УГРОЗООРИЕНТИРОВАННЫЙ МЕЖСЕТЕВОЙ ЭКРАН НОВОГО ПОКОЛЕНИЯ CISCO FIREPOWER

СКОТТ ХАРРЕЛЛ (SCOTT HARRELL)

Цифровая революция, которую переживает современный мир, ведет к небывалому росту количества подключений. Вместе с тем больше возможностей получают и киберпреступники. Чтобы обеспечить предприятиям высочайший уровень защиты и тем самым расширить их возможности в мире цифровых технологий, компания Cisco сделала информационную безопасность приоритетным направлением своей деятельности. На днях компания анонсировала первый полностью интегрированный угрозоориентированный межсетевой экран нового поколения Cisco Firepower серии 4100 для высокопроизводительных приложений, используемых средним и крупным бизнесом.

Обычно ИТ-подразделениям приходится решать проблемы информационной безопасности (ИБ) с помощью набора отдельных специализированных продуктов, в частности обычных межсетевых экранов (МСЭ), чьи возможности защиты от сложных угроз — всего лишь опция. Такие МСЭ не могут обеспечить предприятиям тот уровень автоматизации, ранжирования, осведомленности о контексте, который необходим, чтобы справляться с современными угрозами.

Использование обычных МСЭ не позволяет обслуживающим организациям выполнить обязательства по консолидации платформ и снижению сложности. Более того, им приходится либо разворачивать специальные защитные платформы, либо получать телеметрические данные от обычных МСЭ нового поколения и передавать на другие системы, которые эти данные анализируют и предоставляют сведения о контексте, но уже не в режиме реального времени. Эта структура напоминает Франкенштейна (монстра, созданного из разных частей тела): масса разрозненных технологий, собранных воедино, для управления которыми нужно переключаться между множеством консолей. Такой подход к безопасности необоснованно дорог, сложен и малоэффективен.

Справиться с этими проблемами призван созданный с чистого листа и недавно представленный компанией Cisco МСЭ нового поколения серии 4100 — первый полностью интегрированный, угрозоориентированный МСЭ для защиты организаций [1]. В отличие от обычных МСЭ, он проще и экономичнее, обеспечивает целостный подход к безопасности, а управлять им гораздо удобнее благодаря единому интерфейсу. Следует подчеркнуть, что разработчики придерживались стратегии не наращивать количество устройств и консолей в и без того громоздком стеке технологий безопасности, с которым обычно вынуждены иметь дело компании.

МСЭ Firepower (рис. 1) оптимизирован под высокую производитель-

РИС. 1. ▲ МСЭ Firepower

ность, отличается лучшей в своем классе пропускной способностью (до 80 Гбит/с) и компактностью: высота корпуса — всего одно стоечное место, а плотность вычислительных ресурсов выше, чем у любого обычного МСЭ. Одно из существенных требований к настоящим угрозоориентированным МСЭ — высокая производительность. У Firepower она достаточна для работы на периметре сети и в других высоконагруженных средах.

Ландшафт угроз очень динамичен, поэтому МСЭ нового поколения должны работать так, чтобы организации в режиме реального времени могли угрозы распознавать, ранжировать, отражать, а также автоматизировать реагирование на них. Отличительные особенности МСЭ Firepower:

- ориентация на угрозы;
- мониторинг сети;
- лучшая в отрасли аналитика угроз;
- высокоэффективная нейтрализация известных и неизвестных угроз.

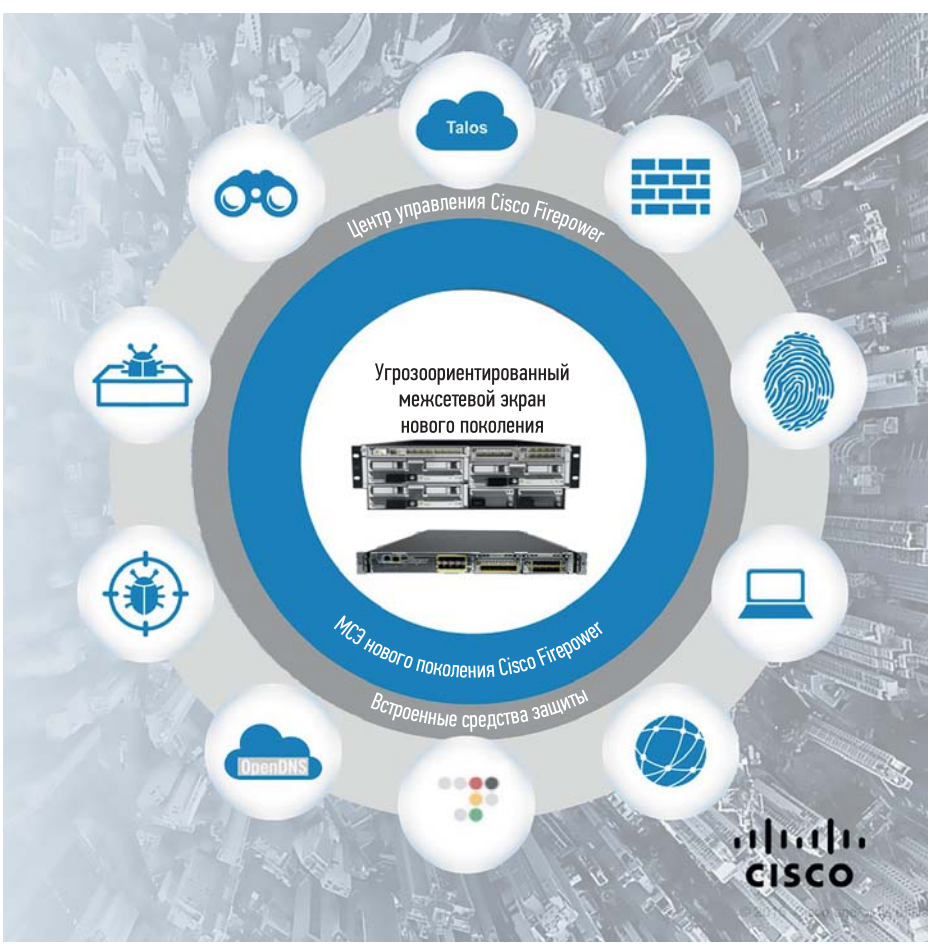
Благодаря Advanced Malware Protection, МСЭ Firepower имеет функцию ретроспективной защиты. Она позволяет как бы отмотать время назад, чтобы быстро обнаружить и устранить последствия изощренных атак, которые могли обойти защиту. В результате время, затрачиваемое на обнаружение инцидента, у заказчиков Cisco существенно меньше, чем в среднем по отрасли.

Cisco создала МСЭ нового поколения Firepower на базе лучшей в отрасли защитной платформы, которая принадлежит ей с момента приобретения два года назад компании Sourcefire. Разработчики корпорации органично совместили эту платформу с лучшими функциями наиболее проверенного МСЭ ASA, чтобы получить устройство с единым интерфейсом и единой консолью управления (рис. 2). Firepower представляет собой лучший в своем классе МСЭ с функцией контроля состояния соединений и следующими сервисами для обнаружения угроз:

- система нового поколения для предотвращения вторжений;
- система Advanced Malware Protection (AMP);
- фильтрация URL-адресов на основе репутации;
- решения компании Radware для защиты от DDoS-атак.

Среди преимуществ Firepower отметим также возможность единого мониторинга сети и настройки политик в Центре управления Cisco Firepower. Это обеспечивает ориентацию на угрозы и автоматизацию, чего нет у обычных МСЭ нового поколения, в которых защита от угроз повышенной сложности — лишь опция.

РИС. 2. ▼ Структура МСЭ Cisco Firepower



Кроме того, в платформу органично встроены решения AMP for Endpoint [2], AMP Threat Grid [3] и Cisco Identity Services Engine [4]. Они позволяют повысить эффективность и улучшить мониторинг всей сети и на оконечных устройствах. AMP for Endpoint — лучшая в отрасли технология защиты оконечных устройств от современного вредоносного кода, позволяющая отправлять результаты своего мониторинга прямо на МСЭ Firepower. Решение Cisco Identity Services Engine (Cisco ISE) также передает информацию о контексте непосредственно на МСЭ, который, в свою очередь, может дать указания Cisco ISE автоматически предпринимать действия в сети от своего имени.

Говоря о кибербезопасности, не стоит забывать и о том, что за созданием действительно качественного продукта стоят кропотливые исследования инцидентов. Значительный вклад в разработку средств защиты МСЭ Firepower и других решений Cisco для информационной безопасности вносит подразделение Cisco Talos — ведущая в мире организация, занимающаяся исследованием и анализом угроз. Именно благодаря достижениям Talos эффективность средств Cisco для обеспечения ИБ получает

«Злоумышленники объединяются и становятся все сильнее, — говорит Дэвид Гекелер (David Goeckeler), старший вице-президент и генеральный менеджер Security Business Group компании Cisco. — Кибератаки приобретают угрожающий размах. Это заставляет предприятия защищаться от растущего числа преступников, крадущих информацию ради прибыли. За последние три года Cisco потратила миллиарды долларов на собственные разработки и приобретение стратегически важных компаний в сфере ИБ. Это позволяет Cisco противостоять наиболее вредоносным атакам. Чтобы применяемые предприятиями цифровые модели эффективно справлялись со своими задачами и управляли рисками, платформа обеспечения безопасности должна быть интегрирована в бизнес. При этом она должна учитывать перспективы развития, т. е. использовать угрозоцентричный подход и обеспечивать повсеместную защиту — от мобильного устройства до облака».

наивысшую оценку по результатам независимого тестирования. МСЭ нового поколения, система нового поколения для предотвращения вторжений и система AMP успешно прошли испытания лаборатории NSS, которые подтвердили, что решение Cisco отражает большее количество угроз, чем любая другая подобная защитная платформа [5].

Вместе с анонсом МСЭ нового поколения Cisco Firepower компания ввела в действие новую консалтинговую службу — Security Segmentation Service, которая призвана помочь организациям выработать стратегии для приоритетных сегментов инфраструктуры. Индивидуальный подход компании выходит за рамки сети и объединяет проверенные практикой модели проектов. Это позволяет улучшить совместимость, локализовать источник атаки, защититься от угроз и утечек данных и внедрить прочие разнообразные меры по ИБ. Segmentation Service разрабатывает для каждого клиента индивидуальную программу, которая позволяет сокращать риски, упрощать аудит, защищать данные и соблюдать самые строгие требования.

Оба новшества Cisco направлены на защиту от опасных и устойчивых угроз кибератак. ⬣

ЛИТЕРАТУРА

1. www.cisco.com/web/RU/news/releases/txt/2016/02/24a.html
2. www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html
3. www.cisco.com/c/en/us/solutions/enterprise-networks/amp-threat-grid/index.html
4. www.cisco.com/c/en/us/products/security/identity-services-engine/index.html
5. www.cisco.com/web/RU/news/releases/txt/2015/08/19b.html