Содержание

Вопрос

Cisco Web Security Appliance (WSA) предоставляют Вредоносное ПО/Защиту от программ-шпионов?

Cisco Web Security Appliance (WSA) предоставляет самую всестороннюю защиту шлюза отрасли против шпионского ПО и находящегося на web вредоносного ПО. Это включает все от Рекламного ПО (который вызывает большинство проблем обеспеченности и использует значительные сетевые ресурсы) к более злонамеренным угрозам, таким как Троянские кони, Налетчики Браузера, Объекты помощника Браузера, Фишинг, Pharming, Системные мониторы, Кейлоггеры, Черви, и т.д.

Основные дифференцирующие звенья веб-Решения по обеспечению безопасности Cisco включают:

1. Встроенный уровень 4 (L4) Монитор трафика просматривает все порты на проводной скорости, обнаруживая и блокируя действие Phone Home и вредоносное ПО. Путем отслеживания всех 65,535 сетевых портов Монитор трафика L4 эффективно останавливает вредоносное ПО, которое пытается обойти порт 80 и также предотвращает постороннего P2P, и IRC отнесся действие.
2. Обработка уровня прокси: Cisco Web Security Appliance также включает Веб - прокси производительности чрезвычайна высокого, наряду с интегрированным кэшированием и ускоряющими возможностями содержания. Основанный на составляющей собственность операционной системе Cisco, AsyncOS, устройство Веба - прокси Cisco может поддержать до 100,000 одновременных подключений так же как 10x больше, чем традиционные основанные на UNIX прокси-серверы. Быть Вебом - прокси обеспечивает всесторонний контроль содержания в уровне приложения - критически важное требование к убеждающейся точности против находящегося на web вредоносного ПО.
3. Первые веб-Фильтры Репутации отрасли предоставляют мощный внешний уровень защиты. Усиливая SenderBase®, веб-Фильтры Репутации Cisco анализируют более чем 50 + другой Веб - трафик и связанные с сетью параметры для точной оценки степени доверия URL. Сложные способы моделирования безопасности используются, чтобы индивидуально взвесить каждый параметр и генерировать одиночный счет в масштабе-10 к +10. Настроенная политика администратора динамично применена, на основе очков репутации.
4. Ускоренное сканирование подписи с помощью Динамической Векторизации и Потоковой передачи Механизма (Механизм DVS). В отличие от устаревших решений для архитектуры, которые полагаются на ICAP и развертывания мультикоробки для обеспечения сканирования вредоносного ПО, WSA Cisco представил Механизм DVS для интегрированного решения для сканирования на коробке. Эта инновационная

платформа использует сложный объект анализирующие и векторизовавшие способы, наряду с потоковым сканированием и кэшированием вердикта, приводящим к до 10x сканирование увеличения пропускной способности по первому поколению основанные на ICAP решения.

5. Система Антивируса лидирующей Cisco усиливает механизм DVS и множественные типы подписи от Webroot для обеспечивания наилучшей защиты против самого широкого разнообразия Находящихся на web угроз. Эти угрозы могут колебаться от рекламного ПО, налетчиков браузера, фишинга и атак pharming к более злонамеренным угрозам, таким как Троянские кони, Системные мониторы и Кейлоггеры. WSA предлагает самую большую вредоносную базу данных подписи отрасли в шлюзе.