CISCO FIREPOWER 2100 — МЕЖСЕТЕВОЙ ЭКРАН СЛЕДУЮЩЕГО ПОКОЛЕНИЯ ДЛЯ ИНТЕРНЕТ-ГРАНИЦЫ

МИХАИЛ КАДЕР

Межсетевой экран Cisco Firepower 2100 Series Next-Generation Firewall (NGFW) разработан для предприятий, имеющих дело с большим количеством конфиденциальных транзакций, таких как банки и розничные сети. С его помощью можно обеспечить безотказную работу и защиту критически важных бизнес-функций и данных.

В марте этого года компания Cisco представила новые средства управления информационной безопасностью, упрощающие работу с устройствами, сетью и облаком: Cisco Firepower Device Manager (для управления устройствами), Cisco Firepower Management Center (для централизованного управления информационной безопасностью) и Cisco Defense Orchestrator (для облачного управления).

В связи с переходом к цифровым бизнес-моделям решения кибербезопасности должны поддерживать масштабирование для добавления новых функций и противостояния новым угрозам и уязвимостям без ухудшения производительности сети и приложений. В реальности это, к сожалению, не так. Включение функции обнаружения вторжений на межсетевом экране может привести к снижению пропускной способности как минимум в два раза. Из-за этого существенно страдают такие веб-приложения для взаимодействия с заказчиками, как интернет-банк и электронная коммерция, которым необходима максимальная производительность и которые чаще других становятся мишенью для злоумышленников. Ради повышения производительности некоторые предприятия отключают функционал обеспечения информационной безопасности, подвергая риску как себя, так и своих заказчиков.

НАДЕЖНАЯ ЗАЩИТА И ПРОИЗВОДИТЕЛЬНОСТЬ

В межсетевых экранах от Cisco 2100 серии впервые в отрасли реализована архитектура с двумя многоядерными ЦПУ, которая позволяет повысить скорость ключевых функций — шифрования, экранирования и защиты. Модели этой серии разработаны для удовлетворения потребностей заказчиков в постоянном поддерживании надлежащего уровня безопасности и вместе с тем — производительности, даже при задействованном функционале анализа угроз.

РИС. 1. Cisco Firepower 2110 и 2120

РИС. 2. Cisco Firepower 2130 и 2140

В новую линейку Cisco Firepower 2100 Series NGFW входят четыре платформы, ориентированные на отражение угроз (2110, 2120, 2130 и 2140), которые обеспечивают пропускную способность от 1,9 до 8,5 Гбит/с и могут использоваться в различных корпоративных конфигурациях — от границы до облака. Все платформы выполнены в компактном форм-факторе 1RU и характеризуются удвоенной плотностью портов с поддержкой 10 GbE и высокой надежностью, необходимой для поддержания непрерывной работоспособности сети. В моделях 2110 и 2120 (рис. 1) 16 фиксированных портов 1 GbE, а модели 2130 и 2140 (рис. 2) отличаются модульностью: могут иметь до 24 портов 1 GbE и 12 портов 10 GbE. Архитектура всех моделей, основанная на двух многоядерных ЦПУ, позволяет поддерживать стабильную пропускную способность при включении функций защиты, добавлять новые функции и методы защиты, а Fast Path ускоряет передачу потоков, не требующих анализа, тем самым еще больше повышая производительность. Также есть возможность интеграции Cisco Firepower NGIPS и Cisco AMP.

ПРОСТОЕ И ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ

Самые внушительные взломы компьютерных сетей показали, что ахиллесовой пятой защиты от киберугроз становится управление. Как отмечается в ежегодном отчете Cisco по кибербезопасности Cisco 2017

Annual Cybersecurity Report, основные проблемы для подразделений обеспечения информационной безопасности связаны с неправильным конфигурированием и пропуском аварийных сообщений. Для борьбы с этими затруднениями Cisco разработала усовершенствованные средства локального, централизованного и облачного управления, которые помогают заказчикам более рационально выстраивать операционные процессы и экономить средства, одновременно удовлетворяя индивидуальные потребности корпоративных пользователей:

- **Firepower Device Manager**. Веб-интерфейс управления (on-box) с помощью мастеров настройки позволяет разворачивать устройства Cisco Firepower NGFW за несколько минут, управлять стандартными политиками и задачами защиты.
- **Firepower Management Center (FMC)**. Дает возможность простого и полнофункционального администрирования большого количества устройств. В новых моделях масштабируемость управления увеличилась на 50% по сравнению с предыдущими. Для дальнейшего улучшения защиты FMC позволяет автоматизировать задачи обеспечения информационной безопасности, включая оценку, тонкую настройку, корреляцию, локализацию (containment) и ликвидацию последствий. При использовании вместе со стандартизованными FMC технологии Cisco Threat Intelligence Director (TID) можно автоматически загружать и коррелировать результаты анализа угроз, поступающие от заказчиков и третьих фирм, обеспечивая дополнительную защиту на уровне датчиков безопасности в сети (рис. 3).
- **Cloud Defense Orchestrator (CDO).** Простой облачный инструментарий позволяет рационализировать и масштабировать управление политиками безопасности, унифицируя разработку и внедрение политик по всей организации.

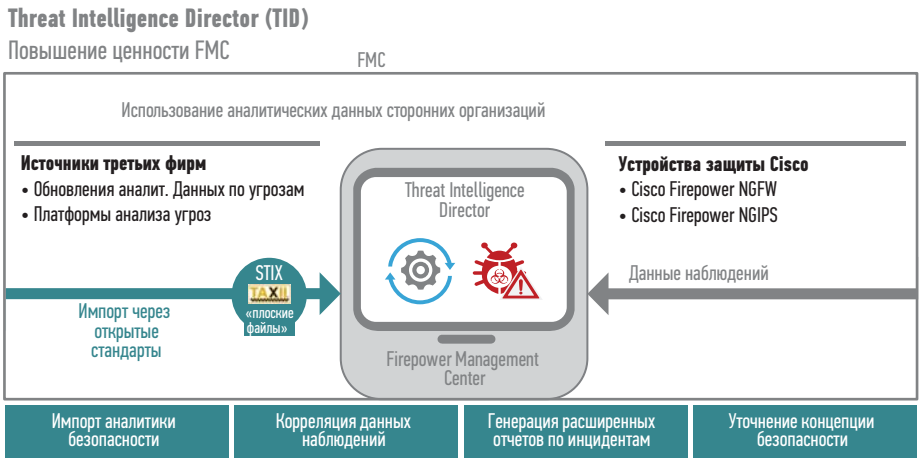

РИС. 3. ▲ Схема работы Threat Intelligence Director