

«Чистый Веб»: описание услуги

«Чистый Веб» представляет собой доступный по подписке веб-сервис для любых организаций, которым необходима всесторонняя защита безопасности при работе с веб-ресурсами. Подключив услугу «Чистый Веб», вы сможете использовать преимущества самых передовых технологий McAfee и ЗАО "Демос-Интернет", включая TrustedSource™, McAfee SmartFilter® и McAfee® Web Gateway Anti-Malware, для фильтрации веб-ресурсов по категориям, на основе их репутации и для защиты от вредоносных программ.

Полная защита входящего и исходящего трафика

«Чистый Веб» предоставляет комплексную защиту всего Web 2.0 трафика. Данная служба позволяет компаниям использовать собственные политики безопасности для автоматического контроля доступа. Трафик, не соответствующий правилам безопасности, блокируется еще до попадания в корпоративную сеть. Для разрешенного трафика служба использует современные средства анализа данных и активного кода в запрошенных web-страницах, тем самым, предоставляя мгновенную защиту против вирусов и другого вредоносного ПО.

Безопасность как услуга для организаций любого размера

«Чистый Веб» предлагает новейшую систему безопасности, которая отличается чрезвычайно простым и эффективным способом развертывания. Нет необходимости в установке программного обеспечения и дополнительного оборудования. Это делает систему быстрой и легкой в использовании.

Не надо заниматься конфигурированием, обновлением и поддержкой. Все это позволяет развертывать высокоэффективную систему при минимальных начальных вложениях и затратах на содержание. Экономится бюджет и ресурсы собственных IT служб клиентов, которые могут быть направлены на решение других важных задач.

Динамичное и интерактивное содержание технологии Web 2.0 открывает двери для новых угроз безопасности, способных преодолеть традиционные средства контроля. Для защиты сотрудников, клиентов, корпоративных сетей и интеллектуальной собственности организации нуждаются в современной системе веб-безопасности. Это должна быть система не просто блокирующая известные вирусы, а еще и способная противостоять скрытым и неизвестным атакам и вредоносным программам.

«Чистый Веб» использует современный анализ содержания кода для блокирования нежелательного контента из веб-трафика. Сканируя активный код и анализируя его содержание и возможное поведение, «Чистый Веб» активно борется со скрытыми угрозами и целенаправленными атаками.

Кроме этого, высокая эффективность, пренебрежимо малые задержки, постоянная доступность и исключительная степень масштабируемости позволяет системе обеспечивать безопасность в самых сложных условиях работы.

Простая интеграция

Отсутствие необходимости в установке ПО на собственном оборудовании избавляет компании от рисков несовместимости программ. В действительности, осуществляется простое перенаправление вашего трафика на мощные сервера дата-центра Демос-Интернет, где трафик проверяется современными средствами контроля. Дата-центр Демос-Интернет спроектирован с учетом требований производительности, достаточной для обработки запросов всех клиентов. В результате конечный пользователь получает безопасный веб-трафик без ощутимых задержек. Посредством интеграции с LDAP и Active Directory организации могут применять политики безопасности к существующим группам пользователей. Пользователи прозрачно идентифицируются без дополнительных программ или изменений в сетевой инфраструктуре, а политики автоматически применяются для каждого конкретного пользователя на основе политики, назначенной его группе.

Веб-фильтрация

Категории веб-сайтов определяются с использованием объективных стандартов и определений. Выбор политики, определяющей категории, которые будут блокироваться, осуществляется в соответствии с принятыми в организации правилами. Благодаря управлению доступом к веб-ресурсам по категориям и применению политик доступа в Интернет в соответствии со спецификой своих потребностей, организации получают возможность:

- Повысить безопасность при работе с веб-ресурсами
- Ввести в действие принятые в организации политики просмотра веб-ресурсов
- Повысить производительность труда
- Уменьшить риски, связанные с нарушением законодательства
- Сфокусировать использование доступа в Интернет на вопросах, касающихся бизнеса

Выбор из более чем 90 категорий в дополнение к преимуществам использования технологии TrustedSource предоставляет непревзойденные возможности по охвату, точности и эффективности защиты web-трафика.

Фильтрация на основе репутации

«Чистый Веб» предоставляет наилучшую защиту, используя комбинацию из системы репутации сайтов и фильтров на основе категорий. Защита на основе репутации сайтов с помощью технологии TrustedSource™ McAfee устанавливает новый стандарт проактивной безопасности с использованием технологии TrustedSource – крупнейшей глобальной системы репутации сайтов. TrustedSource собирает информацию с более чем 10000 сенсоров, расположенных в 82 странах по всему миру и создает досье на любую активность в Интернете по всем сетевым протоколам. Веб-база данных TrustedSource классифицирует похожие типы URL (веб-страницы) по группам в зависимости от категории содержимого и веб-репутации. TrustedSource вычисляет значение репутации, которое в реальном времени показывает степень риска, которому подвергается пользователь при посещении конкретного URL. Чем выше число репутации, тем больше степень риска. Для получения дополнительной информации о веб-репутации посетите веб-сайт www.trustedsource.org

Система обнаруживает отклонение от ожидаемого поведения и создает оценки репутации, характеризующие поведение каждого хоста. При более серьезных угрозах специальные сигналы тревоги оповещают администраторов системы. Применяя постоянный мониторинг Интернета и отслеживая глобальные угрозы безопасности, TrustedSource обеспечивает непревзойденную способность обнаруживать неизвестные и скрытые атаки.

Проактивная защита от вредоносных программ (Anti-Malware) и вирусов

В услуге «Чистый Веб» используются все преимущества Anti-Malware движка McAfee для усовершенствованной защиты против вирусов, троянов, шпионских программ и других угроз Web 2.0. Движок Anti-Malware имеет в своем составе несколько предупреждающих фильтров, сканирующих содержимое веб-страниц, передаваемых по протоколам http и https (SSL), и определяющих их намерения или предсказуемую активность. Посредством сканирования активного содержимого веб-страниц и понимания его намерений или предсказуемого поведения движок Anti-Malware проактивно защищает от смешанных угроз и целевых атак.

Данная проактивная защита против неизвестных вирусов сочетается с комплексным антивирусным модулем, основанным на поиске сигнатур, для блокирования известных атак. В результате данное комплексное решение предоставляет наилучшую защиту от всех возможных web-угроз.

Как это работает

На первоначальном этапе «Чистый Веб» настраивается в соответствии со спецификой подключения к Интернет и потребностями конкретной организации. Учитываются особенности аутентификации и перенаправления трафика. По завершении первоначального этапа пользователи могут начать пользоваться браузерами. Рисунок 1 иллюстрирует как «Чистый Веб» работает по запросу пользователя:

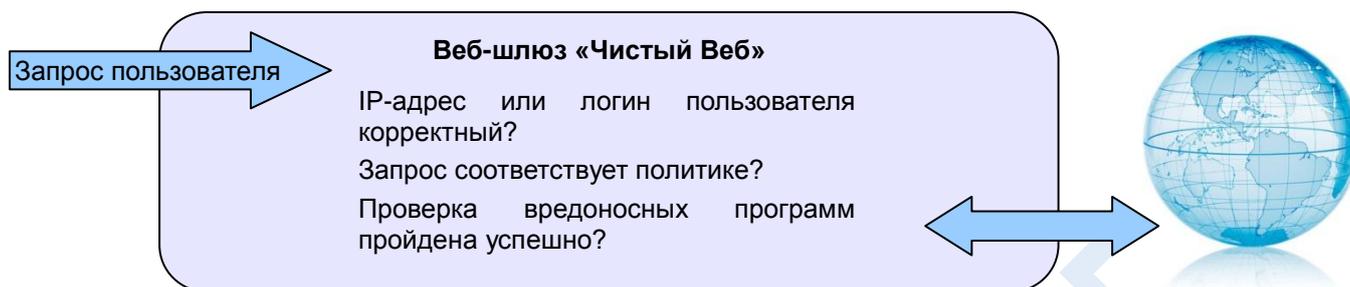


Рис. 1 Запросы пользователя

Когда пользователь запрашивает содержимое веб-страницы, «Чистый Веб» выполняет следующие операции:

- Запрос пользователя перенаправляется на веб-шлюз «Чистый Веб».
- Проверка корректности IP-адреса или логина пользователя.
- Привязка запроса к политике и проверка на категорию и репутацию.
- Получение веб-страницы из Интернет (если его нет в кэше).
- Применение фильтров политики.
- Сигнатурная и проактивная проверка (антивирусное и вредоносное ПО).

Если запрос успешно проходит все эти проверки, то «Чистый Веб» передает веб-страницу пользователю. Если — нет, то «Чистый Веб» выполняет операции в соответствии с вашими настройками.

Управление и отчеты

Организации получают в свое распоряжение инструмент, помогающий определить тенденции использования веб-ресурсов, локализовать проблемы, документировать нежелательную активность на веб.

Ключевые преимущества

Уменьшение затрат в сочетании с более высокой производительностью и масштабируемостью по сравнению с аппаратными решениями

Легкость внедрения

Без необходимости установки дополнительных программ и оборудования организации получают безопасность корпоративного класса с низкими первоначальными и эксплуатационными затратами.

Мощная защита в реальном времени

Постоянно активная защита от вредоносных программ и актуальная информация о репутации Интернет-ресурсов в TrustedSource защищают даже от новейших угроз Web 2.0, причем до проникновения в сеть вредоносного ПО.

Простое управление 24/7

Портал управления с веб-интерфейсом обеспечивает легкость настройки параметров безопасности и управление политиками фильтрации во всех филиалах организаций. Полностью настраиваемая панель управления обеспечивает немедленный доступ к необходимой информации.

Масштабируемость и производительность

Даже крупные организации могут рассчитывать на практически неограниченную масштабируемость с минимальными задержками и без необходимости установки дополнительного оборудования по мере увеличения трафика.

Отчеты и панель управления

Мгновенные снимки текущего состояния, персональные настройки панели администрирования и быстрый доступ к необходимым данным позволяют быть во всеоружии.

Уведомления и предупреждения

Настраиваемые системы предупреждений извещают пользователей о нарушениях и блокировании веб-трафика.

Приложение №1

Категории фильтрации основные

| Название категории | Бизнес |
|-----------------------------|--------|
| Алкоголь | X |
| Анонимайзеры | X |
| Преступная деятельность | X |
| Наркотики | X |
| Экстрим | X |
| Азартные игры | X |
| Игры с присутствием насилия | X |
| Авторский контент | X |
| Ненависть/Дискриминация | X |
| Нелегальное ПО | X |
| Нагота | X |
| P2P/Файл шаринг | X |
| Фишинг | X |
| Порнография | X |
| Провокационные материалы | X |
| Сексуальные материалы | X |
| Социальные сети | X |
| Спамерские адреса | X |
| Шпионское / Вредоносное ПО | X |
| Табак | X |
| Насилие | X |

X – доступ запрещен.

Политика фильтрации контента «Бизнес» (Стандартная политика)

Фильтрация URL

Антивирусная защита

Защита от вредоносного ПО

Проактивная защита

Проверка зашифрованного трафика (SSL)

Политика фильтрации контента «Веб-Почта»

Фильтрация URL

Закрывает доступ к бесплатным ресурсам, предоставляющим доступ к веб-почте

Политика фильтрации контента «Детям до 16»

Фильтрация URL

Антивирусная защита

Защита от вредоносного ПО

Проактивная защита

Проверка зашифрованного трафика (SSL)

Дополнительно закрыт доступ к контенту «для взрослых» на основе ключевых слов (body filter) и добавлены более жесткие категории фильтрации. (см. Приложение №2)

Приложение №2

к Регламенту предоставления доступа к БД «ЧистыйВеб»

Категории фильтрации по URL

| Название категории | Бизнес | Детям до 16... | Веб-почта минус |
|--------------------------------------|--------|----------------|-----------------|
| P2P/Файл шаринг | X | X | |
| Авторский контент | X | X | |
| Азартные игры | X | X | |
| Алкоголь | X | X | |
| Анонимайзеры | X | X | |
| Анонимное ПО | | X | |
| Аптека | | X | |
| Аукционы / Объявления | | X | |
| Бизнес | | | |
| Блоги / Вики | | | |
| Веб-встречи | | | |
| Веб-объявления | | | |
| Веб-почта | | X | X |
| Веб-телефония | | X | |
| Визуальная поисковые системы | | X | |
| Вредоносные сайты | | X | |
| Главные новости | | | |
| Для детей | | | |
| Здоровье | | | |
| Знакомства | X | X | |
| Игры | | X | |
| Игры с присутствием насилия | X | X | |
| Интерактивные веб-приложения | | | |
| Интернет Радио/ТВ | | | |
| Интернет Сервисы | | | |
| Информационная безопасность | | X | |
| Искусство / Культура / Наследие | | | |
| Исторический ревизионизм | | | |
| История | | | |
| Компьютерная преступность | | X | |
| Контент Сервер | | | |
| Личное сетевое хранилище | | X | |
| Маркетинг / Реклама на месте продажи | | | |
| Мгновенные сообщения | | X | |
| Медиа загрузки | | X | |
| Медиа шаринг | | | |
| Мобильный телефон | | X | |

| | | | |
|---|---|---|--|
| Мода / Красота | | X | |
| Нагота | X | X | |
| Наркотики | X | X | |
| Насилие | X | X | |
| Недвижимость | | | |
| Нелегальное ПО | X | X | |
| Ненависть/Дискриминация | X | X | |
| Ненормативная лексика | | X | |
| Новости Usenet | | | |
| Образование / Справка | | | |
| Онлайн покупки | | X | |
| Оружие | | X | |
| Отдых / Хобби | | | |
| Переводчики | | | |
| Персональные страницы | | X | |
| Поиск работы | | | |
| Поисковые системы | | | |
| Политика | | | |
| Порнография | X | X | |
| Портальные сайты | | | |
| Потоковый медиаконтент | | | |
| Правительство / Военные | | | |
| Преступная деятельность | X | X | |
| Провокационные наряды | X | X | |
| Программное обеспечение / оборудование | | | |
| Промодерированный контент | | | |
| Профессиональные сети | | | |
| Публичная информация | | | |
| Путешествия | | | |
| Развлечение | | | |
| Религия / идеология | | | |
| Рестораны | | | |
| Сексуальные материалы | X | X | |
| Случайное обнажение | X | X | |
| Совместное использование ресурсов | | X | |
| Сообщения | | X | |
| Социальные сети | X | X | |
| Спамерские адреса | X | X | |
| Спорт | | | |
| Табак | X | X | |
| Техническая информация | | | |
| Технические бизнес форумы | | X | |

| | | | |
|--------------------------|---|---|--|
| Транспортные средства | | | |
| Удаленные доступ | | X | |
| Условно бесплатное ПО | | X | |
| Финансы / Банковское | | | |
| Фишинг | X | X | |
| Фондовая Торговая | | X | |
| Форум / Доски объявлений | | X | |
| Хостинг доменов | | X | |
| Цифровые открытки | | X | |
| Чаты | | X | |
| Школьные шпаргалки | | X | |
| Шпионское/Вредоносное ПО | X | X | |
| Экстрим | X | X | |
| Юмор | | | |

X – доступ запрещен.