Сравнение средств защиты и контроля доступа в Интернет

Решения Cisco по защите и контролю доступа в Интернет — это лучшая защита от угроз и самые продвинутые методы контроля над динамически меняющимся интернет-контентом и приложениями для всех пользователей, независимо от их местоположения.

Выявление и анализ угроз	Быстрая, комплексная веб-защита, основанная на самой крупной в мире сети обнаружения угроз. Аналитический центр Cisco Collective Security Intelligence (CSI) круглосуточно отслеживает мировой трафик, чтобы компания Cisco могла анализировать аномалии, выявлять новые угрозы и отслеживать тенденции распределения трафика. Этот центр генерирует новые правила, передающие обновления каждые три-пять минут. Благодаря этому наша компания обеспечивает лучшую в отрасли защиту от атак на несколько часов или даже дней раньше, чем конкуренты.
Сканирование для выявления вредоносного ПО в режиме реального времени	Предотвращение атак нулевого часа при помощи нескольких модулей защиты от вредоносного ПО, выполняемых одновременно. Каждый сегмент веб-контента, к которому обращается пользователь (код HTML, изображения, видеоролики в формате Flash и т. п.) проходит анализ с помощью модулей сканирования для обеспечения безопасности с учетом контекста.
Фильтрация URL-адресов, динамический анализ контента, распределение по категориям в режиме реального времени	Устранение рисков злоупотребления, нарушения нормативов и снижения производительности при помощи постоянно обновляемой базы данных URL-адресов Cisco и технологии распределения неизвестных URL-адресов по категориям в режиме реального времени. Администраторы также могут выбрать политики для анализа протокола HTTPS.
Мониторинг и контроль приложений (Application Visibility and Control, AVC)	Контроль использования мобильных приложений, приложений для совместной работы и приложений Web 2.0, а также управление действиями пользователей в этих приложениях. Cisco Web Security выявляет и контролирует несколько сотен приложений и 150 000 микроприложений.
Предотвращение потери данных (Data Loss Prevention, DLP)	Предотвращение утечки конфиденциальных данных из сети путем создания базовых правил DLP на основе контекста. Cisco применяет протокол ICAP (Internet Content Adaptation Protocol, протокол адаптации веб-контента) для интеграции со сторонними решениями DLP в целях более эффективной защиты.
Защищенная мобильность	Защита пользователей, находящихся за пределами корпоративной сети, благодаря интеграции решений Cisco Web Security с безопасным клиентом для мобильных устройств Cisco AnyConnect®.
Централизованное управление и отчетность	Создание отчетов с практическими рекомендациями по угрозам, данным и приложениям. Решения Cisco Web Security предоставляют эффективные централизованные средства для контроля над процессами системы безопасности (например, для управления) и сетевыми процессами (например, для анализа пропускной способности).

Не существует единого универсального подхода к обеспечению безопасности, и не существует единого способа применения средств и технологий Web 2.0 в организациях, поскольку это зависит от потребностей бизнеса, структуры, персонала и культуры. Поэтому у предприятий должен быть выбор. Cisco предлагает целый ряд инновационных решений, реализованных как физически (на территории клиента), так и в виде облачных сервисов, которые предназначены для того, чтобы обеспечить ИТ/ИБ-специалистам на предприятии прозрачность и контроль за работой Web-приложений с целью исключения возможных угроз со стороны Web 2.0 и социальных сетей.

Сравнение средств защиты и контроля доступа в Интернет

	Cisco Web Security Appliance	Cisco FirePOWER Services for ASA	Cisco FirePOWER NGFW	Cisco Cloud Web Security
Основное предназначение	Контроль и защита доступа в Интернет на стороне заказчика	Защита от широкого спектра угроз (расширение Cisco ASA 5500-X)	Защита от широкого спектра угроз	Контроль и защита доступа в Интернет в виде модели SaaS
Фильтрация по категориям	Да (Cisco URL Filtering)	Да (Webroot, в будущем Cisco URL Filtering)	Да (Webroot, в будущем Cisco URL Filtering)	Да (Cisco URL Filtering)
Контроль приложений	Да, движок AVC (только HTTP/HTTPS трафик)	Да (все порты, все протоколы)	Да (все порты, все протоколы)	Да, движок AVC (только HTTP/HTTPS трафик)
Репутационные фильтры	Да (Web Reputation)	Да (собственная база, Web Reputation в будущем)	Да (собственная база, Web Reputation в будущем)	Да (Web Reputation + Conginive Security)
Источник обновления баз категорий и URL	Cisco Collective Security Intelligence	Cisco Collective Security Intelligence	Cisco Collective Security Intelligence	Cisco Collective Security Intelligence
Защита от вредоносного кода	Движки Cisco IronPort DVS™, Webroot™, Sophos, AMP и McAfee	Движок AMP	Движок AMP	Движки McAfee, Webroot, Sophos и AMP
Аутентификация пользователя	Активная (запрос логина и пароля) и пассивная (через AD, LDAP, Kerberos и NTLM)	Аутентификация на базе протоколов (AIM/IMAP/LDAP/ Oracle/ POP3/SIP) и пассивная	Аутентификация на базе протоколов (AIM/IMAP/LDAP/Oracle/ POP3/SIP) и пассивная	Активная (запрос логина и пароля), пассивная (через AD), PIM, SAML и NTLM
Групповые политики	Да, с привязкой к Active Directory	Да, с привязкой к Active Directory	Да, с привязкой к Active Directory	Да
Контроль мобильных и удаленных пользователей	Да (AnyConnect)	Нет встроенной поддержки, но можно заворачивать трафик через VPN	Нет встроенной поддержки, но можно заворачивать трафик через VPN	Да (AnyConnect)
Кеширование HTTP-трафика	Да	Нет	Нет	Нет
Обнаружение утечек информации (DLP)	Да (базовый встроенный DLP, перенаправление на внешний DLP с помощью ICAP)	Нет	Нет	Нет
Способы перенаправления трафика	Прокси, WCCP, policy-based routing	На пути трафика	На пути трафика	Прокси, коннектор (ASA и IOS), AnyConnect
Отчетность/ Интеграция с SIEM	Встроенная/Да	Встроенная/Да	Встроенная/Да	Встроенная/Да
Обработка SSL	Встроенные возможности	С помощью отдельного SSL Appliance (в будущем встроенная)	С помощью отдельного SSL Appliance (в будущем встроенная)	Встроенные возможности (HTTPS Inspection)
Варианты развертывания	Аппаратное или виртуальное устройство	Аппаратный или программный модуль для Cisco ASA	Аппаратное или виртуальное устройство	Облачный сервис
Пропускная способность	До 12000 пользователей	До 15 Гбит/сек	До 120 Гбит/сек	Зависит от используемого коннектора
Масштабирование	Добавление новых WSA с распределением трафика с помощью WCCP или балансировщика	Замена на более производительные устройства	Замена на более производительные устройства или стекирование	Зависит от доступной полосы пропускания

По всем вопросам, связанным с решениями Cisco по информационной безопасности, обращайтесь по e-mail: security-request@cisco.com.