Новая функциональность межсетевого экрана ASA 5500-X Next-Generation Mid-Range Security Appliances

Продолжая развивать свою широко известную стратегию информационной безопасности Cisco SecureX, компания Cisco оснастила самый популярный в мире межсетевой экран Cisco Adaptive Security Appliance новой функциональностью Cisco® ASA CX (решение для информационной безопасности, учитывающее контекст). Это решение выводит платформу Cisco ASA далеко за пределы возможностей, доступных для современных межсетевых экранов "нового поколения", позволяя гораздо лучше распознавать угрозы и очень гибко настраивать правила доступа для различных приложений. Cisco ASA CX дает возможность сетевым администраторам определять, какие именно устройства и пользователи имеют право получить тот или иной тип доступа к сетевым ресурсам, а также к тысяче с лишним приложений и 75 тысячам микроприложений.

Кроме того, Cisco обновила средние модели своих межсетевых экранов, сделав их в 4 раза более производительными и в корне поменяв их архитектуру, которая теперь может быть расширена новой функциональностью без особых усилий и без необходимости установки аппаратных модулей. Если прибавить к этому решение Cisco TrustSec® и платформу управления политиками Cisco Identity Services Engine (ISE), то вполне уместно сказать, что компания Cisco в очередной раз подняла отраслевую планку информационной безопасности на качественно новый уровень.

Потребности современного бизнеса изменили облик сетевой безопасности. Предприятиям приходится поддерживать все больше типов пользователей: обычных сотрудников, субподрядчиков, а иногда и партнеров из числа конкурентов, — предоставляя им все более широкий доступ к приложениям, устройствам и другим ресурсам. В этих обстоятельствах предприятие должно гарантировать, что доступ к приложениям, данным и сервисной функциональности будут получать только пользователи с соответствующими полномочиями, для остальных же эти ресурсы должны быть закрыты. Таким образом, традиционные модели информационной безопасности устарели, и ИТ-отделам приходится искать золотую середину между производительностью и безопасностью.

Предложения Cisco в области информационной безопасности устраняют противоречие между безопасностью и производительностью, позволяя совершенствовать и то, и другое. В результате компании получают возможность повысить мобильность своих сотрудников и снизить риски, свойственные "предприятиям без границ". Cisco предлагает рынку уникальное мощное сочетание средств управления, позволяющих учитывать малейшие детали контекста, идентификации, политик и интеллектуальных функций. Это решение поможет предприятиям ускорить развитие бизнеса и поддержать нужный уровень информационной безопасности для всех устройств во всех сегментах корпоративной сети.

Cisco ASA CX — решение нового поколения для информационной безопасности с учетом контекста

Это решение расширяет платформу ASA, еще выше поднимая отраслевую планку прозрачности и глубины детализации систем управления. Cisco ASA CX распознает более тысячи приложений, таких как Facebook, Google+, LinkedIn, Twitter и iTunes, и подразделяет их на 75 тысяч с лишним микроприложений. Затем все микроприложения сводятся в простые для понимания категории, что позволяет администраторам межсетевых экранов легко разрешать или запрещать доступ к тем или иным частям "большого" приложения (к примеру, микроприложения Facebook распределяются по категориям "бизнес", "сообщество", "образование", "развлечения", "игры" и т.д.). В результате ИТ-отделы получают возможность предоставлять пользователям доступ к большему количеству приложений, сводя к минимуму число абсолютных запретов.

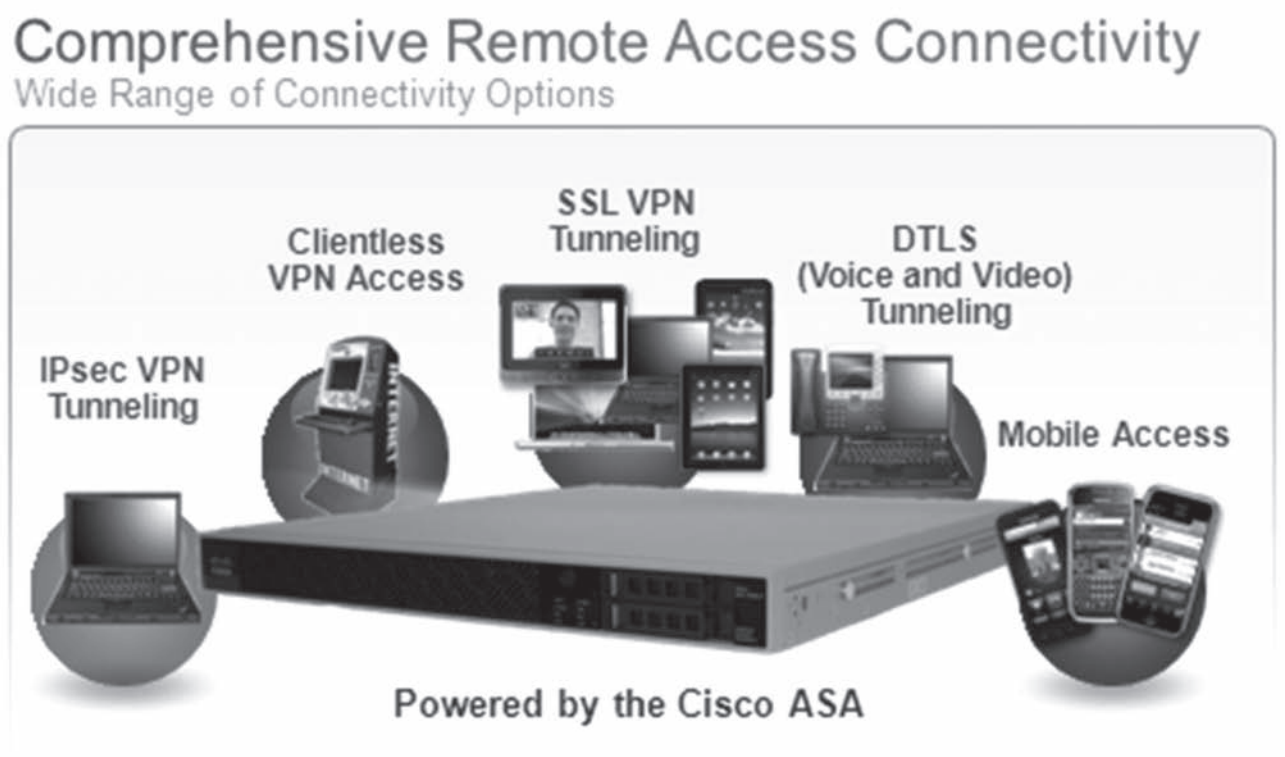
Cisco ASA CX использует широкие возможности сетевой архитектуры безопасности Cisco SecureX Framework, учитывающей контекст и работающей в унифицированных сетях доступа, граничных сетях, сетях корпоративных подразделений и центров обработки данных, а также в облачных сетевых сегментах. Эта архитектура полностью поддерживается продуктами и услугами Cisco для информационной безопасности.

Cisco ASA CX отличается от всех других межсетевых экранов. Только это решение использует систему SecureX для получения полного доступа к интеллектуальным сетевым функциям и агрегации данных, поступающих из локальной сети, с помощью системы Cisco AnyConnect Secure Mobility, а также для получения информации о хакерских угрозах в режиме, близком к реальному времени, из глобального центра Cisco Security Intelligence Operation (Cisco SIO), непрерывно предоставляющего заказчикам Cisco самый высокий уровень защиты.

Это решение дает сетевым администраторам возможность устанавливать устройства и приложения с высоким уровнем защиты и управляемости. Администраторы получают четкие данные о типе устройства, установленной на нем операционной системе, местоположении устройства и текущем уровне безопасности.

Решения Cisco TrustSec и Cisco ISE

Решения Cisco TrustSec 2.1 и ISE 1.1 дают пользователю полное представление о сети с помощью новых датчиков, интегрированных в сетевую инфраструктуру для автоматического распознавания и классификации всех подключенных к сети устройств. Кроме того, решение ISE 1.1 предоставляет в реальном времени результаты целенаправленного сканирования оконечных устройств в соответствии с принятыми политиками, что позволяет еще лучше и точнее классифицировать сетевые устройства. Вместе взятые эти решения выдают самое точное и полное представление обо всей корпоративной инфраструктуре, независимо от ее размеров. Помимо этого, TrustSec 2.1 расширяет поддержку новаторской технологии Cisco Security Group Access (SGA), предоставляющей пользователю возможность детального управления политиками в проводных и беспроводных сетевых инфраструктурах.



Средние модели устройств безопасности Cisco ASA 5500-X

В состав семейства новых высокопроизводительных устройств нового поколения для информационной безопасности Cisco ASA входят модели ASA 5512-X, 5515-X, 5525-X, 5545-X и 5555-X, оптимизированные для установки в граничных сегментах сетей, предоставляющих доступ в Интернет как малым, так и большим предприятиям. Учитывая контекст с помощью архитектуры Cisco SecureX Framework, эти устройства поддерживают множество услуг информационной безопасности без установки дополнительных аппаратных модулей, работают на мультигигабитных скоростях, предоставляют широкий выбор интерфейсов и обладают резервными блоками питания — и все это заключено в компактный корпус 1RU. В качестве опции предлагается более широкая и глубокая защита сети с помощью интегрированных облачных и виртуализированных программных сервисов информационной безопасности, поддерживаемых центром анализа сетевых угроз Cisco SIO.

Сертификация в области информационной безопасности

Cisco обновила программы сертификации в сфере информационной безопасности — Cisco CCNA® Security, Cisco CCNP® Security и Cisco Security Specialist. Теперь эти программы включают изучение систем ASA и предоставляют обучаемым знания и практические навыки, учитывающие передовой опыт лучших специалистов по сетевой безопасности, инженеров и экспертов, использующих новейшее оборудование, устройства и решения Cisco.

Вместо того, чтобы сосредотачиваться исключительно на межсетевом экране, компания Cisco учитывает широкий контекст, в котором межсетевой экран выступает как живая, активная и динамичная часть отлично защищенной сети, — говорит Кристофер Янг (Christopher Young), старший вице-президент компании Cisco возглавляющий подразделение информационной безопасности и взаимодействия с государственными органами. — Cisco встраивает функции информационной безопасности в саму сеть, используя ее уникальные возможности в области учета контекста, интеллектуальных сервисов и управления. Никакая другая часть вашей инфраструктуры не имеет таких широких знаний о происходящем, как сеть. Мы приступаем к активному использованию этих знаний и начинаем с межсетевого экрана.

Cisco ISE предоставляет нашей компании лучшее в своем классе решение для информационной безопасности с удивительно тонкой настройкой, дающей нам полное представление о пользователях без установки дополнительного оборудования, — отметил Дэвид Кеннеди (David Kennedy), вице-президент компании Diebold, Inc. и главный директор по безопасности. — Cisco — давний доверенный поставщик компании Diebold, где безопасность считается неотъемлемой частью корпоративной культуры. Мы правильно сделали, поручив Cisco решение своих задач в области глобальной сетевой безопасности. Решение Cisco ISE позволило нам упростить управление корпоративной безопасностью и помогло надежно идентифицировать и защитить каждого пользователя и каждое устройство, подключаемое к нашей сети.

Решения Cisco AnyConnect, ASA, ASA CX и IronPort позволили нам реализовать давнюю мечту — создать систему информационной безопасности, в которой все компоненты взаимодействуют друг с другом и работают как единое целое, — заявил Ник Янг (Nick Young), менеджер по поддержке сетей из компании Four Seasons Healthcare (FSHC). — Использование продуктов Cisco для информационной безопасности помогло нам упростить управление, повысить прозрачность

Продолжение читайте на 46 стр.

Начало читайте на 45 стр.

и лучше реагировать на требования бизнеса. Мы перестали думать о том, что можно или нельзя разрешать, и сосредоточились исключительно на пресечении несанкционированных действий. С нетерпением ждем новых решений, способных управлять всеми перечисленными устройствами через единую глобальную консоль.

Решение Cisco ASA 5500-X отлично подходит для межсетевого экранирования с высокой производительностью и поддержкой множества услуг информационной безопасности, одновременно работающих на межсетевом экране, — утверждает президент корпорации Little eArth Corporation Co., Ltd. (LAC) Осаму Саито (Osamu Saito). — Устройства Cisco ASA превосходят наши требования к межсетевым экранам и системам предотвращения вторжений (IPS), работающим на одном устройстве. Мы с удовольствием используем устройства ASA в своем японском центре информационной безопасности и с их помощью предоставляем самый высокий уровень защищенности организациям, работающим на территории Японии.

Медицинский центр Sentara стремится предоставлять своим пациентам услуги самого высокого качества, — говорит Чад Спирс (Chad Spiers), директор компании Sentara Healthcare, отвечающий за инфраструктуру для передачи голоса и данных. — Cisco ISE полностью соответствует нашим высоким стандартам информационной безопасности, повышения эффективности операций и удовлетворения нормативных и законодательных требований. Использование стандарта 802.1x позволяет поддерживать динамический авторизованный пользовательский доступ, распознавать клинические данные, не допускать их смешивания с обычными пользовательскими данными и блокировать передачу медицинских данных на сотни устройств, многие из которых подчиняются требованиям FDA и регулируются поставщиками.

Cisco и Xerox развивают решение TrustSec, чтобы правильно отреагировать на взрывообразный рост количества персональных устройств, используемых на рабочем месте, — заявил Рик Дастин (Rick Dastin), президент подразделения корпорации Xerox по разработке продукции для корпоративного сектора. — Чтобы защитить конфиденциальную информацию, компаниям нужно в первую очередь защитить сетевые оконечные устройства: принтеры, планшетные компьютеры, веб-камеры и так далее, — и незамедлительно внедрить политики информационной безопасности. TrustSec дает ИТ-менеджерам возможность автоматически идентифицировать, отслеживать и контролировать все устройства из центральной точки. TrustSec обеспечивает надежную защиту входящих и исходящих каналов на этих устройствах.

Cisco Systems Holding BV,
Представительство в Республике Беларусь
220034, г.Минск, ул. Платонова, 1Б,
Бизнес-центр «Виктория Плаза»
E-mail: pburba@cisco.com
Сайт: www.cisco.com