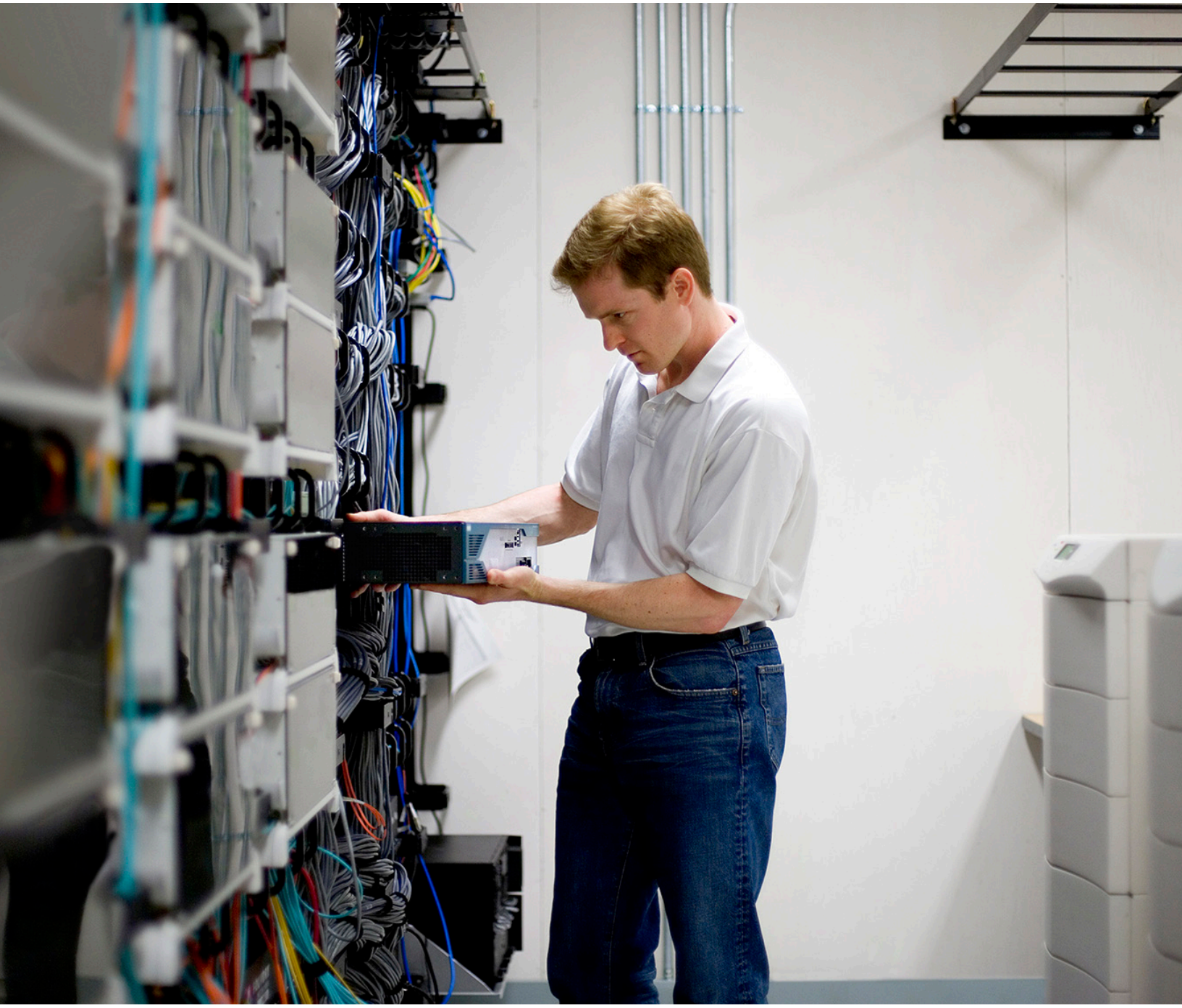
Подготовьтесь к будущему – сделайте периметр сети интеллектуальным



Краткий обзор

В новой цифровой реальности периметр корпоративной сети приобрел исключительное значение. Его часто недооценивают, однако сетевой периметр является важным фактором успеха любого цифрового предприятия. Необходимо учитывать все, что происходит по периметру сети.

- Это передний край защиты от проникновения ненадежных или вредоносных устройств и программ.
- Это канал, по которому приложения и услуги – как правило, созданные благодаря значительным инвестициям – доставляются целевым пользователям.
- Это стратегический шлюз между географически распределенными организациями.
- Это мост между вашей компанией и вашими заказчиками.
- Это точка подключения и администрирования устройств Интернета вещей (IoT).
- Это то место, где вы действительно можете понять, что происходит с вашим бизнесом.

Развертывая периметр сети, некоторые компании уверены, что все сетевые решения по сути одинаковы. Cisco придерживается другого мнения: современный цифровой бизнес требует широких интеллектуальных возможностей на сетевом периметре.

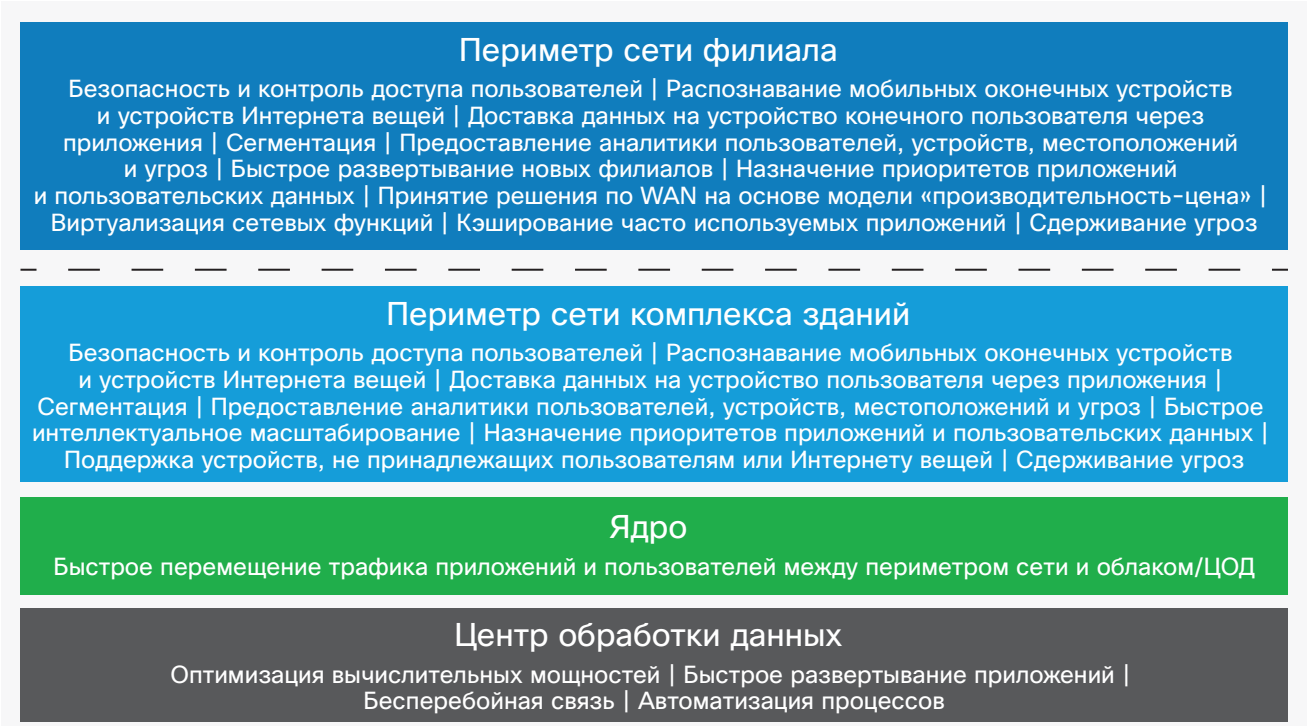
Мы предлагаем решения и стратегически важную функциональность, которые помогут вашему бизнесу успешно развиваться. Cisco реализует для периметра цифровой сети архитектуру, которая обладает следующими ключевыми возможностями.

- Защита критически важных ресурсов по всему периметру. Организации смогут предотвращать 99,2 % сетевых атак, если будут использовать сеть как сенсор и регулятор безопасности. Кроме того, они получат ценную аналитику, которая поможет им усовершенствовать защиту и в результате быстрее реагировать на нарушения.
- Отслеживание работы приложений и устройств с ускоренным в 8 раз роумингом и мониторингом более 1200 приложений. Сегодня это стало возможным благодаря стратегическому партнерству с Apple и инновациям в области беспроводного доступа.
- Быстрое масштабирование сети по мере роста вашего бизнеса за счет программно-определяемого подхода к построению беспроводных и проводных LAN, а также WAN. Благодаря отделению программного обеспечения от аппаратного уровня и виртуализации периметра WAN это сокращает затраты на развертывание на 79 %.
- Платформа для удовлетворения будущих потребностей – программируемая, основанная на стандартах – позволяет быстро добавлять новую функциональность по мере необходимости.
- Более подробная и быстрая аналитика для ритейла и гостиничного бизнеса – с детализацией данных о местоположении до одного метра.

Сегодня сеть имеет ключевое значение для поддержки важных преобразований в любой организации, которая ступила на путь цифровизации. Такие преобразования помогут организациям повысить гибкость и производительность, эффективнее взаимодействовать с клиентами и защищать свою интеллектуальную собственность и ресурсы.

Периметр сети становится центральным компонентом в таких преобразованиях, отвечая за самый широкий набор задач по сравнению с сетями ядра и ЦОД. Если сравнить разные уровни сети, как показано на рис. 1, сетевой периметр выполняет широкий круг задач в сети кампуса. То же можно сказать и о сетях филиалов.

Рис. 1. Сетевые уровни и их функции



Значение периметра сети

Цифровизация делает сетевой периметр ключевым участком сети. Необходимо учитывать все, что происходит по периметру.

- **Это передний край защиты.** Периметр – это то место, где применяются и утверждаются политики безопасности с учетом доступа к необходимым вам ресурсам. Без должного контроля доступа ваш бизнес подвергается риску незаконного проникновения и распространения угроз, и этот риск возрастает по мере расширения ландшафта угроз. Точкой вторжения может стать устройство, микропрограммное обеспечение и даже операционная система.
- **Это канал доставки конечным пользователям важных приложений, в которые вложены значительные средства.** На периметре сети определяются приоритеты. Недостаточное обслуживание по периметру сети препятствует внедрению и освоению новых приложений, что, в свою очередь, снижает окупаемость инвестиций.
- **Это стратегически важный шлюз, который служит связующим звеном между географически распределенными организациями.** Важно предоставить удобный и высокоскоростной доступ к сети всем сотрудникам, партнерам и клиентам независимо от их местонахождения. Недостаточно развитая сеть не способна обеспечить стабильный и единообразный доступ к услугам для конечных пользователей.
- **Это мост между организацией и ее клиентами.** Если вы работаете в розничной торговле или гостиничном бизнесе, неудовлетворительный доступ затруднит персональное взаимодействие с клиентами и негативно отразится на репутации вашего бренда.
- **Периметр сети должен обеспечить поддержку растущих потребностей в устройствах IoT.** Практически во всех отраслях периметр сети преобразует физическую среду, позволяя перейти на цифровые бизнес-модели, усовершенствовать процессы и сократить расходы. Без необходимой функциональности по периметру сети организации будут отставать по таким показателям, как эксплуатационная эффективность и сокращение расходов.
- **Это то место, где вы действительно можете понять, что происходит с вашим бизнесом.** В распределенной сети только периметр позволяет увидеть весь сетевой трафик, предоставляя исчерпывающие данные и важную аналитику. На основе данных о пользователях, приложениях, устройствах и угрозах формируется ценная аналитика, которая помогает организациям принимать взвешенные решения

для поддержки своих сотрудников, снижения рисков и затрат и предоставления необходимой информации целевым пользователям. Без нужного уровня детализации эти данные нельзя считать надежными, так как они не позволяют сформировать точную картину.

«Коммодитизация» периметра – это хорошо?

Многие решения для сетевого периметра реализованы на основе готовых компонентов для проектирования и создания сетевых устройств в соответствии со всеми отраслевыми стандартами. Часто это делается ради снижения затрат на разработку и производство оборудования – по готовым проектам от производителей комплектующих. Это ведет к «коммодитизации» периметра. Такой подход, когда на первом месте стоят затраты и управление, а не инновации для роста и безопасности, подвергает вашу организацию значительным рискам.

Каковы эти риски?

Все компоненты и архитектуры доступны не только производителям устройств. Они также могут попасть в руки тех, кто планирует незаконно проникнуть в сеть. Каждое устройство, подключенное к сети, может стать окном для проникновения в сеть. Сегодня организации все чаще полагаются в своей работе и бизнес-процессах на мобильные устройства и устройства Интернета вещей, предоставляя им доступ к своей сети. Им следует изучить решения, обеспечивающие безопасный сетевой доступ с проверкой и перепроверкой трафика на каждом участке сети: от периметра до ЦОД.

Еще один риск состоит в том, что в результате новых требований бизнеса придется перепроектировать сеть. Готовые решения разработаны для большого количества текущих сценариев использования, но имеют ограничения с точки зрения гибкости и настройки с учетом конкретных требований. Они также не готовы к непредвиденному развитию вашей сети. Сетевая платформа должна адаптироваться к стремительным изменениям современного цифрового мира.

Большинство «готовых» решений разработаны в точном соответствии с отраслевыми стандартами, что важно для удовлетворения базового набора требований. Однако стандарты могут меняться. Процесс стандартизации может сильно растянуться, а потребности производителей устройств, разработчиков приложений и пользователей постоянно меняются. Если оставаться в рамках привычных стандартов, можно отстать и утратить возможность соответствовать растущим ожиданиям пользователей. В некоторых случаях решение может начинаться с соответствия стандартам, но предусматривает возможность добавления функциональности по мере необходимости. Такие решения соответствуют требованиям динамичного цифрового мира и не ограничены стандартами, на усовершенствование и утверждение которых могут уходить годы.

Существует также риск нарушения целостности устройства. Мошенники могут перехватывать устройства во время транспортировки в разные страны мира и изменять компоненты (например, заменять процессоры или вставлять «жучки» для получения конфиденциальных данных).

Какова реальная стоимость

Целью «коммодитизации» периметра часто становится снижение стоимости разработки и производства и как следствие возможность продажи продуктов по более низкой цене. Однако при оценке стоимости необходимо учитывать не только чистые капитальные и даже операционные расходы, но и расходы, связанные с риском. Все организации разные, и невозможно определить фактическую стоимость, единую для всех. Однако можно принять во внимание следующее.

- Цена нарушения безопасности. Для многих организаций их интеллектуальная собственность и ресурсы имеют критически важное значение. Каковы будут последствия, если что-то из этого попадет в чужие руки? Мошеннические организации блестяще извлекают прибыль из чужой интеллектуальной собственности путем вымогательства, требований выкупа и перепродажи тем, кто предлагает за нее более высокую цену. Согласно некоторым исследованиям, сумма выкупа за медицинские карты достигала 40 долл. США за штуку. Больницы с тысячами медицинских карт рискуют стать жертвами вымогательства огромных денег за возврат своей собственности.
- Цена отказа от использования сотрудниками новых важных бизнес-приложений и сервисов. Многие организации вкладывают значительную часть своего бюджета в новые приложения и системы для повышения производительности работы персонала. Если сотрудникам неудобно работать с этими приложениями или сервисами, они начнут избегать их, и окупаемость таких инвестиций резко упадет.
- Цена утраченных возможностей. Если вы работаете в розничной торговле или гостиничном бизнесе, то наверняка взаимодействуете с существующими и потенциальными клиентами через их мобильные устройства. Но если людям сложно подключиться к вашему сервису, ваша организация теряет возможность привлечь такого клиента и повлиять на его решения.

- Цена отсутствия прозрачности. На периметре сети сосредоточено огромное количество данных о пользователях, их устройствах, используемых приложениях, маршрутах передвижения и даже о потенциальных угрозах. Без такого уровня прозрачности ваша организация может тратить бесчисленные часы, пытаясь понять, как пользователи взаимодействуют со средой, обращаются к информации и используют ее. Можно даже пропустить угрозу, которая могла бы быть выявлена на раннем этапе.

Cisco предоставляет функции аналитики на сетевом периметре

Cisco применяет другой подход, отличный от «коммодитизации». Мы вкладываем значительные средства в разработку инноваций, которые помогут организациям перейти на цифровые технологии. Мы уделяем особое внимание защите важных ресурсов, чтобы система могла взаимодействовать с большим числом приложений и устройств и обеспечивала более глубокий и быстрый анализ данных. Cisco помогает вам адаптироваться по мере развития бизнеса и подготовиться к любым будущим изменениям. Для этого мы создаем уникальную функциональность с нуля или улучшаем функциональность, уже проверенную на практике. Благодаря решениям Cisco вы сможете соответствовать всем требованиям периметра сети как сейчас, так и в будущем.

Защита важных ресурсов по периметру сети

Периметр сети – это зона риска номер один, так как именно здесь предоставляется сетевой доступ новым пользователям и устройствам. Чтобы понимать, что происходит в сети, и держать ее под контролем, необходимо иметь надежный периметр.

Согласиться с тем, что «коммодитизация» решений безопасности периметра сети будет эффективной, значит признать, что готовая, стандартная система безопасности работает. Но если это так, то почему такие явления, как кража информации, вымогательство и выкупы быстро стали настоящей индустрией, которая сегодня оценивается в 1 триллион долл. США?

Существующие подходы к информационной безопасности периметра не работают. Компания Cisco – лидер рынка. С помощью ее инновационных технологий вы всегда сможете понять, что или кто перед вами, а также оценить надежность «кандидата», прежде чем пускать его в сеть и предоставлять право роуминга.

Приведем ряд инновационных решений Cisco® в области защиты периметра сети и несколько примеров их использования заказчиками.

- **Идентификация и определение надежности устройств и пользователей**. Оборудование сетевого периметра Cisco включает наибольшее число технологий для проверки профилей оконечных устройств. Кроме того, Cisco AnyConnect® Security Agent выполняет проверку на надежность и соответствие политике, прежде чем предоставить доступ в производственную сеть. Такая точная идентификация оконечных устройств полностью защитит сеть от несанкционированных и «нездоровых» (зараженных вредоносным ПО) устройств. Доступ в сеть будет предоставляться только после полной проверки и авторизации.
- **Изменение прав доступа с учетом оценки угроз**. Благодаря интеграции с платформой Cisco Identity Services Engine права доступа для пользователей и устройств могут автоматически меняться с учетом изменения оценки угроз STIX или оценки уязвимостей CVSS. STIX и CVSS – это широко используемые выражения для обозначения степени серьезности угроз безопасности и уязвимостей.
- **Интеграция программно-определяемой сегментации**. Сегментация и управление ею с виртуальными LAN и списками контроля доступа (ACL) обычно затруднены и еще более осложняются, когда сегментация становится основным условием защиты операций Интернета вещей. Оборудование сетевого периметра Cisco поставляется с программно-определяемой сегментацией Cisco TrustSec®, встроенной в операционную систему, и специализированной интегральной схемой ASIC. Это обеспечивает простую и высокопроизводительную идентификацию и сегментацию от точки входа до ЦОД.
- **Сеть как регулятор**. Это программно-определяемая сегментация в оборудовании сетевого периметра, которая позволяет мгновенно и последовательно применять политику безопасности для контроля доступа и изоляции угроз. Благодаря интеграции с Identity Services Engine, Cisco Stealthwatch и Cisco Security Technology Associate можно вызвать политику для изоляции угрозы – и все это из одного окна, или одного продукта.
- **Сеть как сенсор**. Пользуйтесь функциями сквозного мониторинга NetFlow и интерпретации данных Cisco StealthWatch. Поскольку все устройства сетевого периметра Cisco включают технологию Flexible NetFlow, в вашем распоряжении функции сквозного мониторинга для выявления любого аномального поведения.

В отличие от стандартизированных решений, которые не позволяют видеть поведение пользователей при подключении к сети или во время просмотра веб-страниц.

- **Интеграция самообучающейся сети Stealthwatch**. Эта инновация позволит всем устройствам филиальных сетей обмениваться данными о поведении пользователей и устройств и приобретать «знания» о том, что разрешено в сети. Это ускоряет реагирование, упрощает операции и повышает общую масштабируемость.
- **Мгновенное применение политики готовности к защите defcon (DEFense readiness CONdition)**. Это означает, что вы сможете предварительно задавать политики реагирования на такие катастрофические события, как вредоносное ПО «нулевого дня» или быстро распространяющаяся хакерская атака. Одним нажатием кнопки можно изменить политику доступа для каждого устройства в сети и таким образом ограничить или прекратить всю связь, пока угроза не будет устранена.
- **Идентификация оконечных устройств Интернета вещей и автоматическая сегментация**. Датчики в устройствах сетевого периметра Cisco помогают идентифицировать самый большой набор медицинских устройств IoT, и эта технология начинает применяться во множестве других отраслей. Благодаря интеграции с такими передовыми технологиями, как Identity Services Engine, устройства сетевого периметра смогут лучше распознавать и автоматически сегментировать малоизвестные оконечные устройства и автоматически добавлять их в определенные сегменты сети для защиты от атак. Таким образом, когда работник подключает устройство к сети, это устройство идентифицируется, классифицируется и помещается в соответствующий сегмент сети безопасности.
- **Быстрое сдерживание и нейтрализация угроз**. Устройства сетевого периметра Cisco интегрированы с Identity Services Engine и TrustSec, и, если Cisco или партнер по интеграции технологий обнаруживают атаку, они могут поместить оконечное устройство, представляющее угрозу, в сегмент сети с помощью службы ИТ или автоматически. Угрозы выявляются быстрее, а их нейтрализация происходит практически мгновенно.
- **Обнаружение вредоносного ПО в зашифрованном трафике**. В то время как хакеры находят все более незаметные способы проникновения в сеть, Cisco использует все возможности для исследования сетевых фреймов и выявления вредоносного кода – даже в зашифрованном трафике.
- **Безопасность облака и защита от вредоносного ПО и программ-вымогателей**. Интеграция с сервисом Cisco Umbrella для сетей филиалов делает устройства сетевого периметра Cisco важной частью решения Cisco для защиты от программ-вымогателей. Этот «зонт» не дает сотрудникам заходить на подозрительные, скомпрометированные или вредоносные сайты. Он также блокирует ботам вредоносного ПО и программ-вымогателей доступ к их родительскому объекту, препятствуя вредоносной активности.
- **Защита мобильности сотрудников**. Мобильные работники и их устройства чаще всего становятся точками проникновения вредоносного ПО в корпоративные сети, поскольку они свободно пользуются Интернет-доступом вне офиса. Агент безопасности Cisco AnyConnect с VPN может быть дополнен решениями Cisco Advanced Malware Protection и Cisco Umbrella for Mobility для защиты за пределами сети. Он также позволяет подключаться ко многим устройствам сетевого периметра Cisco через VPN. В стандартизированной среде никакие подобные средства мобильной защиты с одним агентом не работают.
- **Целостность сетевого устройства**. Для проникновения в системы и их взлома у хакеров гораздо больше путей и возможностей, чем просто уязвимрсти в приложениях и операционных системах. Они атакуют весь программный и аппаратный стек сетевых устройств, поэтому безопасность сетевого устройства имеет решающее значение для системы безопасности. Как уже показал опыт с операционными системами и приложениями, новые уязвимости сетевых устройств скорее всего будут обнаруживаться и дальше. Компания Cisco разрабатывает программное и аппаратное обеспечение с регрессионным тестированием по самым строгим правилам, чтобы ее заказчики работали в безопасной и надежной сети.

Ускоренный и более глубокий анализ данных

На сетевом периметре Cisco сосредоточен весь комплекс знаний о том, что действительно происходит в вашем бизнесе, включая обширные данные о ваших пользователях и о том, какие устройства и приложения они используют. Периметр может понимать эти устройства и получать от них ценные знания, которые позволят автоматически адаптироваться к изменениям и новым потребностям. Периметр сети предоставляет данные с привязкой к местоположению. По этим данным проще понять, как пользователи взаимодействуют со средой, что

дает возможность принимать более обоснованные бизнес-решения. А по данным, полученным при расследовании угроз, можно понять, как эти угрозы проникают в бизнес.

С помощью платформы Cisco IOx Fog Computing периметр может выбирать оптимальное место обработки данных (в локальной среде или в облаке), что поможет организации повысить производительность и снизить расходы. Средства аналитики геолокации, реализованные в Cisco Connected Mobile Experiences (CMX), обеспечивают детальную аналитику местоположения на основе данных Wi-Fi и Bluetooth Low Energy (BLE), что позволяет составить реальную картину того, как люди взаимодействуют со средой и пространством.

Организации типа B2C, такие как розничные магазины, гостиницы и учебные заведения, уже сейчас могут получать данные о местоположении с точностью менее одного метра благодаря Wi-Fi + BLE, что напрямую влияет на их выручку. Среди примеров – повышение на 20 % выручки, не связанной со сдачей номеров, в отеле Hyatt Regency, трехкратное увеличение времени пребывания посетителей и улучшение качества обслуживания на 80 % в торговом центре Stary Browar. И все это благодаря персонализированному обслуживанию через мобильные устройства.

Кроме того, Cisco Prime™ предоставляет всестороннюю информацию о ваших конечных пользователях, их устройствах и приложениях, используемых в сети. Это позволяет лучше планировать сеть, оценивать восприятие пользователями новых приложений и последовательно снижать затраты.

Адаптация по мере роста бизнеса благодаря автоматизации

Чем большим количеством пользователей, устройств и мест приходится управлять, тем больше потребность в автоматизированных процессах и услугах с возможностями обслуживания в «день 0» и «день 1». В пространстве проводной и беспроводной связи коммутационные структуры кампуса и ЦОД с отдельным программным оверлеем, работающим на специализированных интегральных схемах (ASIC), обеспечивают следующие преимущества:

- расширенные возможности масштабирования;
- гарантированное качество услуг;
- безопасность;
- другие услуги для физических и виртуальных устройств, приложений и пользователей.

Виртуализация сети обеспечивает управление сетью и политиками по типам пользователей, что позволяет быстро осуществлять запуск и настройку приложений и сдерживать угрозы. Этот централизованный подход дает возможность безопасно развертывать новые удаленные точки за минуты вместо дней независимо от типа подключения.

Контроллер Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) обеспечивает централизованное подключение по схеме «подключи и работай» (plug and play, PnP) и удобную функциональность QoS для автоматизированного развертывания на периметре. Он также обеспечивает динамическую установку приоритетов для важных приложений.

Cisco предоставляет программную гибкость для индивидуальной настройки. Благодаря тесной интеграции программной и аппаратной платформ мы можем обеспечить вашей организации значительные преимущества, которые проявят себя в WAN и на периметре сетевого доступа. Компоненты, настроенные для WAN, включают в себя быстродействующую интегральную схему ASIC, а программное обеспечение управления облаком превращает решение Cisco Enterprise Network Functions Virtualization (Enterprise NFV) в реальность, в которой сетевые сервисы развертываются за минуты, а не за месяцы. Enterprise NFV предоставляет функции вычисления, хранения, сетевой инфраструктуры, управления и обеспечения качества для сетевых сервисов, что позволяет снизить сложность в сетях филиалов и предоставлять услуги по требованию на сетевом периметре.

Организации на 79 % снизили расходы на развертывание с помощью APIC-EM PnP и на 85 % ускорили выделение ресурсов с помощью приложений APIC-EM Intelligent WAN.

Обслуживая большое количество пользователей, подключающихся с объектов всех типов, периметр сети может работать как в больших кампусах, так и на небольших удаленных объектах. Глобальные представления топологии с автоматизированными средствами PnP значительно снижают стоимость подключения или модернизации таких устройств, как коммутатор, маршрутизатор или точка доступа. Дополнительные приложения на контроллере служат повышению качества услуг во всей сети и быстро защищают важный для бизнеса трафик от некритически важных потребителей полосы пропускания. Такие специальные приложения, как Intelligent WAN (IWAN), выделяют ресурсы, выполняют мониторинг и устраняют неполадки в системе безопасности, осуществляют шифрование, выбор пути, гарантируют прозрачность приложений и контроль над WAN.

Кроме того, ПО Cisco ONE™ обеспечивает ценный и гибкий способ покупки ПО для периметра вашей сети. На каждом этапе жизненного цикла продукта программное обеспечение Cisco ONE упрощает приобретение продуктов, управление сетью и ее модернизацию. Добейтесь быстрой окупаемости растущих инвестиций с помощью постоянных инноваций, обновлений и модернизации физических и виртуальных машин.

Контроль работы приложений и устройств

Cisco – единственная в своей отрасли компания, сотрудничающая с лидером рынка мобильных устройств Apple в области качества обслуживания мобильных пользователей. Это партнерство, имеющее стратегическую важность для обеих компаний, применяет реализованную в сети аналитику для обеспечения высококачественного доступа Wi-Fi за счет оптимального роуминга. Иными словами, это быстрый способ повышения производительности труда сотрудников благодаря использованию важных бизнес-приложений на устройствах Apple iOS.

Компании могут рассчитывать на восьмикратное ускорение роуминга, повышение надежности звонков через Wi-Fi на 66 % и снижение затрат на управление сетью благодаря меньшему количеству идентификаторов SSID, а конечные пользователи смогут на 30 % продлить срок службы батареи устройства iOS.

На протяжении многих лет компания Cisco разрабатывала инновации в области Wi-Fi, которые выходят за рамки текущих стандартов и становятся надежной и проверенной основой для новых. Технология беспроводного доступа Cisco Aironet® предоставляет инновации для поддержки большого количества подключений с лучшей передачей сигнала, повышением производительности устройств и удобства работы с приложениями. Cisco также была основоположником технологии Flexible Radio Assignment, которая оптимизирует работу сети Wi-Fi, не ограничивая доступность радиочастот. Эта способность позволяет точкам беспроводного доступа выявлять неожиданные потребности в использовании диапазона частот беспроводной связи и автоматически адаптировать беспроводную сеть к новым потребностям. Это важно в пространствах, где за беспроводную полосу пропускания конкурирует большое количество пользователей.

Успех цифрового бизнеса зависит от приложений, которые используются для повышения производительности и взаимодействия с клиентами. Cisco предоставляет функции контроля и мониторинга приложений, которые обнаруживают приложения на периметре проводной и беспроводной сети. Мы используем интеллектуальное управление маршрутами для выбора оптимального маршрута WAN, оптимизируя доставку по вашей проводной или беспроводной локальной сети, чтобы обеспечить пользователям максимальное удобство использования приложений.

С помощью APIC-EM и инфраструктуры Cisco Prime организации могут видеть более 1200 приложений и задавать приоритеты для важных бизнес-приложений одним щелчком мыши.

Периметр может контролировать и оптимизировать работу сотрудников в физическом пространстве. Предоставляя защищенную и интеллектуальную сетевую платформу, цифровой потолок Cisco расширяет преимущества Интернета вещей, объединяя управление всевозможными сетями в здании, включая:

- освещение;
- теплоснабжение и охлаждение;
- IP-видео;
- датчики Интернета вещей;
- и многие другие системы.

Цифровой потолок открывает новые возможности для эффективной работы сотрудников и снижает эксплуатационные расходы объектов.

Решение на будущее

Периметр Cisco разработан для поддержки задач будущего, без операционной системы Cisco IOS-XE с ее программируемостью на основе стандартов и моделей, благодаря чему сеть готова к добавлению новой функциональности и адаптации к будущим изменениям в среде, бизнесе и отрасли. Это делает сеть периметра открытой, программируемой и расширяемой.

Периметр переходит с настраиваемой модели, где сегментация и разграничение доступа добавляются в конфигурацию сети отдельно для каждого устройства, на полностью автоматизированное решение на основе политик. В будущем не нужно будет предоставлять сетевые ресурсы напрямую. Можно будет использовать политику как выражение намерения. Кроме того, можно будет указать, какие пользователи или группы должны иметь доступ к определенным привилегированным группам приложений или наборам данных в корпоративной среде или в облаке. Сеть будет предоставляться автоматически в соответствии с этой политикой, но с сохранением возможностей для мониторинга, устранения неполадок, ремонта или применения дополнительных услуг для определенного трафика.

Периметр также становится полностью программируемым. Решения оркестрации могут взаимодействовать с периметром через стандартные интерфейсы API, основанные на моделях, скрипты Python или другие инструменты в стиле Linux. Это упрощает интеграцию периметра в современные методы разработки программного обеспечения, обеспечивая беспрецедентную гибкость и возможность настройки.

Непрерывные инновации по периметру сети

С развитием средств связи и появлением новых возможностей компании приходят к пониманию того, что такое преобразование потребует фундаментальных изменений в их инфраструктуре и новых средств аналитики данных и управления ими. Мы поддерживаем эти преобразования, предлагая инновации в области инфраструктуры, управления инфраструктурой и аналитики для получения ценной оперативной информации на основе имеющихся данных.

Цель Cisco – уйти от реактивной модели в поиске и устранении неполадок к проактивному подходу, сократив время на разрешение проблем с нескольких дней до нескольких минут. Для этого мы будем рассматривать каждое устройство как датчик и элемент распределенной обработки данных. Получая данные с устройств на периметре и обеспечивая распределенную обработку данных ближе к их источнику, мы можем анализировать их со скоростью пропускной способности канала и получать ценную аналитику за счет машинного обучения.

Крупнейшая база установленного оборудования и решений на основе ASIC Cisco позволяет нам разрабатывать и выпускать аппаратное и программное обеспечение, оптимизированное для аналитики. Используйте потенциал огромной базы установленного оборудования и ПО. Сочетание проводных и беспроводных технологий в одной сети будет означать, что аналитика на сетевом периметре будет помогать вам в устранении неполадок за считанные секунды независимо от того, происходят они на периметре или в другом месте. А со временем вы сможете устранять проблемы еще до их возникновения. Это поможет ИТ-отделам выполнять соглашения об уровне обслуживания (SLA) и соответствовать будущим требованиям по производительности для сетей и приложений.

Заключение

В условиях, когда так много зависит от периметра сети, «коммодитизация» проводных и беспроводных сетей LAN и WAN связана с рисками нарушения безопасности, снижения производительности или доходов, потери возможностей и отсутствия прозрачности. Периметр сети Cisco позволяет организациям пойти дальше готовых решений, основанных на стандартах, и обеспечить получение ценной аналитики на сетевом периметре.

Этот подход позволит организациям:

- Обеспечить безопасность бизнеса, надежно укрепив первую линию защиты.
- Уверенно предоставлять приложения целевым пользователям.
- Создать условия для эффективной работы сотрудников независимо от их местонахождения или используемого устройства.
- Взаимодействовать с клиентами и предлагать им новые услуги и продукты.
- Эффективно управлять устройствами IoT и оптимизировать физическую среду.
- Получить объективную картину того, что действительно происходит в бизнесе.

Дополнительная информация

Подробнее см. на веб-странице, посвященной технологии унифицированного доступа Cisco: http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.

C11-737691-00 08/16