Comprendre la protection contre les programmes malveillants et les logiciels espions des appliances Web sécurisées

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Aperçu
- Principaux facteurs de différenciation de SWA
  - Moniteur de trafic de couche 4 intégré (L4TM)
  - Traitement de la couche proxy
  - Filtres de réputation Web
  - Moteur DVS (Dynamic Vectoring and Streaming)
  - Système Cisco Anti-Malware
- Autres informations utiles

Introduction

Ce document décrit les fonctionnalités complètes de protection contre les programmes malveillants et les logiciels espions de l'appliance Web sécurisé Cisco (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration 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.

Aperçu

Cisco SWA est conçu pour fournir des mécanismes de défense de passerelle robustes et complets contre un large éventail de logiciels espions et de programmes malveillants basés sur le Web. Il contrecarre efficacement les menaces, qu'il s'agisse de logiciels publicitaires, connus pour leur utilisation massive des ressources réseau ou de problèmes de prise en charge, ou de menaces plus graves, telles que les chevaux de Troie, les pirates de navigateur, les objets d'assistance de navigateur, le phishing, le pharming, les moniteurs système, les enregistreurs de frappe et les vers.

Principaux facteurs de différenciation de SWA

Moniteur de trafic de couche 4 intégré (L4TM)

Le Moniteur de trafic de couche 4 est capable d'analyser tous les ports réseau (65 535 au total) à haut débit (vitesse filaire), assurant ainsi une détection et un blocage complets des programmes malveillants et des tentatives de communication non autorisées. Cette fonctionnalité empêche efficacement les programmes malveillants de contourner les ports courants tels que les ports 80 et 443, et elle supprime également les activités indésirables P2P (Peer-to-Peer) et IRC (Internet Relay Chat).

Traitement de la couche proxy

Le SWA intègre un proxy Web hautes performances avec des fonctionnalités intégrées de mise en cache et d'accélération du contenu. Optimisé par le logiciel Cisco AsyncOS propriétaire, ce proxy Web peut gérer jusqu'à dix fois plus de connexions que les serveurs proxy UNIX classiques. En tant que proxy Web, il facilite l'inspection exhaustive du contenu au niveau de la couche application, ce qui est essentiel pour une défense précise contre les programmes malveillants basés sur le Web.

Filtres de réputation Web

En tant que filtres de réputation Web innovants, ils fournissent une couche de défense supplémentaire. À l'aide de SenderBase®, ces filtres évaluent plus de 50 paramètres de trafic Web et de réseau pour déterminer la fiabilité des URL. Des techniques de modélisation de sécurité avancées sont utilisées pour attribuer des pondérations individuelles à chaque paramètre, aboutissant à un score de réputation compris entre -10 et +10. Les stratégies configurées par l'administrateur s'adaptent dynamiquement en fonction de ces scores.

Moteur DVS (Dynamic Vectoring and Streaming)

Le moteur DVS introduit une analyse accélérée des signatures dans le SWA, se démarquant des architectures traditionnelles qui dépendent du protocole ICAP (Internet Content Adaptation Protocol) et des déploiements multi-boîtiers pour l'analyse des programmes malveillants. Cette plate-forme de pointe utilise des techniques sophistiquées d'analyse d'objets, de vectorisation, de balayage de flux et de mise en cache de verdict ; en multipliant par dix le débit d'analyse par rapport aux solutions ICAP de première génération.

Système Cisco Anti-Malware

Ce système exploite le moteur DVS aux côtés de plusieurs types de signatures provenant de Webroot, offrant une protection inégalée contre un large éventail de menaces basées sur le Web. Le spectre des menaces inclut les logiciels publicitaires, les pirates de navigateur, le phishing, les attaques de pharming et d'autres entités malveillantes telles que les chevaux de Troie, les moniteurs système et les enregistreurs de frappe. SWA dispose de la base de données de signatures de programmes malveillants la plus importante du marché au niveau de la passerelle, assurant ainsi une protection complète.

Cisco Web Security Appliance est positionné comme leader dans la sécurisation des passerelles réseau contre un large éventail de menaces basées sur le Web, assurant à la fois une protection robuste et un débit réseau hautes performances.

Autres informations utiles

- Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance

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.