Bloquer le trafic dans l'appliance Web sécurisée

Table des matières

Introduction

Ce document décrit les étapes à suivre pour bloquer le trafic dans Secure Web Appliance (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA.

Cisco recommande que vous ayez :

- SWA physique ou virtuel installé.
- Accès administratif à l'interface utilisateur graphique (GUI) de 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.

Blocage du trafic

Le blocage du trafic dans le SWA est une étape cruciale pour assurer la sécurité du réseau, maintenir la conformité avec les politiques internes et se protéger contre les activités malveillantes. Voici quelques raisons courantes de blocage du trafic :

Raisons du blocage par source

- Inondation par un ou plusieurs utilisateurs : lorsqu'un ou plusieurs utilisateurs génèrent un trafic excessif, le réseau peut être submergé, ce qui entraîne une dégradation des performances et des interruptions potentielles de service.
- Accès aux ressources non approuvées par les applications (agents utilisateurs) : certaines applications peuvent tenter d'accéder à des ressources non approuvées ou potentiellement dangereuses. Le blocage de ces agents utilisateur permet d'éviter les failles de sécurité et les fuites de données.
- Restriction de l'accès à Internet pour des plages d'adresses IP spécifiques : il est possible que certaines adresses ou plages d'adresses IP ne puissent pas accéder à Internet en raison de stratégies de sécurité ou pour empêcher une utilisation non autorisée.
- Comportement de trafic suspect : le trafic présentant des modèles ou des comportements inhabituels qui pourraient indiquer une activité malveillante ou des menaces de sécurité doit être bloqué pour protéger le réseau.

Raisons du blocage par destination

- Conformité avec les politiques internes de l'entreprise : les entreprises ont souvent des politiques qui limitent l'accès à certains sites Web ou ressources en ligne pour garantir la productivité et la conformité avec les exigences légales ou réglementaires.
- Sites non approuvés : le blocage de l'accès aux sites Web considérés comme non fiables ou potentiellement dangereux permet de protéger les utilisateurs contre le phishing, les programmes malveillants et autres menaces en ligne.
- Comportement malveillant : les sites connus pour héberger du contenu malveillant ou pour s'engager dans des activités nuisibles doivent être bloqués pour empêcher les incidents de sécurité et les violations de données.

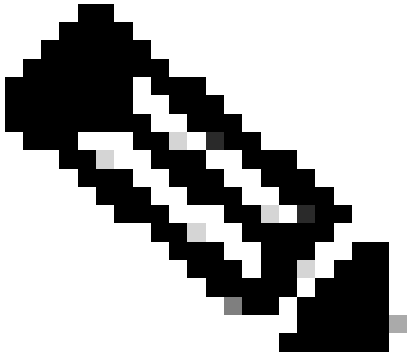
.

Étapes de blocage du trafic

En général, il y a 3 étapes principales pour bloquer le trafic dans SWA :

- Créez un profil d'identification pour le ou les utilisateurs.
- Bloquez le trafic HTTPS dans la stratégie de décodage.
- Bloquez le trafic HTTP dans la stratégie d'accès.

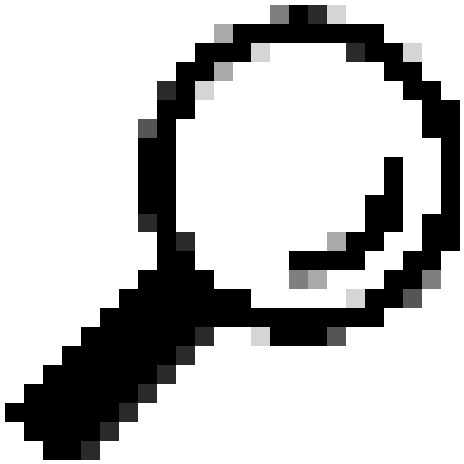
Étapes	Empêcher des utilisateurs spécifiques d'accéder à des sites Web	Empêcher des utilisateurs spécifiques d'accéder à certains sites Web

Catégorie d'URL personnalisée	Sans objet.	Créez une catégorie d'URL personnalisée pour les sites auxquels vous prévoyez de bloquer l'accès. Pour plus d'informations, consultez le site : Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco
Profil D'Identification	Étape 1. Dans l'interface graphique utilisateur, choisissez Web Security Manager, puis cliquez sur Identification Profiles. Étape 2. Cliquez sur Add Profile pour ajouter un profil. Étape 3. Utilisez la case à cocher Enable Identification Profile pour activer ce profil ou pour le désactiver rapidement sans le supprimer. Étape 4. Attribuez un nom de profil unique. Étape 5. (Facultatif) Ajoutez une description. Étape 6. Dans la liste déroulante Insérer au-dessus, choisissez l'emplacement de ce profil dans le tableau. Étape 7. Dans la section Méthode d'identification de l'utilisateur, sélectionnez Exempter de l'authentification/identification. Étape 8. Dans la section Define Members by Subnet, saisissez les adresses IP ou les sous-réseaux que ce profil d'identification doit appliquer. Vous pouvez utiliser des adresses IP, des blocs CIDR (Classless Inter-Domain Routing) et des sous-réseaux.	 Remarque : pour bloquer l'accès à certains sites Web pour tous les utilisateurs, il n'est pas nécessaire de créer un profil d'ID distinct. Cela peut être géré efficacement par le biais de la politique globale de décodage/d'accès. Étape 1. Dans l'interface graphique utilisateur, choisissez Web Security Manager, puis cliquez sur Identification Profiles. Étape 2. Cliquez sur Add Profile pour ajouter un profil. Étape 3. Utilisez la case à cocher Enable Identification Profile pour activer ce profil ou pour le désactiver rapidement sans le supprimer. Étape 4. Attribuez un nom de profil unique. Étape 5. (Facultatif) Ajoutez une description.

		Étape 6. Dans la liste déroulante Insérer au-dessus, choisissez l'emplacement de ce profil dans le tableau. Étape 7. Dans la section Méthode d'identification de l'utilisateur, sélectionnez Exempter de l'authentification/identification. Étape 8. Dans la section Define Members by Subnet, saisissez les adresses IP ou les sous-réseaux que ce profil d'identification doit appliquer. Vous pouvez utiliser des adresses IP, des blocs CIDR (Classless Inter-Domain Routing) et des sous-réseaux. Étape 9. Cliquez sur Advanced et ajoutez la catégorie d'URL que vous souhaitez bloquer l'accès à celle-ci.
Politique de déchiffrement	Étape 1. Dans l'interface graphique utilisateur, choisissez Web Security Manager, puis cliquez sur Decryption Policy. Étape 2. Cliquez sur Add Policy pour ajouter une stratégie de décodage. Étape 3. Utilisez la case à cocher Enable Policy pour activer cette stratégie. Étape 4. Attribuez un nom de stratégie unique. Étape 5. (Facultatif) Ajoutez une description. Étape 6. Dans la liste déroulante Insérer au-dessus de la politique, sélectionnez la première politique. Étape 7. Dans la section Profils d'identification et utilisateurs, sélectionnez le profil d'identification que vous avez créé dans les étapes précédentes.	Étape 1. Dans l'interface graphique utilisateur, choisissez Web Security Manager, puis cliquez sur Decryption Policy. Étape 2. Cliquez sur Add Policy pour ajouter une stratégie de décodage. Étape 3. Utilisez la case à cocher Enable Policy pour activer cette stratégie. Étape 4. Attribuez un nom de stratégie unique. Étape 5. (Facultatif) Ajoutez une description. Étape 6. Dans la liste déroulante Insérer au-dessus de la politique, sélectionnez la première politique. Étape 7. Dans la section Profils d'identification et utilisateurs, sélectionnez le profil d'identification que vous avez créé dans les étapes précédentes.

Étape 8. Envoyer.

Étape 9. Sur la page Decryption Policies, sous URL Filtering, cliquez sur le lien associé à cette nouvelle stratégie de décodage.

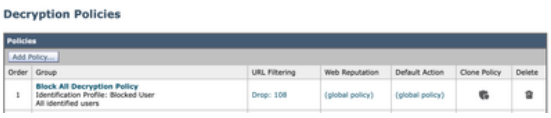


Conseil : étant donné que vous bloquez toutes les catégories d'URL, vous pouvez optimiser la stratégie en supprimant les catégories d'URL personnalisées et en utilisant uniquement les catégories d'URL prédéfinies. Cela réduit la charge de traitement sur le SWA en évitant l'étape supplémentaire de mise en correspondance des URL avec des catégories d'URL personnalisées.

Étape 10. Sélectionnez Drop comme action pour chaque catégorie d'URL.

Étape 11. Sur la même page, faites défiler vers le bas jusqu'à URL non classées et choisissez Drop dans la liste déroulante.

Étape 12. Envoyer.



Étape 8. Envoyer.

Étape 9. Sur la page Decryption Policies, sous URL Filtering, cliquez sur le lien associé à cette nouvelle stratégie de décryptage.

Étape 10. Sélectionnez Drop comme action pour la catégorie d'URL personnalisée créée pour les sites Web bloqués.

Étape 11. Cliquez sur Submit.

Image - Bloquer certaines URL dans la stratégie de déchiffrement

	Image - Politique de décodage pour bloquer tout le site Web pour certains utilisateurs	
Politique d'accès	Étape 1. Dans l'interface graphique utilisateur, choisissez Web Security Manager, puis cliquez sur Access Policy. Étape 2. Cliquez sur Add Policy pour ajouter une stratégie d'accès. Étape 3. Utilisez la case à cocher Enable Policy pour activer cette stratégie. Étape 4. Attribuez un nom de stratégie unique. Étape 5. (Facultatif) Ajoutez une description. Étape 6. Dans la liste déroulante Insérer au-dessus de la politique, sélectionnez la première politique. Étape 7. Dans la section Profils d'identification et utilisateurs, sélectionnez le profil d'identification que vous avez créé dans les étapes précédentes. Étape 8. Envoyer. Étape 9. Sur la page Access Policies, sous Protocols and User Agents, cliquez sur le lien associé à cette nouvelle stratégie d'accès. Étape 10. Dans la liste déroulante Edit Protocols and User Agents Settings, sélectionnez Define Custom Settings. Étape 11. Dans Block Protocols : sélectionnez pour les deux FTP sur HTTP et HTTP. Étape 12. Dans HTTP CONNECT Ports, supprimez chaque numéro de port pour bloquer tous les ports.	Étape 1. Dans l'interface graphique utilisateur, choisissez Web Security Manager, puis cliquez sur Access Policy. Étape 2. Cliquez sur Add Policy pour ajouter une stratégie d'accès. Étape 3. Utilisez la case à cocher Enable Policy pour activer cette stratégie. Étape 4. Attribuez un nom de stratégie unique. Étape 5. (Facultatif) Ajoutez une description. Étape 6. Dans la liste déroulante Insérer au-dessus de la politique, sélectionnez la première politique. Étape 7. Dans la section Profils d'identification et utilisateurs, sélectionnez le profil d'identification que vous avez créé dans les étapes précédentes. Étape 8. Envoyer. Étape 9. Sur la page Access Policies, sous URL Filtering, cliquez sur le lien associé à cette nouvelle stratégie d'accès Étape 10.Sélectionnez Bloquer comme action pour la catégorie d'URL personnalisée créée pour les sites Web bloqués. Étape 11. Envoyer. Étape 12. Valider les modifications.  Image - Bloquer certaines URL dans la stratégie

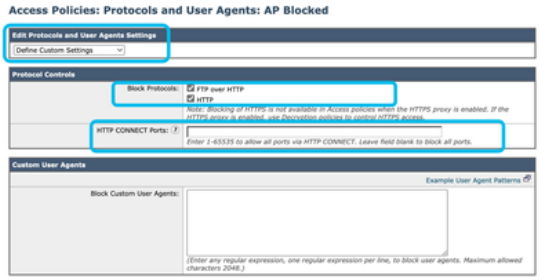
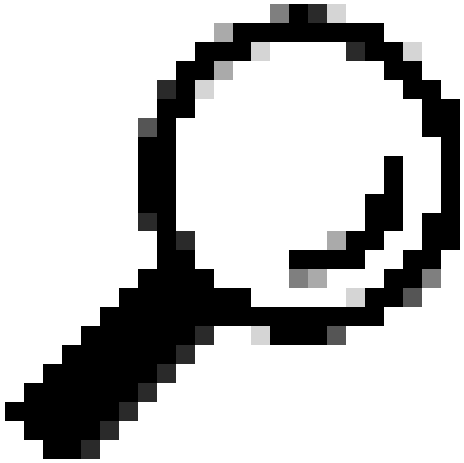


Image - Blocage des protocoles et des ports de connexion dans la stratégie d'accès

Étape 13. Envoyer.

Étape 14. (Facultatif) Dans la page Access Policies, sous URL Filtering, cliquez sur le lien associé à cette nouvelle stratégie d'accès et sélectionnez Bloquer comme action pour chaque catégorie d'URL et URL non classées, puis envoyer.



Conseil : étant donné que vous bloquez toutes les catégories d'URL, vous pouvez optimiser la stratégie en supprimant les catégories d'URL personnalisées et en utilisant uniquement les catégories d'URL prédéfinies. Cela réduit la charge de traitement sur le SWA en évitant l'étape supplémentaire de mise en correspondance des URL avec des catégories d'URL personnalisées.

d'accès

	Étape 16. Valider les modifications.  Stratégie d'accès aux images pour bloquer tous les sites	

Attention : dans un déploiement de proxy transparent, SWA ne peut pas lire les agents utilisateur ou l'URL complète du trafic HTTPS à moins que le trafic ne soit décrypté. Par conséquent, si vous configurez le profil d'identification à l'aide d'agents utilisateur ou d'une catégorie d'URL personnalisée avec des expressions régulières, ce trafic ne correspond pas au profil d'identification.

Blocage de sites à l'aide d'expressions régulières dans un

déploiement proxy transparent

Dans le déploiement de proxy transparent, si vous prévoyez de bloquer une catégorie d'URL personnalisée qui a la condition Expressions régulières - par exemple, si vous bloquez l'accès à certaines chaînes YouTube - vous pouvez utiliser ces étapes :

Étape 1. Créez une catégorie d'URL personnalisée pour le site principal. (Dans cet exemple : YouTube.com).

Étape 2. Créez une stratégie de décodage, affectez cette catégorie d'URL personnalisée et définissez l'action sur Déchiffrer.

Étape 3. Créez une stratégie d'accès, affectez la catégorie d'URL personnalisée aux expressions régulières (dans cet exemple, la catégorie d'URL personnalisée pour les chaînes YouTube) et définissez l'action sur Bloquer.

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - GD(General Deployment) - Classify End-Users for Policy Application [Cisco Secure Web Appliance] - Cisco
- Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco
- Comment exempter le trafic Office 365 de l'authentification et du déchiffrement sur l'appareil de sécurité Web Cisco (WSA) - Cisco

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.