Защищенные сети без границ

Ценность решения Cisco "защищенные сети без границ"

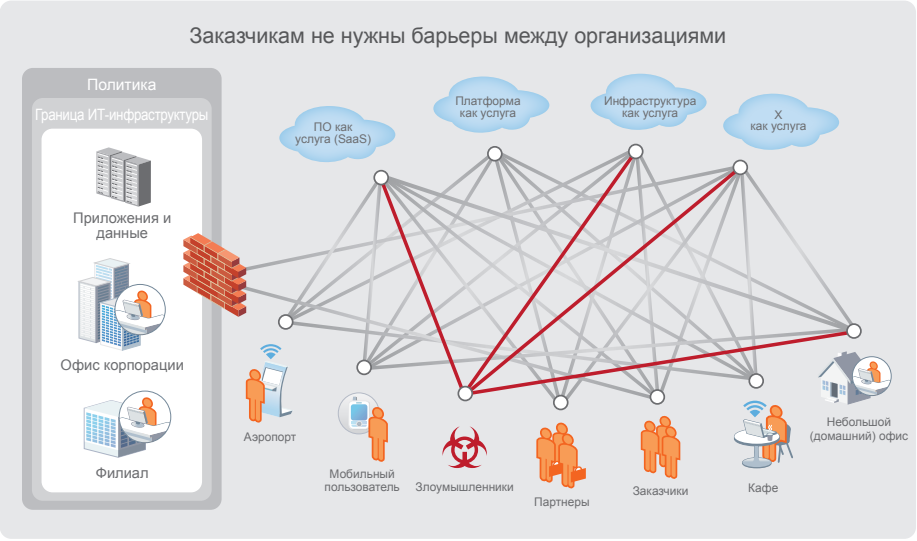
Комплексный подход в сфере безопасности, который реализован в решении Cisco® "защищенные сети без границ", позволяет сотрудникам поддерживать высокий уровень производительности, и сохранять при этом контроль над сложностью ИТ-инфраструктуры и затратами на ее поддержку.

Решение Cisco® "защищенные сети без границ" — это архитектурный подход к интеграции средств безопасности в распределенную сеть. Благодаря гибким решениям, интегрированной и комплексной защите, а также интеллектуальным средствам упреждающего реагирования решение Cisco® "защищенные сети без границ" расширяет зону обеспечения безопасности с возможностью использования необходимым сотрудникам, устройствам и в нужном месте. Эта архитектура позволяет заказчикам создавать решения, обеспечивающие надежную защиту организации и позволяющие эффективно бороться с постоянно возникающими угрозами для бизнеса и безопасности (см. рис. 1).

Проблемы, решаемые с помощью архитектуры

Традиционные подходы обеспечения безопасности предназначались для защиты ресурсов от угроз и вредоносного ПО. Решить эту задачу становилось все труднее в постоянно меняющихся условиях обеспечения безопасности. Сегодня наличие разнообразных технологий, устройств и инфраструктуры коммуникаций расширило наши возможности для совместной работы и подержания связи. Хотя преимущества прогресса очевидны, но возникают и дополнительные риски, которые ставят новые задачи для специалистов по безопасности.

Рис. 1. Расширение безопасности в среде "без границ"



Организациям по-прежнему нужно обеспечивать защиту от угроз, безопасность ценных данных и ресурсов, а также поддерживать необходимый уровень контроля для соблюдения установленных норм. Однако для распределенных рабочих ресурсов и сети "без границ", используемой для их поддержки, требуется создание новой стратегии безопасности для выполнения следующих задач.

- Обеспечение совместной работы — организации внедряют новые приложения для интегрированных сервисов голосовой, видео- и конференц-связи. Для защиты этих приложений от уязвимостей, снижения рисков и поддержания доступности необходимо обеспечить их безопасность.
- Рост популярности пользовательских электронных устройств. Популярность мобильных компьютерных устройств на потребительском рынке обусловила их появление в корпоративных сетях. Хотя их использование обеспечивает оперативность действий конечных пользователей, ИТ-подразделениям и подразделениям, занимающимся обеспечением безопасности, необходимо определить способ защиты подключений этих устройств, а также распространить на них действие соответствующих сервисов и политик безопасности.
- Модели предоставления "ПО как услуга" (SaaS). Размещение большего числа приложений и служб в распределенных сетевых сервисах может представлять значительные эксплуатационные преимущества, но организациям необходима гарантия защиты данных, выходящих за пределы корпоративных сетей, и уверенность в сохранении безопасности.

Эти тенденции способствуют появлению новой модели безопасности, даже если организация стремится к постоянному контролю затрат и снижению уровня сложности ИТ-инфраструктуры для повышения эффективности эксплуатации.

Обзор решения Cisco "защищенные сети без границ"

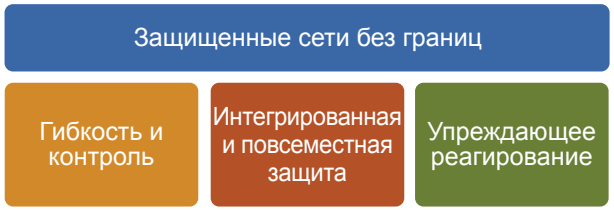
У защищенных сетей без границ есть три основные характеристики (см. рис.2).

- Гибкость. Решение Cisco "защищенные сети без границ" использует основные концепции безопасности, управление угрозами, защиту данных, безопасные подключения, и распространяет их действие на распределенные ресурсы. Это решение предоставляет компаниям и их сотрудникам гибкость и свободу выбора способов усовершенствования бизнес-процессов без ущерба для контроля над применением политик и снижением уровня риска.
- Интегрированные и повсеместные решения. Чтобы обеспечить решение критически важных бизнес-задач в сфере информационной безопасности, в решении Cisco "защищенные сети без границ" предусмотрено внедрение средств безопасности в различных форм-факторах для упрощения развертывания. Используя сеть в качестве платформы, предприятия могут применять интегрированные средства обеспечения сетевой безопасности, отдельные устройства, решения на хостинге, гибридные решения или использовать модель "ПО как услуга" (SaaS) для создания широкого спектра решений безопасности. Для достижения максимальной выгоды от вложений в безопасность компания Cisco создает экосистему партнерских отношений и предоставляет профессиональные услуги для создания одного из наиболее полных предложений на рынке.

Защищенные сети без границ

- Системы упреждающего реагирования. Аналитический центр Cisco в сфере информационной безопасности (SIO) использует распределенные средства отслеживания угроз для создания расширенной инфраструктуры управления угрозами, которая обеспечивает обнаружение угроз, анализ на основе репутации и разработку методик отражения угроз для поддержания наивысшего уровня безопасности ИТ-инфраструктур заказчиков Cisco.

Рисунок 2. Защищенные сети без границ



Архитектура, основанная в соответствии с данными принципами, позволяет заказчикам создавать гибкие решения, отвечающие постоянно меняющимся задачам бизнеса и безопасности.

Примеры решений

Безопасность мобильных пользователей

Решение Cisco Secure Mobility предоставляет инновационный способ защиты мобильных сотрудников на платформах ПК или смартфонов (рис. 3). Это решение упрощает работу конечных пользователей, обеспечивая постоянное подключение к сети и защиту с одновременной реализацией комплексных политик ИТ-администраторами, которые занимаются управлением безопасности распределенных ресурсов.

Рис. 3. Решение Cisco Secure Mobility

Cisco ScanSafe

С увеличением количества удаленных сотрудников и ужесточением требований к полосе пропускания возрастает необходимость в приближении сервисов безопасности к пользователю. Решение Cisco ScanSafe предлагает реализацию политик безопасности и интеллектуальных средств в качестве web-сервисов для упрощения развертывания и эксплуатации при одновременном расширении охвата распределенных трудовых ресурсов.

Cisco TrustSec

Безопасный доступ ко всей сети и ресурсам на основе политик — это ключевой фактор любой стратегии безопасности. Благодаря определению последовательного набора политик решение Cisco TrustSec обеспечивает основу, помогающую заказчикам получать сведения о пользователях, подключающихся к сети, а также контролировать и управлять их действиями. Решение TrustSec обеспечивает безопасность с поддержкой идентификации и предоставляет сервисы, которые могут применяться к любым пользователям, подключающимся к защищенной сети без границ в любой точке мира и в любое время.

Преимущества архитектуры

Для специалистов в сферах ИТ и безопасности решение Cisco "защищенные сети без границ" предоставляет следующие возможности:

- упрощает распространение необходимых средств безопасности на системы современных сотрудников;
- увеличивает производительность, обеспечивая гибкость и свободу выбора для сотрудников;
- позволяет внедрять новые бизнес-модели, такие как модель "ПО как услуга" (SaaS), без ущерба для безопасности;
- помогает управлять рисками и обеспечивать соответствие нормативным требованиям.

Для конечных пользователей решение Cisco "защищенные сети без границ" предоставляют следующие возможности:

- предоставляет возможность выбора места и времени получения доступа к информации;
- позволяет выбирать используемые устройства для доступа к информации и выполнения работы;
- обеспечивает безопасность и постоянный доступ пользователей, позволяя им не беспокоиться о подключении. Вместо этого они просто работают.

Почему Cisco?

Подход Cisco представляет подлинно архитектурный подход к безопасности. Благодаря интеграции средств безопасности во все элементы сети Cisco упрощает задачу соблюдения современных требований безопасности независимо от приложений и сервисов. Решение Cisco "защищенные сети без границ" сочетает гибкость с одновременным обеспечением управления, интегрированной и повсеместной защиты и функциями упреждающего реагирования для расширения безопасности на необходимые устройства, местоположения и пользователей. В результате предприятия получают возможность создавать решения, обеспечивающие безопасность всей организации и достижение бизнес-целей.

C45-578562-00 01/10