Understand Secure Web Appliance Malware and Spyware Protection

Contents

Introduction

This document describes the comprehensive malware and spyware protection features of the Cisco Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SWA administration.

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Overview

The Cisco SWA is engineered to deliver robust and comprehensive gateway defense mechanisms against a wide spectrum of spyware and web-based malware. It efficiently counters threats ranging from adware, which is notorious for causing significant network resource drain and supportability challenges, to more severe threats including trojans, browser hijackers, browser helper objects, phishing, pharming, system monitors, keyloggers, and worms.

Key Differentiators of SWA

Integrated Layer 4 Traffic Monitor (L4TM)

The L4 Traffic Monitor is capable of scanning all network ports (65,535 in total) at wire speed, ensuring comprehensive detection and blocking of malware and unauthorized communication attempts. This functionality effectively thwarts malware trying to bypass common ports such as Ports 80 and 443, and it also suppresses rogue Peer-to-Peer (P2P) and Internet Relay Chat (IRC) activities.

Proxy-Layer Processing

The SWA incorporates a high-performance web proxy with integrated caching and content acceleration capabilities. Powered by Cisco proprietary AsyncOS, this web proxy can manage up to ten times more connections than conventional UNIX-based proxy servers. As a web proxy, it facilitates exhaustive content inspection at the application layer, which is essential for precise defense against web-based malware.

Web Reputation Filters

As the industry pioneering web reputation filters, these provide an additional layer of defense. Utilizing SenderBase®, these filters evaluate over 50 web traffic and network-related parameters to determine a URLs trustworthiness. Advanced security modeling techniques are employed to assign individual weights to each parameter, culminating in a reputation score ranging from -10 to +10. Administrator configured policies adapt dynamically based on these scores.

Dynamic Vectoring and Streaming (DVS) Engine

The DVS Engine introduces accelerated signature scanning within the SWA, standing apart from legacy architectures that depend on Internet Content Adaptation Protocol (ICAP) and multi-box deployments for malware scanning. This cutting-edge platform utilizes sophisticated object parsing, vectoring techniques, stream scanning, and verdict caching, achieving up to a tenfold increase in scanning throughput compared to first-generation ICAP-based solutions.

Cisco Anti-Malware System

This system leverages the DVS Engine alongside multiple signature types sourced from Webroot, offering unparalleled protection against a diverse array of web-based threats. The spectrum of threats includes adware, browser hijackers, phishing, pharming attacks, and more malicious entities like trojans, system monitors, and keyloggers. SWA boasts the industry largest malware signature database at the gateway, ensuring comprehensive protection.

The Cisco Web Security Appliance is thus positioned as a leader in securing network gateways against an extensive range of web-based threats, ensuring both robust protection and high-performance network throughput.

Related Information

- User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance