Bloquer le trafic dans l'appliance Web sécurisée

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Bloquer le trafic

- Raisons du blocage par source
- Raisons du blocage par destination

Étapes de blocage du trafic

Bloquer des sites utilisant des expressions régulières dans un déploiement de proxy transparent

Autres informations utiles

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 vous recommande d'avoir :

- 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.

Bloquer le 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 fiables 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 IP spécifiques : Il est possible que certaines adresses ou plages 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 comportements ou des modèles 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 aux politiques internes de l'entreprise : Les entreprises ont souvent des politiques qui restreignent l'accès à certains sites Web ou ressources en ligne pour garantir la productivité et la conformité aux exigences légales ou réglementaires.
- Sites non approuvés : Le blocage de l'accès à des sites Web considérés comme douteux 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 se livrer à 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 utilisateur graphique, sélectionnez Web Security Manager, puis choisissez Identification Profiles. Étape 2. Choisissez Add Profile pour ajouter un profil. Étape 3. Utilisez la case à cocher Activer le profil d'identification pour activer ce profil ou 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 User Identification Method, sélectionnez	 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 utilisateur graphique, sélectionnez Web Security Manager, puis choisissez Identification Profiles. Étape 2. Choisissez Add Profile pour ajouter un profil. Étape 3. Utilisez la case à cocher Activer le profil d'identification pour activer ce profil ou le désactiver

	Exempt from authentication/ identification. Étape 8. Dans Définir les membres par sous-réseau, entrez les adresses IP ou les sous-réseaux auxquels s'applique ce profil d'identification. Vous pouvez utiliser des adresses IP, des blocs CIDR (Classless Inter-Domain Routing) et des sous-réseaux.	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 User Identification Method, sélectionnez Exempt from authentication/ identification. Étape 8. Dans Définir les membres par sous-réseau, entrez les adresses IP ou les sous-réseaux auxquels s'applique ce profil d'identification. Vous pouvez utiliser des adresses IP, des blocs CIDR (Classless Inter-Domain Routing) et des sous-réseaux. Étape 9. Choisissez Advanced et ajoutez la catégorie d'URL à laquelle vous souhaitez bloquer l'accès.
Politique de déchiffrement	Étape 1. Dans l'interface graphique, sélectionnez Web Security Manager, puis choisissez Decryption Policy. Étape 2. Choisissez 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 une stratégie ci-dessus, sélectionnez la première stratégie. Étape 7. Dans les profils d'identification et utilisateurs,	Étape 1. Dans l'interface graphique, sélectionnez Web Security Manager, puis choisissez Decryption Policy. Étape 2. Choisissez 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 une stratégie ci-dessus, sélectionnez la première stratégie. Étape 7. Dans les profils d'identification et utilisateurs,

<table>
<tr>
<td></td>
<td>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 Supprimer comme action pour chaque catégorie d'URL.

Étape 11. Sur la même page, faites défiler jusqu'à Uncategory URLs et choisissez Drop from drop-down list.

Étape 12. Envoyer.

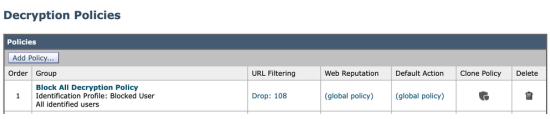


Image - Politique de décodage pour bloquer tout le site Web pour certains utilisateurs</td>
<td>sélectionnez le profil d'identification que vous avez créé dans les étapes précédentes.

Étape 8. Envoyer.

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

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

Étape 11. Cliquez sur Envoyer.

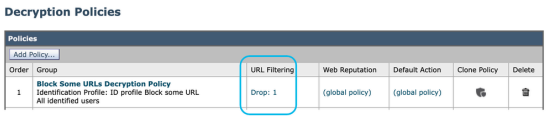


Image - Bloquer certaines URL dans la stratégie de déchiffrement</td>
</tr>
<tr>
<td>Politique d'accès</td>
<td>Étape 1. Dans l'interface graphique, sélectionnez Web Security Manager, puis cliquez sur Access Policy.</td>
<td>Étape 1. Dans l'interface graphique, sélectionnez Web Security Manager, puis cliquez sur Access Policy.</td>
</tr>
</table>

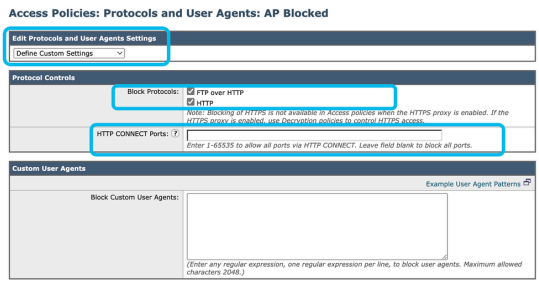
	Étape 2. Cliquez sur Add Policy pour ajouter une stratégie d'accès. Étape 3. Utilisez la case à cocher Enable Policy pour activer cette stratégie. Étape 4. Attribuez un nom de stratégie unique. Étape 5. (Facultatif) Ajoutez une description. Étape 6. Dans la liste déroulante Insérer une stratégie ci-dessus, sélectionnez la première stratégie. Étape 7. Dans les 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 Modifier les paramètres des protocoles et des agents utilisateur, sélectionnez Définir les paramètres personnalisés. Étape 11. Dans Protocoles de blocage, activez la case à cocher FTP sur HTTP et HTTP. Étape 12. Dans HTTP CONNECT Ports, supprimez chaque numéro de port pour bloquer tous les ports.  	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 une stratégie ci-dessus, sélectionnez la première stratégie. Étape 7. Dans les 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 URL personnalisée créée pour les sites Web bloqués. Étape 11. Cliquez sur Submit. Étape 12. Confirmer les modifications  Image - Bloquer certaines URL dans la stratégie d'accès

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 Block comme action pour chaque catégorie d'URL et les URL non classées puis Submit.

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 15. Validez les modifications.



Stratégie d'accès aux images pour bloquer tous les sites

Mise en garde : Dans un déploiement de proxy transparent, SWA ne peut pas lire les agents utilisateur ou l'URL complète pour le 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.

Bloquer des sites utilisant des expressions régulières dans un déploiement de 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 : création d'une catégorie d'URL personnalisée pour le site principal (Dans cet exemple : YouTube.com).

Étape 2 : création d'une stratégie de déchiffrement, attribution de cette catégorie d'URL personnalisée et définition de 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.

Autres informations utiles

- 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.