

TippingPoint™ X505

ТЕХНИЧЕСКИЕ ДАННЫЕ

Встраивание искусственного интеллекта в работу сети

TippingPoint X505 является первой интегрированной платформой безопасности, разработанной на основе передовой архитектуры предотвращения вторжений TippingPoint, использующей расширенные функции виртуальных частных сетей (VPN) и брандмауэра, управление полосой пропускания и обеспечивающей качество услуг и фильтрацию веб-контента

Платформа TippingPoint X505 предназначена для удовлетворения потребностей разветвленных предприятий, региональных представительств или компаний среднего размера благодаря применению тех же передовых возможностей систем предотвращения вторжений TippingPoint и службы цифровых вакцин Digital Vaccine™, которые используются для информационной защиты многих крупных предприятий. Платформа TippingPoint X505 является первым всеобъемлющим решением по безопасности с таким соотношением производительности и цены, которое позволяет филиалам предприятий обладать лучшей в своем классе системой информационной безопасности корпоративного уровня.

TippingPoint X505 использует передовые возможности систем предотвращения вторжений TippingPoint для непрерывной очистки сети от враждебного трафика: вирусов, «червей», «тройных программ», попыток «Фишинга», программ шпионов, угроз VoIP, а также другого вредоносного трафика. Для непрерывной защиты группа безопасности Digital Vaccine TippingPoint постоянно разрабатывает новые фильтры, также известные как виртуальные программные заплатки для своевременной защиты от попыток использования известных и вновь обнаруженных уязвимостей. Эти фильтры уязвимостей способны блокировать множество вариантов атаки на одну уязвимость, обеспечивая непрерывную защиту от угроз типа Zero-Day. В дополнение к фильтрам защиты служба Digital Vaccine производит обновление приобретенных клиентами устройств TippingPoint X505 множеством новых фильтров, предназначенных для защиты от различных угроз, таких как программы шпионы, «Фишинг» приложения и P2P.

Обновления цифровой вакцины Digital Vaccine поставляются клиентам автоматически каждую неделю или немедленно при обнаружении вновь выявленных критических уязвимостей или угроз.

«Рекомендованные настройки защиты» TippingPoint предоставляют возможность использования предварительно настроенных политик для автоматического и точного блокирования атак без проведения предварительной настройки, значительно снижая объем времени и ресурсов, необходи-

мых для защиты сети и обеспечения ее надежной и безопасной работы.

В дополнение к передовым функциям IPS платформа TippingPoint X505 включает IPSec VPN, брандмауэр с отслеживанием состояния соединения, фильтрацию веб-контента и основанное на политиках ограничение трафика, позволяющее с высокой точностью контролировать полосу пропускания как исходящего, так и входящего трафика. Одним из самых замечательных свойств платформы X505 является то, что все функции взаимокombинируемые. Например, в туннеле IPSec VPN могут совместно применяться система предотвращения вторжения IPS и ограничения трафика, эффективно защищая от распространения «червей» между филиалами предприятия, в то же время предоставляя приоритет телефонным звонкам VoIP между сайтами в целях улучшения качества голосовой связи VoIP.

Другой уникальной отличительной чертой платформы TippingPoint X505 являются возможности управления полосой пропускания. Работа таких некритических приложений, как файлообменные сети, может быть ограничена с целью высвобождения большой полосы пропускания. С другой стороны, работе таких критических приложений, как проведение видеоконференций или передача голоса по IP, может быть дан приоритет с целью обеспечения качества услуг. TippingPoint X505 также предоставляет возможность использования службы фильтрации веб-контента, которая повышает продуктивность работы и снижает риск ответственности организации путем включения соответствующей политики использования содержимого Интернета.

Платформа TippingPoint X505 поддерживается системой управления безопасностью TippingPoint SMS, платформой управления корпоративного уровня, которая предоставляет интуитивное управление множеством устройств TippingPoint IPS или X505. Система управления безопасностью TippingPoint SMS поставляется в виде предустановленного на заводе-изготовителе программного обеспечения, изначально упрощает процедуру установки, и является единственной системой управления IPS, обладающей механизмами обеспечения высокой доступности

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Производительность

- 50+ Мбит/с IPS
- 50+ Мбит/с VPN (3DES/AES)
- 100+ Мбит/с с использованием брандмауэра
- 128 000 подключений

Порты/выводы

- 4 порта данных 10/100
- 1 порт управления 10/100
- 1 консольный порт RS232/DB9
- 1 порт USB (зарезервировано для будущего использования)
- 1 вход стандарта IEC для подключения электропитания

Возможности

- Неограниченное количество пользовательских лицензий
- 50 зон безопасности (4 на физическом уровне)
- 250 ассоциаций безопасности с использованием протокола IPSec
- Поддержка одновременно 1000 туннелей виртуальной частной сети Phase 2 IPSec

Управление

- Локальный менеджер безопасности (HTTPS); CLI (локальная консоль, SSH); SNMP; система управления безопасностью TippingPoint SMS

VPN

- Шифрование 3DES/DES/AES
- Цифровые сертификаты/X.509
- Поддержка протоколов сервера PPTP и L2TP/IPSec для клиентского доступа к виртуальной частной сети

Режим развертывания брандмауэра

- Проверка пакетов с отслеживанием состояния соединений
- NAT (с маршрутизацией, прозрачная, смешанная), NAT/PAT, перенаправление портов и межзонный брандмауэр
- Работа по расписанию
- Настраиваемые службы/группы

Фильтрация контента и URL-адресов

- Встроенная фильтрация WEB трафика
- Черные и белые списки URL -адресов
- Возможность отмены положения фильтров с применением проверки подлинности
- Управляемый подпиской фильтр контента
 - 6 миллионов объединяемых по категориям URL-адресов
 - 40 категорий контента
 - 65 языков/200 стран
- Неограниченный размер базы данных

Стандарты и сертификаты безопасности

- UL 60950-1, EN60950-1, CSA 22.2 №.60950, IEC 60950

Устойчивость к ЭМИ

- EN55022 Class A, FCC Part 15 Class A, ICES-003 Class A, VCCI Class A, ANSI C63.4 Class As

Электропитание

- Напряжение на входе: 100 - 240 В переменного тока
- Частота напряжения: 50/60 Гц
- Потребляемый ток: 3 - 6 А (макс)
- Потребляемая мощность: 200 Вт (макс)

Условия окружающей среды

- Диапазон рабочих температур: 0 - 40°C
- Диапазон температур хранения: -20 - 80°C • Влажность: 5 - 95 % (без конденсации)

Размеры

- Возможен монтаж в рабочую стойку 19"
- Высота: 51 мм
- Ширина: 438 мм
- Глубина: 305 мм
- Вес: 5,8 Кг



сти и отказоустойчивости.

Упреждающие меры обеспечения безопасности сети

Платформа TippingPoint X505 основана на тех же передовых технологиях IPS и службы цифровой вакцинации Digital Vaccine, которые используются для информационной защиты тысяч корпоративных сетей во всем мире. Осуществляя полную, всеобъемлющую проверку пакетов по уровням 2-7, платформа X505 обеспечивает максимальную степень защиты для исключения возможности таких угроз, как вирусы, «черви», «троянские программы», смешанных угроз, DoS-атак, а также целого спектра иных угроз. Система предотвращения вторжений TippingPoint IPS обладает наибольшим количеством наград среди устройств того же класса.

Максимизация работы критических бизнес-приложений

Платформа TippingPoint X505 позволяет приоритезировать работу ответственных бизнес-приложений, работающих в режиме реального времени, включая приложения видеоконференций, IP -телефонии и интерактивного дистанционного обучения. Инновационный подход к организации туннелей обеспечивает безопасность работы широковеб-приложений для проведения видеоконференций как существующих, так и следующих поколений, а также иных критических бизнес-приложений. В частности, TippingPoint X505 способен приоритезировать как входящий, так и исходящий трафик приложения, в том числе внутри и снаружи туннеля IPSec VPN. Эта уникальная функция предоставляет возможность обеспечить высокое качество голосовых соединений VoIP для удаленных пользователей или офисов компании.

Фильтрация контента для контроля корректного использования Интернета TippingPoint X505 способна блокировать или ограничить работу некритических бизнес-приложений и применять политики корректного использования Интернет, тем самым улучшая производительность и снижая трафик, используемый не по назначению. Данная функция может ограничить использование доступа в Интернет только для корпоративных целей и обеспечить защиту от возможности привлечения к правовой или социальной ответственности за использование недопустимого веб-контента.

Фильтрация контента настраивается с помощью указания категорий, доступ к которым следует ограничить. База данных фильтров веб-узлов расположена на регионально-распределительных серверах и доступна устройствам X505 в реальном режиме времени, что устраняет необходимость загрузки постоянно увеличивающейся базы данных недопустимого веб-контента.

БЕЗОПАСНОСТЬ

Защита клиента и сервера

- Предотвращает атаки на уязвимые приложения и операционные системы
- Исключает необходимость в дорогостоящей установке специальных пакетов исправлений
- Блокирует составные атаки

Защита реального времени Digital Vaccine™ – «цифровая вакцинация» в реальном времени

- Превентивная защита от угроз
- Автоматическое распространение фильтров
- Рекомендованные настройки

Защита от программ шпионов и приложений Peer-to-Peer

- Обеспечивает защиту клиентов от заражения приложениями сruage
- Предотвращает заражение червями изнутри сети (от ноутбуков), а также несанкционированную выгрузку данных мобильных пользователей.
- Блокирует или ограничивает работу одноранговых соединений, а также программ мгновенных сообщений

Наличие нескольких зон безопасности

- Различные уровни применения политик:
 - Подсети отделов предприятия
 - Корпоративные демилитаризованные зоны DMZ
 - Сети ученик/учитель
 - Привилегии по времени суток

Гибкое управление политиками

- Объектно-ориентированные правила политик:
 - Сеть/зона безопасности/группа IP-адресов
 - привилегии по времени суток
 - Сервисное приложение
 - по расписанию/по времени суток
 - Туннели VRN
- Унифицированное управление несколькими службами:
 - Фильтрация веб-контента
 - Управление трафиком
 - Проверка подлинности пользователя
 - Управление устройством

Шифрование и проверка подлинности

- Использование шифрования нового поколения IPSec, в том числе аппаратного ускорения DES, 3DES и AES
- Проверка подлинности цифрового сертификата X.509 на основе данных как внутреннего, так и стороннего центров сертификатов
- Проверки подлинности пользователя через веб-интерфейс
- Группы, обладающие несколькими привилегиями

Мгновенный доступ к постоянно обновляемым базам недопустимых URL-адресов, обеспечивает Вам максимальную защиту.

Служба «цифровой вакцинации» Digital Vaccine™: Спокойствие и уверенность

Служба «цифровой вакцинации» Digital Vaccine TippingPoint - это служба ежегодной подписки, которая обеспечивает постоянное обновление платформы TippingPoint X505 для защиты от новых угроз. Служба Digital Vaccine также предоставляет доступ к Центру контроля угроз (ТМС) TippingPoint, который является центральной интеллектуальной службой для систем предотвраще-

- Локальная и внешняя базы данных RADIUS

Фильтрация URL-адресов

- Настраиваемые списки управления доступом к URL-адресам
- Использование регулярных выражений для описания URL-адресов

Фильтрация веб-контента

- Ежегодная подписка включает:
 - 40 категорий типов контента
 - Неограниченный список URL-адресов

КОММУНИКАЦИОННЫЕ ВОЗМОЖНОСТИ

Продвинутое управление трафиком

- Ограничение входящего и исходящего трафика:
 - VoIP
 - Трафик видео-конференций
 - Трафик критичных бизнес-приложений
- Приоритизация трафика внутри и вне туннелей VPN
- Гибкие способы контроля на основе политик:
 - Расписания по времени суток
 - Тип обслуживания

Встроенная поддержка клиента VPN

- Список поддерживаемых операционных систем включает:
 - Microsoft
 - Apple
- Список поддерживаемых протоколов включает:
 - PPTP
 - L2TP/IPSec
 - IPSec

Гибкость развертывания

- Поддержка смешанных сетей вне зависимости от топологии и схемы назначения IP-адресов:
 - Прозрачный режим работы
 - С поддержкой маршрутизации
 - NAT (в том числе Virtual Server и PAT)
 - Комбинированные развертывания
 - Динамическая маршрутизация (RIP V1 и 2)
 - 802.1Q VLAN Tagging

Широковещательная маршрутизация IP поверх протокола IPSec

- Поддержка широковеб-маршрутизации PIM-DM между сайтами внутри IPSec VPN функций, для поддержки приложений проведения IP-конференций нового поколения

ния вторжений TippingPoint IPS. Центр контроля угроз производит анализ появляющихся уязвимостей и постоянно разрабатывает новые сигнатуры и алгоритмы блокирования сетевых атак. Веб-узел Центра контроля угроз ПМС TippingPoint является основным ресурсом пользователей TippingPoint X505, предоставляя наиболее свежие на данный момент фильтры атак и обновления программного обеспечения, а также документацию по продуктам.