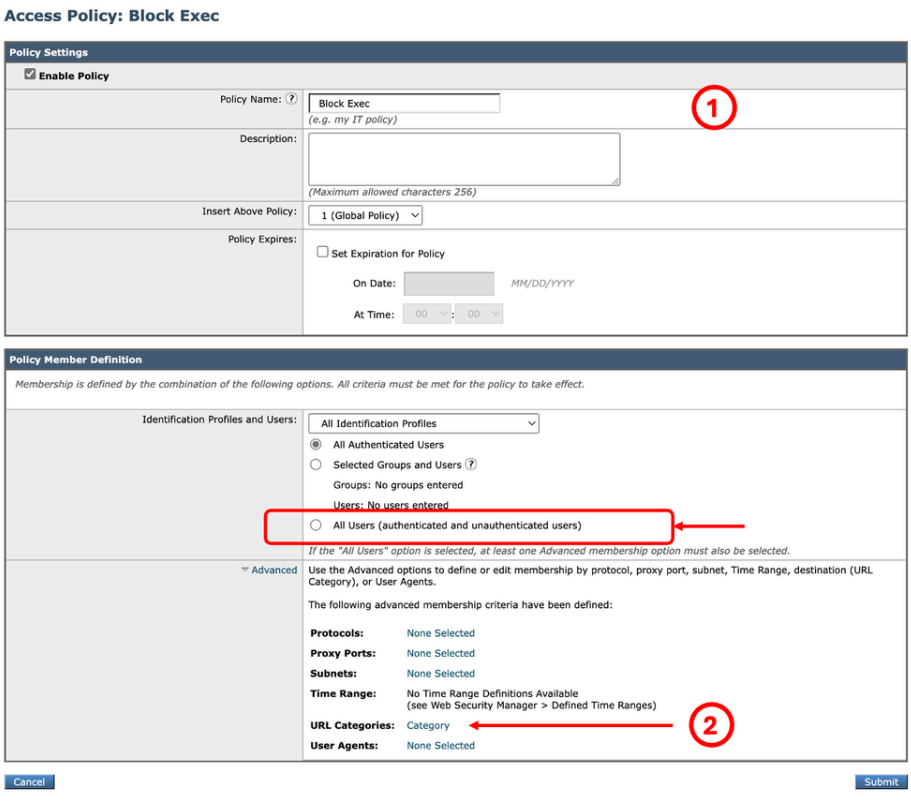
	Image - Définir le déchiffrement comme action
Étape 3.Bloquer les fichiers exécutables	Étape 3.1.Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Access Policies. Étape 3.2.Cliquez sur Ajouter une stratégie. Étape 3.3.EnterName pour la nouvelle stratégie. Étape 3.4.(Facultatif) Sélectionnez le profil d'identification auquel s'applique cette stratégie. Conseil : (Facultatif) Si vous souhaitez appliquer la stratégie à tous les utilisateurs, même s'ils ne sont pas authentifiés, sélectionnez Tous les utilisateurs (utilisateurs authentifiés et non authentifiés). 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 Envoyer. 

Image - Stratégie d'accès

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 Stratégies d'accès, assurez-vous que l'action Filtrage d'URL est définie sur Surveiller.

Étape 3.9. Dans la page Stratégies d'accès, cliquez sur le lien à partir de Objets pour la nouvelle stratégie.

Image - Sélectionner les objets

Image : sélectionnez le filtrage des URL.

Étape 3.10. Dans le menu déroulant, sélectionnez Définir les paramètres de blocage des objets personnalisés.

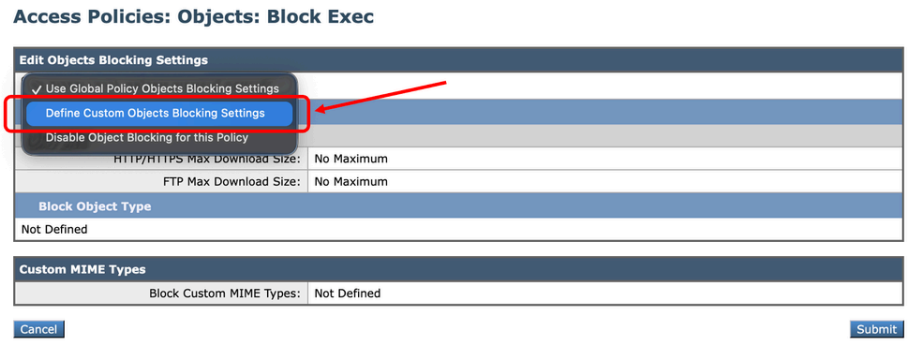


Image - Définir des objets personnalisés

Étape 3.11.Cliquez surCode exécutable pour sélectionner les types d'objets à bloquer.

Étape 3.12.Cliquez sur Installers pour sélectionner les types d'objets que vous souhaitez bloquer.

Étape 3.13. En outre, vous pouvez entrer les types MIME des

fichiers que vous souhaitez bloquer dans la section Types MIME personnalisés.

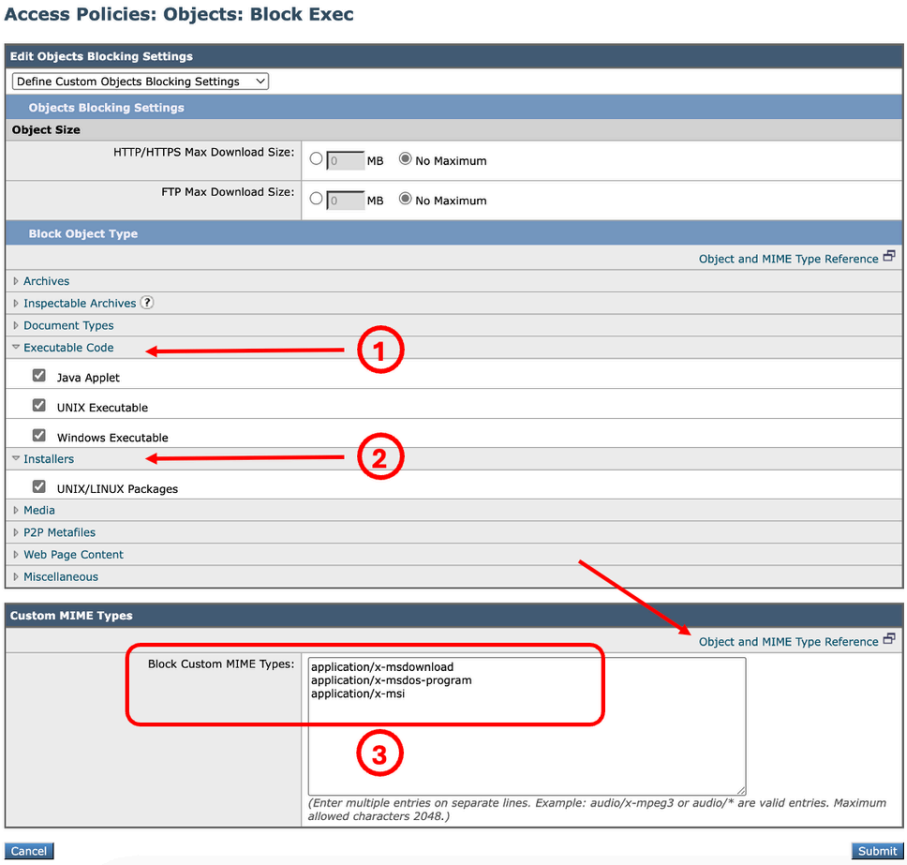


Image : configuration des objets à bloquer

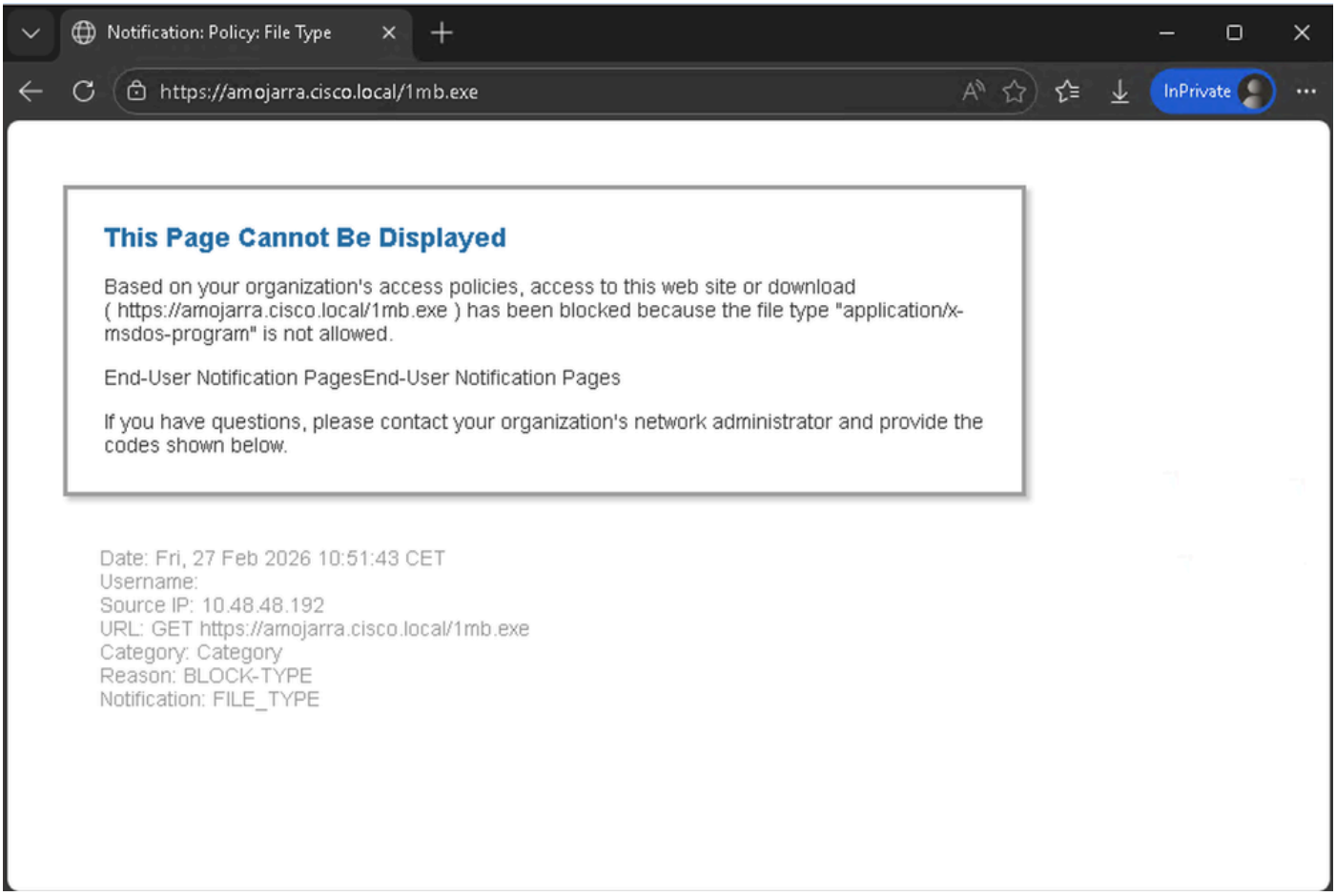
Conseil : Pour afficher la liste des types MIME, cliquez sur Object and MIME Type Reference.

Étape 3.14.Submit.

Étape 3.15.Validez les modifications.

Validation du blocage des extensions de fichier

Dans cet exemple, lorsqu'un utilisateur tente de télécharger un fichier exécutable, la page d'avertissement suivante s'affiche :



Page Image - Notification de blocage

Conseil : Pour configurer la page de notification de l'utilisateur final, accédez à Services de sécurité à partir de l'interface utilisateur graphique, cliquez sur Notification de l'utilisateur final et modifiez la section Pages de notification de l'utilisateur final.

À partir des journaux d'accès, vous pouvez voir deux lignes de journal liées au trafic.

La première ligne de journal est liée à la stratégie de déchiffrement (Nom : DecryptingTraffic) qui décrypte le trafic. L'action est DECRYPT_CUSTOMCAT

La deuxième ligne du journal d'accès est liée à la politique d'accès (Nom : Block_Exec) que nous avons créé à l'étape 2.3. L'action est BLOCK_ADMIN_FILE_TYPE

Policy (politique)	Fichier journal des accès
Politique de déchiffrement	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ - DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7-DecryptingTraffic-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",-,-,-,"-,-,-,-,"-,-,-,-,-,-,"-,-",-,-",-",-,-,-",-",-",-",-",-",-",-",-",-",-",-",-",1.71,0,-,-",-",-",-,-",-,-",-",-",-,-,-"-,-",-,-> -

Politique d'accès	1772186576.735 2242 10.48.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.application locale/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",ns,0,"-",0,0,0,-,"-,-,-,-,-,-,"-,-,-,"-,-,-,-,"nc",-,"-","-","-","-","-","Inconnu","Inconnu",-","-",0.00,0,-,-,"Inconnu",-","-"-,-","-,-"-","-",-","-,-,"-,-"-,-,-,-> -

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.