

# Cisco ASA с сервисами FirePOWER



Представляем первый в отрасли адаптивный межсетевой экран нового поколения (NGFW), предназначенный для расширенной защиты от новейших угроз и вредоносных программ. Cisco® ASA с сервисами FirePOWER™ обеспечивает интегрированную защиту от угроз на протяжении всего процесса атаки – перед ее началом, во время атаки и после ее завершения. Он объединяет в одном устройстве возможности защиты меж сетевого экрана Cisco ASA и лучшие в отрасли функции защиты от угроз и вредоносных программ Sourcefire®. Это решение расширяет возможности меж сетевого экрана Cisco ASA серии 5500-X и превосходит другие решения NGFW.

Самый надежный в отрасли межсетевой экран ASA включает систему предотвращения вторжений нового поколения (NGIPS) и улучшенные средства защиты от вредоносных программ Sourcefire. Это решение доступно на платформах NGFW Cisco ASA серий 5500-X и 5585-X.

## Выход за границы традиционной концепции защиты «Эшелонированная оборона»

Традиционная концепция «Эшелонированная оборона» предполагает приобретение организациями целого ряда решений по безопасности – включая межсетевые экраны, шлюзы VPN, веб-фильтры и прочие приложения – от разных поставщиков. Такой подход повышает сложность сетевой архитектуры, поскольку эти продукты не всегда совместимы. Отсутствие унифицированной системы защиты создает множество белых пятен, которые повышают уязвимость организаций. Злоумышленники используют эти уязвимости для атак, о которых компании зачастую даже не догадываются. Как правило, организациям приходится создавать несколько служб для установки и управления этими разрозненными решениями защиты. Эти службы безопасности пытаются устранить пробелы в системе защиты, выполняя процедуры вручную. Такой подход неэффективен и ненадежен. Такая среда не позволяет быстро реагировать на изменения ландшафта угроз.

Межсетевой экран Cisco ASA с сервисами FirePOWER объединяет несколько уровней безопасности на одной платформе, что снижает стоимость приобретения нескольких решений и управления ими. Такой интегрированный подход сочетает лучшую в своем классе технологию безопасности с многоуровневой защитой, которые интегрированы в одно устройство. Это обеспечивает значительную экономию по сравнению с разрозненными решениями защиты. Кроме того, вы

получаете прозрачность всех объектов и событий сети, которая значительно превосходит возможности, предлагаемые традиционными решениями. Имея полную контекстуальную информацию, вы сможете видеть все ресурсы, для которых требуется защита. Белые пятна, используемые злоумышленниками для совершения атак, полностью устраняются. Полная прозрачность сети позволяет быстро обнаруживать и классифицировать угрозы в зависимости от степени риска. Система автоматически оценивает возможные последствия и расставляет приоритеты. При этом сокращается число событий, связанных с мониторингом и реагированием на угрозы. Операции выполняются в потоковом режиме, что значительно сокращает время обнаружения и устранения угроз.

## Непревзойденная прозрачность сети

Управление межсетевым экраном Cisco ASA с сервисами FirePOWER осуществляется централизованно через консоль управления Cisco FireSIGHT™ Management Center, которая предоставляет службам безопасности полный контроль всех действий в сети. Это распространяется на пользователей, устройства, обмен данными между виртуальными машинами, уязвимости, угрозы, клиентские приложения, файлы и веб-сайты. Целостная действенная система обнаружения признаков вторжения сопоставляет подробную информацию о событиях в сети и на терминальных устройствах и выявляет заражение.

Кроме того, Cisco FireSIGHT Management Center предоставляет сведения о движении вредоносных файлов. Это помогает отследить распространение вируса, чтобы определить и быстро устранить источник заражения.

Решение Cisco Security Manager помогает управлять масштабируемым и централизованным потоком сетевых операций. Оно включает богатый набор функций, в том числе управление политиками и объектами, управление событиями, подготовку отчетности и устранение неполадок меж сетевого экрана Cisco ASA. Для маленьких и простых систем Cisco Adaptive Security Device Manager (ASDM) предоставляет средство управления операциями меж сетевого экрана на основе графического интерфейса пользователя.

Инструменты управления корпоративного класса Cisco помогают администраторам упростить системы, повысить прозрачность сети и обеспечить полный контроль межсетевых экранов нового поколения.



## Возможности и преимущества

Cisco ASA с сервисами FirePOWER предоставляет следующие возможности.

- **Высокая прозрачность и контроль приложений (AVC).** Более 3000 элементов управления на уровне приложений в случае риска могут активировать политики обнаружения угроз IPS, что позволяет значительно повысить эффективность защиты.
- **Ведущий в отрасли межсетевой экран Cisco ASA с системой предотвращения вторжений нового поколения FirePOWER (NGIPS).** Высокоэффективная система предотвращения атак и полная контекстуальная информация о пользователях, инфраструктуре, приложениях и содержимом позволяют обнаруживать многовекторные угрозы и автоматизировать процесс защиты.
- **Фильтрация URL-адресов по репутации и категориям.** Фильтрация URL-адресов обеспечивает комплексное оповещение и контроль над подозрительным веб-трафиком. Она применяет политики для сотен миллионов URL-адресов в более чем 80 категориях.
- **Усовершенствованная защита от вредоносного ПО.** Эффективное обнаружение вторжений и низкая стоимость владения обеспечивают оптимальный вариант защиты, позволяющий быстро выявлять, анализировать и предотвращать распространение вредоносного ПО и возникающих угроз, которые могут быть пропущены на других уровнях защиты.

## Преимущества решений Cisco

Межсетевой экран Cisco ASA – это наиболее широко применяемый в мире межсетевой экран корпоративного уровня с удаленным доступом к сетям VPN и расширенными возможностями кластеризации. Быстрый и безопасный доступ и высокая надежность систем обеспечивают непрерывность бизнес-процессов. Решение было разработано компанией Cisco – мировым лидером в области безопасности сетей, которая занимается разработкой межсетевых экранов уже более 15 лет. Благодаря приобретению компании Sourcefire – лидера по разработке интеллектуальных решений в области информационной безопасности – компания Cisco еще лучше может обеспечивать высокий уровень прозрачности, автоматизации и комплексной защиты от угроз на протяжении всего процесса атаки.

## Дальнейшие шаги

Подробные сведения о межсетевом экране Cisco ASA с сервисами FirePOWER можно получить на веб-сайте [www.cisco.com/go/asafps](http://www.cisco.com/go/asafps).