Introduction

Cette rubrique contient les sections suivantes :

À propos de Secure Web Appliance

Cisco Secure Web Appliance (SWA) intercepte et surveille le trafic Internet et applique des politiques pour assurer la protection de votre réseau interne contre les programmes malveillants, la perte de données sensibles, la perte de productivité et d'autres menaces Internet. Secure Web Appliance de Cisco agit comme un serveur proxy, en interceptant les demandes Web des utilisateurs et en analysant le contenu Web demandé à la recherche de menaces potentielles telles que des programmes malveillants, des virus et des tentatives d'hameçonnage. Diverses technologies de sécurité sont utilisées, par exemple le filtrage d'URL, l'analyse antivirus, le filtrage basé sur la réputation et Advanced Malware Protection pour assurer la sécurité du trafic Web. Dans l'ensemble, Secure Web Appliance aide les organisations à sécuriser leur trafic Web, à appliquer les politiques d'utilisation et à se protéger contre les menaces Web, ce qui contribue à créer un environnement de navigation Web plus sûr et plus contrôlé pour les utilisateurs.

Thèmes connexes

- http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

Utilisation de l'interface Web de l'appliance

Exigences du navigateur de l'interface Web

Voici les exigences pour accéder à l'interface Web :

- Les témoins et JavaScript doivent être pris en charge et activés par votre navigateur.
- Le navigateur doit être en mesure d'afficher des pages HTML contenant des feuilles de style en chaîne (CSS).
- L'Cisco Secure Web Appliance suit les environnements cibles définis par YUI : http://yuilibrary.com/yui/environments/
- Votre session expire automatiquement après 30 minutes d'inactivité.
- Certains boutons et liens de l'interface Web entraînent l'ouverture de fenêtres supplémentaires. Par conséquent, vous devrez peut-être configurer les paramètres de blocage des fenêtres contextuelles du navigateur pour utiliser l'interface Web.

Note N'utilisez qu'une seule fenêtre ou un seul onglet de navigateur à la fois pour modifier la configuration de l'appliance. Ne modifiez pas l'appliance en même temps à l'aide de l'interface Web et de l'interface de ligne de commande. La modification simultanée de l'appliance à partir de plusieurs emplacements entraîne un comportement inattendu et n'est pas prise en charge.

Pour accéder à l'interface graphique, votre navigateur doit prendre en charge JavaScript et être activé pour accepter JavaScript, et il doit être en mesure d'afficher les pages HTML contenant des feuilles de style en chaîne (CSS).

Table 1: Navigateurs et versions pris en charge

Navigateur	Windows 10	MacOS 10.6
Safari	—	version 7.0 ou ultérieure
Google Chrome	Dernière version stable	Dernière version stable
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	Dernière version stable	Dernière version stable
Microsoft Edge	Dernière version stable	Dernière version stable

Les navigateurs ne sont pris en charge que pour les systèmes d'exploitation officiellement pris en charge par le navigateur.

Vous devrez peut-être configurer les paramètres de blocage des fenêtres contextuelles de votre navigateur pour utiliser l'interface graphique, car certains boutons ou certains liens de l'interface entraîneront l'ouverture de fenêtres supplémentaires.

Vous pouvez accéder à l'ancienne interface Web de l'appliance sur n'importe lequel des navigateurs pris en charge.

La résolution prise en charge pour la nouvelle interface Web de l'appliance (AsyncOS 11.8 et versions ultérieures) est comprise entre 1 280 x 800 et 1 680 x 1 050. La meilleure résolution d'affichage pour tous les navigateurs pris en charge est de 1 440 x 900.

Note Cisco ne recommande pas d'afficher la nouvelle interface Web de l'appliance avec des résolutions plus élevées.

Activation de l'accès à l'interface Web sur les appliances virtuelles

Par défaut, les interfaces HTTP et HTTPS ne sont pas activées sur les appliances virtuelles. Pour activer ces protocoles, vous devez utiliser l'interface de ligne de commande.

Étape 1 Accédez à l'interface de commande en ligne. Consultez Accès à l'interface de commande en ligne.

Étape 2 Exécutez la commande `interfaceconfig`.

Appuyez sur Enter (Entrée) à une invite pour accepter la valeur par défaut.

Recherchez les invites pour HTTP et HTTPS et activez le ou les protocoles que vous utiliserez.

Recherchez les invites de l'API AsyncOS (supervision) pour HTTP et HTTPS et activez le ou les protocoles que vous utiliserez.

Accès à l'interface Web de l'appliance

Si vous utilisez une appliance virtuelle, consultez Activation de l'accès à l'interface Web sur les appliances virtuelles , on page 3.

Étape 1 Ouvrez un navigateur et entrez l'adresse IP (ou le nom d'hôte) de Secure Web Appliance. Si l'appliance n'a pas été configurée précédemment, utilisez les paramètres par défaut :

`https://192.168.42.42:8443`

-ou-

`http://192.168.42.42:8080`

où `192.168.42.42` est l'adresse IP par défaut, `8080` est le paramètre du port d'administration par défaut pour HTTP et `8443` est le port d'administration par défaut pour `HTTPS`.

Sinon, si l'appliance est actuellement configurée, utilisez l'adresse IP (ou le nom d'hôte) du port M1.

Note Vous devez utiliser un numéro de port lors de la connexion à l'appliance (par défaut, le port `8080`). Le fait de ne pas spécifier de numéro de port lors de l'accès à l'interface Web entraînera l'affichage d'un port par défaut 80, une page d'erreur proxy sans licence.

Étape 2 [Nouvelle interface Web uniquement] Connectez-vous à l'ancienne interface Web et cliquez sur **Secure Web Appliance pour obtenir une nouvelle apparence. Essayez** pour accéder à la nouvelle interface Web! Lorsque vous cliquez sur ce lien, un nouvel onglet s'ouvre dans votre navigateur Web et vous conduit à

`https://wsa_appliance.com:<trailblazer-https-port>/ng-login`, où `wsa_appliance.com` est le nom d'hôte de l'appliance et `<trailblazer-https-port>` est le port HTTPS trailblazer configuré sur l'appliance.

Note

- Vous devez vous connecter à l'ancienne interface Web de l'appliance.
- Assurez-vous que votre serveur DNS peut résoudre le nom d'hôte d'interface de l'appliance que vous avez spécifié.
- Par défaut, la nouvelle interface Web a besoin des ports TCP 6080, 6443 et 4431 pour être opérationnelle. Assurez-vous que ces ports ne sont pas bloqués dans le pare-feu d'entreprise.
- Le port par défaut pour accéder à la nouvelle interface Web est 4431. Cela peut être personnalisé à l'aide de la commande d'interface de ligne de commande `trailerblazerconfig`. Pour plus d'informations sur la commande d'interface de ligne de commande `trailblazerconfig`, consultez Commandes de l'interface de ligne de commande Secure Web Appliance.
- La nouvelle interface Web a également besoin de ports d'API AsyncOS (supervision) pour HTTP et HTTPS. Par défaut, ces ports sont 6080 et 6443. Les ports de l'API AsyncOS (supervision) peuvent également être personnalisés dans la commande d'interface de ligne de commande `interfaceconfig`. Pour plus d'informations sur la commande d'interface de ligne de commande `interfaceconfig`, voir Commandes de l'interface de ligne de commande Secure Web Appliance.

  Note Les ports sont activés par défaut, mais une fois désactivés, ils seront réactivés après la mise à niveau.

- Si vous modifiez ces ports par défaut, assurez-vous que les ports personnalisés de la nouvelle interface Web ne doivent pas non plus être bloqués dans le pare-feu d'entreprise.

Étape 3 Lorsque l'écran de connexion de l'appliance s'affiche, saisissez votre nom d'utilisateur et votre phrase secrète pour accéder à l'appliance.

Par défaut, l'appliance est livrée avec le nom d'utilisateur et la phrase secrète suivants :

- Nom d'utilisateur : **admin**
- Phrase secrète : **ironport**

Si c'est la première fois que vous vous connectez avec le nom d'utilisateur **admin** par défaut, vous serez invité à modifier immédiatement la phrase secrète.

Étape 4 Pour afficher une liste des tentatives d'accès récentes à l'appliance, réussites ou échecs, pour votre nom d'utilisateur, cliquez sur l'icône d'activité récente (**i** ou **!** en cas de réussite ou d'échec respectivement) devant l'entrée « Logged in as » (Connecté en tant que) dans le coin supérieur droit de la fenêtre de l'application.

Validation des modifications dans l'interface Web

Étape 1 Cliquez sur **Commit Changes** (Valider les modifications).

Étape 2 Entrez des commentaires dans le champ Commentaire si vous le souhaitez.

Étape 3 Cliquez sur **Commit Changes** (Valider les modifications).

Note Vous pouvez apporter plusieurs modifications à la configuration avant de toutes les valider.

Effacement des modifications dans l'interface Web

Étape 1 Cliquez sur **Commit Changes** (Valider les modifications).

Étape 2 Cliquez sur **Abandon Changes** (Ignorer les modifications).

Langues prises en charge

AsyncOS peut afficher son interface graphique et son interface de ligne de commande dans l'une des langues suivantes :

- Allemand
- Anglais
- Espagnol
- Français
- Italien
- Japonais
- Coréen
- Portugais
- Russe
- Chinois
- Taïwanais

Réseau Cisco SensorBase

Le réseau Cisco SensorBase est une base de données de gestion des menaces qui suit des millions de domaines à travers le monde et gère une liste de supervision mondiale du trafic Internet. SensorBase fournit à Cisco une évaluation de la fiabilité des domaines Internet connus. L'Cisco Secure Web Appliance utilise les flux de données SensorBase pour améliorer la précision des scores de réputation Web.

Avantages et confidentialité de SensorBase

La participation au réseau Cisco SensorBase signifie que Cisco recueille des données et les partage avec la base de données de gestion des menaces SensorBase. Ces données comprennent des informations sur les attributs de demande et la façon dont l'appliance traite les demandes.

Cisco reconnaît l'importance du maintien de votre confidentialité et ne recueille ni n'utilise de renseignements personnels ou confidentiels tels que les noms d'utilisateur et les phrases secrètes. En outre, les noms de fichiers et les attributs d'URL qui suivent le nom d'hôte sont masqués pour assurer la confidentialité. En ce qui concerne les transactions HTTPS déchiffrées, le réseau SensorBase reçoit uniquement l'adresse IP, le score de réputation de sites Web et la catégorie d'URL du nom du serveur dans le certificat.

Si vous acceptez de participer au réseau SensorBase, les données envoyées par votre appliance sont transférées de manière sécurisée à l'aide du protocole HTTPS. Le partage des données améliore la capacité de Cisco à réagir aux menaces Web et à protéger l'environnement de votre entreprise contre les activités malveillantes.

Activation de la participation au réseau Cisco SensorBase

Note La participation standard au réseau SensorBase est activée par défaut lors de la configuration du système.

Étape 1 Choisissez **Security Services > SensorBase** (Services de sécurité > SensorBase).

Étape 2 Vérifiez que la participation au réseau SensorBase est activée.

Lorsque cette option est désactivée, aucune donnée collectée par l'appliance n'est renvoyée aux serveurs du réseau SensorBase.

Étape 3 Dans la section du niveau de participation, choisissez l'un des niveaux suivants :

- **Limited** (Limité). La participation de base résume les renseignements sur le nom du serveur et envoie des segments de chemin hachés MD5 aux serveurs du réseau SensorBase.
- **Standard.** La participation améliorée envoie l'URL complète avec des segments de chemin non brouillés aux serveurs du réseau SensorBase. Cette option aide à fournir une base de données plus robuste et améliore continuellement l'intégrité des scores de réputation Web.

Étape 4 Dans le champ AnyConnect Network Participation (Participation au réseau AnyConnect), choisissez d'inclure ou non les informations recueillies auprès des clients qui se connectent aux Cisco Secure Web Appliance à l'aide du client Cisco AnyConnect.

Les clients AnyConnect envoient leur trafic Web vers l'appliance à l'aide de la fonctionnalité Secure Mobility.

Étape 5 Dans le champ Excluded Domains and IP Addresses (Domaines et adresses IP exclus), saisissez facultativement les domaines ou les adresses IP à exclure du trafic envoyé vers les serveurs SensorBase.

Étape 6 Envoyez et validez vos modifications.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.