Trend Micro™

INTERSCAN™ WEB SECURITY

Превосходная защита от интернет угроз и управление безопасностью при доступе в Интернет

Традиционые системы защиты на уровне интернет-шлюза, опирающиеся на периодические обновления данных об угрозах, неспособны защитить в нынешних условиях. В дополнение к блокировке вредоносного кода, неуместных сайтов и целевых атак, администраторам безопасности также требуется обеспечить безопасное использование популярных сервисов на базе Web 2.0 и облачного ПО, снизив накладные расходы и загрузку каналов связи.

Trend Micro™ InterScan™ Web Security обеспечивает динамическую защиту в отношении киберугроз на уровне интернет-шлюза. Растущее число используемых пользователями на рабочем месте облачных приложений и сервисов требует прозрачности для понимания связанных с ними рисков. Путем интеграции контроля приложений, сканера наличия эксплойтов нулевого дня, антивирусной проверки, обнаружения APT, проверки веб-репутации в реальном времени, фильтрации URL и обнаружения ботнетов, InterScan Web Security обеспечивает превосходную защиту от сложных угроз. Помимо этого, опциональная интеграция с Deep Discovery Analyzer обеспечивает анализ подозрительных файлов в изолированной среде (песочницах), позволяя выявить и защитить организацию от абсолютно новых типов угроз и изощренных целевых атак (например, атак типа watering hole).
Вы сможете также предотвратить утечку данных благодаря встроенному модулю защиты от утечек (DLP), входящему в InterScan Web Security. Настраиваемые шаблоны, входящие в опциональный модуль Data Loss Prevention, отфильтруют данные в соответствии с требованиями регуляторов и политиками организации. Интеграция с DLP на веб-шлюзе реализует следующее:

- Контентная фильтрация исходящего трафика для выявления конфиденциальных данных
- Создание политик на базе настраиваемых шаблонов защитит персональную информацию, позволив добиться требуемого уровня соответствия регуляторам
- Формирование отчетов о нарушениях политик DLP с привязкой к пользователям
- Встроенные инструменты аудита для оценки эффективности политик DLP

БЕЗОПАСНОСТЬ НА УРОВНЕ ВЕБ-ШЛЮЗА

Аспекты защиты

- Интернет-шлюз

Блокирование угроз

- Облачные приложения
- Приложения Web 2.0
- Постоянные изощрённые угрозы (APT)
- Эксплойты нулевого дня
- Вредоносное ПО
- Потери данных
- Вирусы и черви
- Ботнеты и отклики к командным центрам управления (C&C)
- Шпионы и кейлоггеры
- Вредоносный мобильный код
- Руткиты
- Фишинговые атаки
- Угрозы в контенте

Интеграция с

- LDAP
- Active Directory™
- SNMP

ПРЕИМУЩЕСТВА

Превосходная защита

- Уменьшает нагрузку при защите оконечных систем, останавливая большую часть угроз на шлюзе путем интеграции сканера эксплойтов, антивирусного сканера, детектирования APT средствами веб-репутации, фильтрации URL, а также защиты Java апплетов и ActiveX
- Обеспечивает безопасное и целевое использование Интернет путем мониторинга опасного контента
- Блокирует угрозы по мере их возникновения
- Обеспечивает почти мгновенное получение новых данных об угрозах через обновления

Наглядность и управляемость

- Централизованное управление распределенными шлюзами в реальном времени
- Мониторинг использования веб ресурсов с устранением проблем по мере их обнаружения
- Управление и отчетность по более, чем 1000 интернет-протоколов и приложений
- Возможность создания гранулированных политик для контроля всех веб активностей с учетом времени, проведенного в Интернет

Проще и дешевле

- Повышает нормы использования существующих серверов, снижая издержки
- Работает как виртуальное или программное устройство для консолидации ЦОД и стандартизации
- Централизация управления распределенными веб-шлюзами по всему миру
- Улучшение уровней защиты за счет быстрой активации новых возможностей
- Меньше времени на восстановление после сбоев благодаря встроенным функциям отказоуйстойчивости и масштабируемости
- Упрощение процедур обновления ОС и данных об угрозах, контроля версионности и тестирования

ПРЕИМУЩЕСТВА

Контроль приложений

- Мониторинг и отчетность для более, чем 1000 интернет-протоколов и приложений, включая месенджеры, одноранговые сети, соцсети и потоковый медиаконтент
- Настраиваемые политики дают сотрудникам возможность использовать облачные сервисы, избегая рисков и сохраняя ресурсы
- Создание гранулированных политик обеспечивают контроль всех веб активностей с учетом затраченного сотрудником времени

Отмеченные наградами шлюзовые антивирус и антишпион

- Проверяет входящий и исходящий трафик на наличие вирусов
- Предотвращает проникновение вирусов в сеть, снижая нагрузку при антивирусной защите на настольных ПК
- Блокирует загрузку вирусов и шпионов, ботнеты, попытки откликов и туннелирования ВПО
- Закрывает «лазейку» в виде HTTPS благодаря его расшифровке и проверке контента
- Также возможна избирательная расшифровка HTTPS трафика, чтобы обеспечить сбалансированность защиты контента и приватности сотрудника

Веб репутация с корреляцией данных об угрозах

Технология веб репутации на базе Trend Micro™ Smart Protection Network™ блокирует доступ к сайтам с опасной активностью

- Защита в отношении новых угроз и подозрительной активности в реальном времени
- Выявляет и блокирует коммуникации с ботнетами и их командными центрами (C&C), используя глобальную и локальную аналитику

Мощные и гибкие средства фильтрации URL и активного кода

- Использует категоризацию и репутацию URL для определения нежелательных или опасных сайтов
- Предлагает на выбор шесть различных действий для настройки веб доступа, включая: мониторинг, разрешение, оповещение, блокировка, блокировка с парольным разрешением, временные квоты
- Поддерживает блокирование на уровне объекта внутри веб страниц, таких как гибридные приложения на базе технологии Web 2.0
- Блокировка скрытых загрузок и доступа к шпионским и фишинговым сайтам

Расширенная защита от угроз

Опциональная интеграция с Deep Discovery Analyzer дополняет традиционные средства возможностями запуска файлов в песочницах для выявления скрытых угроз в офлайне.

- Отправляет файлы в настроенную пользователем среду(ы) симуляции и отслеживает подозрительную активность
- Коррелирует полученные данные с глобальной базой угроз Trend Micro для получения данных об атаке и атакующем
- Использует адаптивные данные об угрозах для блокировки командных центров (C&C), обнаруженных в процессе анализа
- Идентифицирует атаки, используя непрерывно обновляемые данные об угрозах и правила корреляции, получаемые от глобальной сети Smart Protection Network и выделенной команды аналитиков

Возможности управления и отчетность в реальном времени

Централизация журналов, отчетности, управления настройками и синхронизации политик по всем серверам InterScan Web Security, независимо от их географии. Благодаря единой консоли, администраторы смогут более эффективно управлять всей защитой Интернет в компании от настройки политик до мониторинга.

- Непрерывный мониторинг Интернет активностей обеспечит полную прозрачность
- Простая отчетность станет инструментом принятия решений, позволив сразу же устранять найденные риски
- Централизация настроек и отчетности при эксплуатации в режиме распределенных офисов при множестве устройств
- Возможность создания настраиваемых отчетов
- Поддержка анонимного журналирования и отчетности для защиты приватности сотрудников
- Журналирование и отчетность с отдельных устройств централизованно обрабатываются в единой системе с целью снижения нагрузки на каждом из них и ретроспективной оценкой событий по всей инфраструктуре

Опциональный модуль iDLP

Расширяет существующую защиту, обеспечивая соответствие требованиям регуляторов и предотвращая утечки данных. Возможности DLP, встроенные в InterScan Web Security, могут быть активированы в одно нажатие.

- Отслеживает и фиксирует перемещение конфиденциальных данных наружу
- Идентифицирует рискованные бизнес-процессы и улучшает исполнение корпоративных политик
- Выявляет и предотвращает нецелевое использование данных (на базе слов, регулярных выражений и атрибутов файлов)
- Снижает число административных задач благодаря использованию единой системы управления на базе Control Manager, объединяющий данные всех решений Trend Micro в одной веб-консоли
- Установка модуля не требует какого-либо расширения мощностей оборудования или изменений ПО

Шаблоны Data Loss Prevention (DLP) для соответствия требованиям

Чтобы помочь защитить критически важные данные и выполнить ключевые требования регуляторов, в модуле предусмотрено 100 готовых шаблонов и возможность создания собственных

Требования регуляторов

- PCI/DSS — международный стандарт безопасности данных для платежных карт
- IBAN — International Bank Account Number

Персональные данные

- Банковская и финансовая информация
- Данные держателя платежной карты

Прочее

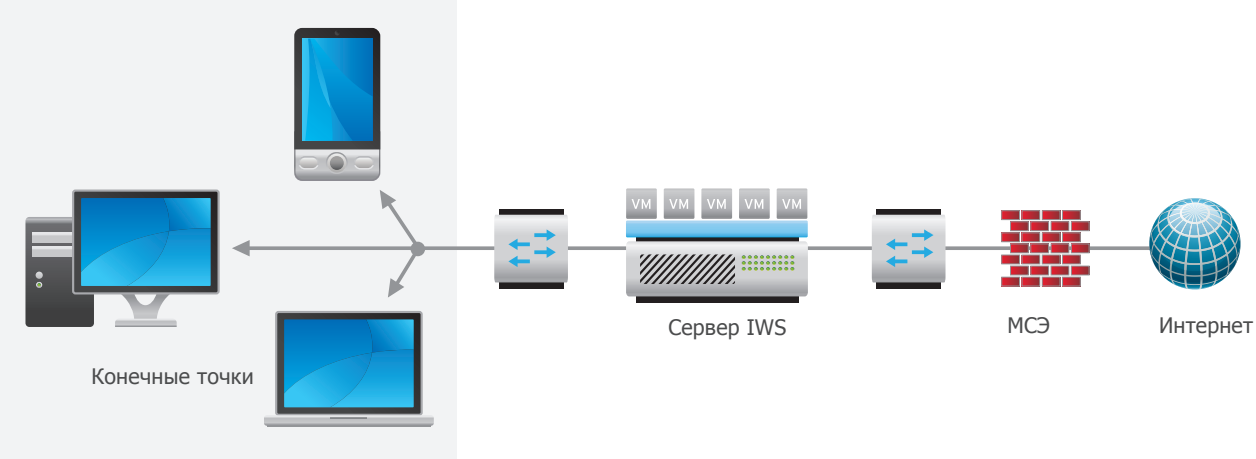
- Идентификаторы исходного кода
- Исполняемые файлы
- Более 170 типов файлов, включая MS Office , базы данных, мультимедийный контент и сжатые файлы
- И многое другое

ПОДДЕРЖИВАЕТ МНОЖЕСТВО ВАРИАНТОВ РАЗВЕРТЫВАНИЯ

InterScan Web Security (IWS) рассчитан на то, чтобы вписаться в любую инфраструктуру. Решение поддерживает множество вариантов установки, включая режим моста, ICAP, WCCP, явный и обратный режимы прокси.

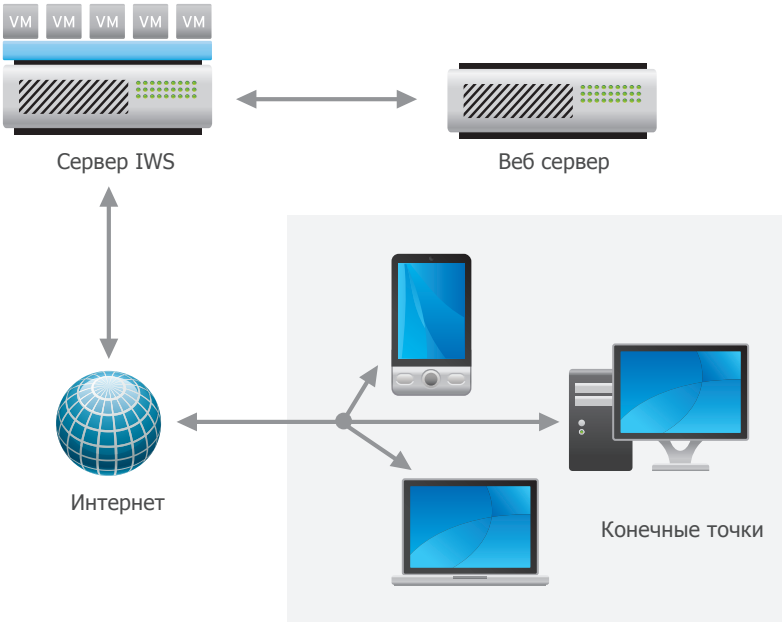
Режим прозрачного моста

В режиме прозрачного моста IWS объединяет два сетевых сегмента и прозрачно для пользователей сканирует весь трафик, а не только HTTP(s) и FTP. Режим моста является наиболее простым способом добавления решения в существующую топологию сети предприятия и не требует внесения изменений на уровне пользовательских систем, маршрутизаторов или коммутаторов. IWS действует по принципу “bump in the wire”, обеспечивая все функциональные возможности проверки контента.



Реверсивный прокси

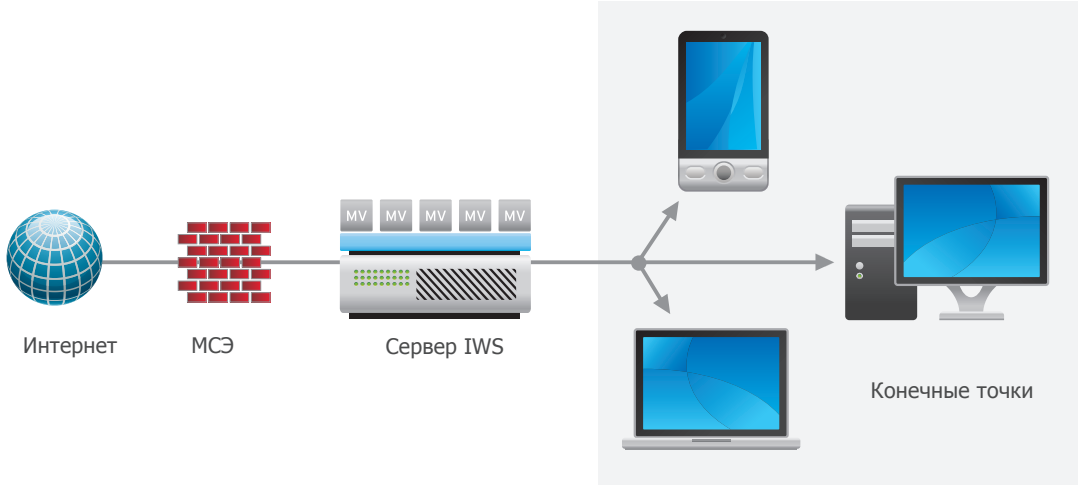
IWS может быть развернут в режиме реверсивного прокси для защиты веб сервера от выгрузки ВПО. В таком режиме решение устанавливается перед перед веб сервером, который он защищает. Режим реверсивног прокси полезен, когда веб сервер допускает выгрузку файлов от клиентов. Провайдеры услуг также могут использовать решение в качестве HTTP прокси для защиты и контроля трафика, полученного от клиентов, использующих интерактивные сайты.



ПОДДЕРЖИВАЕТ МНОЖЕСТВО ВАРИАНТОВ РАЗВЕРТЫВАНИЯ (продолжение)

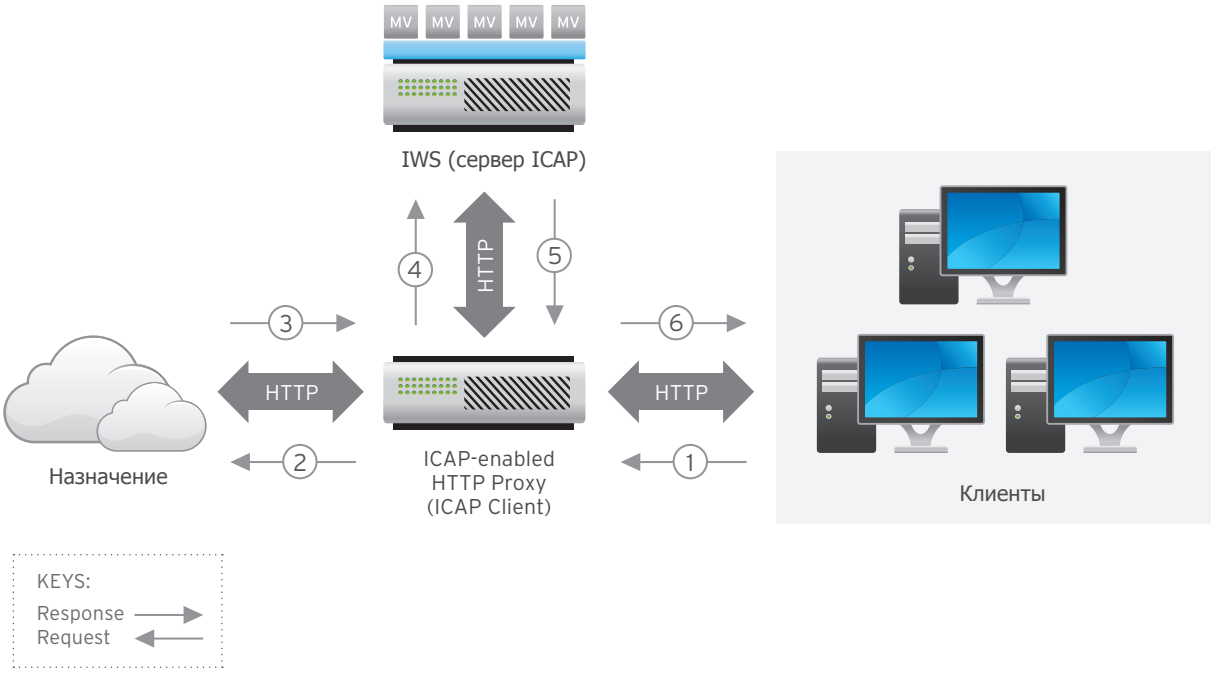
Явный прокси

IWS может быть развернут в качестве явно заданного для клиентов прокси сервера. Установка IWS как в режиме моста, так и в режиме явного прокси возможны с учетом специфики существующей инфраструктуры. Кроме того, поддерживаются режимы ICAP и WCCP, когда необходимо избирательно маршрутизировать интернет трафик со стороны существующего прокси или иного устройства.



Internet Content Adaption Protocol (ICAP)

IWS поддерживает интеграцию со сторонними кэширующими и обычными прокси серверами, а также сетевыми хранилищами через интерфейс ICAP v1.0 (например, Blue Coat Proxy, EMC Isilon Scale-Out Network-Attached Storage, NetApp NetCache и Cisco Content Engines). В таком режиме IWS принимает соединения ICAP от серверов с поддержкой ICAP v1.0, обеспечивая защиту контента, загруженного на сервер и наоборот - доставленного клиентам.



ВАРИАНТЫ РАЗВЕРТЫВАНИЯ

Программное устройство

- Установка специально подготовленного ПО с вшитой ОС на сертифицированное оборудование
- Certified by Trend Micro: Путем длительных и всесторонних проверок Trend Micro сертифицирует платформы на предмет совместимости с разрабатываемыми решениями. См перечень сертифицированных платформ на сайте Trend Micro www.trendmicro.com/go/certified

Виртуальное устройство

- Развертывание в виртуальной среде с использованием технологий гипервизора
- Microsoft® Hyper-V™ Virtual Appliance
- VMware Ready Virtual Appliance: Rigorously tested and validated by VMware, achieving VMware Ready validation. Supports VMware ESX or ESXi v3.5+ and vSphere

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ

Совместимость с серверными платформами

Виртуальные устройства:

- VMware ESX/ESXi v3.5 или выше; Microsoft Hyper-V Windows 2008 SP1 или Windows 2008 R2
- Windows Server 2012 Hyper-V

Программные устройства

- Наиболее актуальные данные по сертифицированным платформам можно найти на сайте Trend Micro www.trendmicro.com/go/certified

Процессор

Минимальные требования:

- Single 2.0 GHz Intel™ Core2Duo™ 64-bit processor supporting Intel VT™ or equivalent

Рекомендованные требования:

- До 4000 пользователей: Dual 2.8 GHz Intel Core2Duo 64-bit processor or equivalent
- До 9500 пользователей: Dual 3.16 GHz Intel QuadCore™ 64-bit processor or equivalent

Память

Минимальные требования:

- 4GB RAM

Рекомендованные требования:

- До 4000 пользователей: 6GB RAM
- До 9500 пользователей: 24GB RAM
- До 15,000 пользователей: 32GB RAM

Дисковое пространство

Минимальные требования:

- 20GB RAM

Рекомендованные требования:

- 300GB of disk space (Automatically partitions the detected disk space as required)

TREND MICRO™

Securing Your Journey to the Cloud