



Решение проблем клиентов

Физические границы исчезают. Заказчикам необходимо поддерживать мобильных сотрудников, управлять аутсорсингом и реагировать на резкий рост популярности персональных электронных устройств. Кроме того, наличие угроз обуславливает необходимость более эффективной системы защиты инфраструктуры бизнеса и ценных информационных активов. Наконец, отраслевые стандарты и нормативные документы устанавливают строгие требования, которые распространяются на множество организаций. Решение Cisco® TrustSec, основной компонент системы защиты сетей без границ, позволяет заказчикам обеспечить безопасную совместную работу, повысить уровень защищенности ИТ-инфраструктуры и гарантировать соответствие нормативным требованиям.

Основные функции

Решение Cisco TrustSec обеспечивает комплексную защиту сетей и доступа к крайне важным ресурсам благодаря контролю и наблюдению за всеми пользователями, а также обнаружению и мониторингу устройств с поддержкой IP. Решение осуществляет эти функции с помощью механизма контроля доступа на основе политик, сетей с поддержкой идентификации, а также средств обеспечения конфиденциальности и целостности данных в сети.

Контроль доступа на основе политик. Решение Cisco TrustSec предоставляет средства управления сетевым доступом на основе согласованной политики для пользователей (например, сотрудников, подрядчиков и гостей), конечных устройств (ноутбуков, IP-телефонов и принтеров) и сетевых устройств (коммутаторов, маршрутизаторов и т. д.). Решение Cisco TrustSec позволяет управлять предоставлением доступа пользователю или устройству, указывать политики безопасности для конечных устройств (например, соответствие состояния устройства установленным требованиям) и определять сетевые ресурсы, доступные пользователям в сети.

Сети с поддержкой идентификации. Решение Cisco TrustSec использует данные идентификации конечных пользователей и устройств, а также дополнительные параметры (такие как время, местонахождение и роль пользователя в организации) для предоставления подходящих средств управления политиками безопасности. Решение TrustSec также обеспечивает дополнительные сетевые сервисы на основе ролей, включая поддержку Медиасети Cisco и качество обслуживания для важных бизнес-приложений, связанных с конкретными ролями пользователей.

Конфиденциальность и целостность данных. Решение Cisco TrustSec защищает каналы передачи данных в коммутируемых средах с помощью стандарта шифрования IEEE 802.1AE. Конфиденциальность и целостность данных обеспечиваются на последовательной основе между устройствами на

уровне порта коммутатора. Инфраструктура коммутации Cisco поддерживает необходимые средства управления, чтобы такие важные приложения безопасности как межсетевые экраны, системы предотвращения вторжений и средства анализа контента могли осуществлять анализ потоков данных.

Преимущества

Обеспечение безопасной совместной работы. Cisco TrustSec в динамическом режиме назначает права доступа и сервисы для пользователей и устройств с целью обеспечения активной поддержки ресурсов. Согласованные и эффективные сетевые возможности с учетом ролей, предоставляемые решением TrustSec, обеспечивают безопасную бизнес-среду для совместной работы и бесперебойную работу пользователей.

Повышение уровня безопасности. Решение Cisco TrustSec защищает доступ к сети (проводной, беспроводной или VPN) и сетевым ресурсам, обеспечивая авторизацию и работоспособное состояние конечных устройств. Решение TrustSec позволяет применять политики безопасности во всей сети. Более того, решение TrustSec обеспечивает конфиденциальность и целостность сетевых данных благодаря шифрованию на уровне порта коммутатора.

Обеспечение соответствия нормативным требованиям. Решение Cisco TrustSec обеспечивает соответствие нормативным требованиям благодаря наличию сведений о пользователях в сети, их действиях и типах ресурсов, к которым им предоставлен доступ. Заказчики могут использовать эти данные и возможности для контроля, аудита и создания отчетов в рамках деятельности по обеспечению соответствия нормативным требованиям.

Линейка продуктов

Решение Cisco TrustSec включает три группы продуктовых компонентов: инфраструктура, политика и конечные устройства.

Компоненты инфраструктуры. Коммутаторы Cisco Catalyst® серий 2900/3560/3700/4500/6500 и коммутаторы Cisco Nexus™ 7000 поддерживают аутентификацию и авторизацию пользователей сети. Доступ к сети определяется политиками, идентификационными данными пользователя и другими атрибутами. К гибким методам аутентификации относятся 802.1X, web-аутентификация и резервный метод аутентификации по MAC-адресу (MAB), управляемые с помощью одной конфигурации для каждого порта коммутатора. Более того, коммутаторы Cisco могут пометать каждый пакет данных сведениями, идентифицирующими пользователя, что позволяет развертывать дополнительные средства управления в любом месте сети. Необходимо также отметить, что коммутаторы Cisco Nexus теперь поддерживают MACSec (стандарт шифрования IEEE 802.1AE) для обеспечения конфиденциальности и целостности передаваемых данных.



Компоненты политики. Система Cisco Secure Access Control System (ACS) — это простой, но довольно мощный сервер политики для централизованной сетевой идентификации и контроля доступа. Cisco Secure ACS включает модель политики на основе правил и новый интуитивно понятный интерфейс управления, предназначенный для оптимального контроля и наблюдения. Последняя версия Cisco Secure ACS также позволяет ИТ-администраторам быстро выявлять потенциальные проблемы благодаря средствам всестороннего мониторинга и устранения неполадок.

Решение Cisco NAC Manager — это центр политик и управления для среды развертывания на базе устройства NAC Appliance. Он предназначен для определения прав пользователей в соответствии с ролевой моделью разграничения доступа и политик безопасности конечных устройств.

Сервер Cisco NAC оценивает и обеспечивает соблюдение политики безопасности в средах развертывания NAC на основе NAC Appliance.

Профилировщик Cisco NAC Profiler поддерживает развертывание системы контроля доступа на основе политик, обеспечивая обнаружение, профилирование, размещение на основе политик и мониторинг после подключения всех конечных устройств.

Гостевой сервер Cisco NAC обеспечивает процесс управления гостевым доступом к сети, который включает в себя контроль, уведомление, управление и создание отчетов для всех гостевых учетных записей и сетевых действий.

Компоненты конечных устройств. Cisco Secure Services Client (SSC) помогает заказчикам при развертывании единой системы аутентификации для доступа как к проводным, так и беспроводным сетям. Он обеспечивает аутентификацию пользователей и устройств 802.1X и управляет их идентификацией, а также в целях безопасности ведет протоколы сетевого доступа. Агент Cisco NAC Agent — это дополнительный облегченный программный агент, устанавливаемый на конечном устройстве. Он выполняет тщательную проверку профиля безопасности устройства, анализируя сервисы, файлы и параметры реестра. Помимо указанных выше двух клиентов для стандартных конечных устройств IP-телефоны Cisco имеют расширенные встроенные возможности клиента для интеграции с решением Cisco TrustSec.

Профессиональные услуги по внедрению решения TrustSec

Интеллектуальные персонализированные профессиональные услуги Cisco и наших партнеров предоставляют возможности проверки политик, анализа и разработки для подготовки сети к развертыванию решения TrustSec. Услуги Cisco основаны на оптимальных методиках и позволяют организациям провести быстрое и экономичное развертывание полного решения для аутентификации и доступа, обеспечивая при этом передачу информации для последующей эффективной эксплуатации внедренного решения.

Примеры использования

Вариант развертывания 1: развертывание на основе 802.1X

В этом сценарии система Cisco Secure ACS используется в качестве сервера политики для аутентификации пользователей, подключающихся к проводной сети. Устройство доступа к сети (коммутатор) обеспечивает доступ к сети и ресурсам на основании учетных данных пользователей (собираемых Cisco SSC) и сведений об их роли в организации. Для повышения уровня контроля может применяться дополнительная защита, например, добавление тегов и списки управления доступом (ACL) групп безопасности. Развертывание решения 802.1X можно также дополнить профилировщиком Cisco NAC Profiler и сервером гостевого доступа Cisco NAC Guest Server.

Вариант развертывания 2: развертывание на основе устройства NAC Appliance

При использовании подхода на основе устройства NAC Appliance менеджер Cisco NAC Manager является сервером политики, работающим с сервером Cisco NAC Server для аутентификации пользователей и оценки их устройств по локальной сети, беспроводным подключениям или подключениям по VPN. Доступ к сети и ресурсам выполняется на основании учетных данных пользователей и их ролей в организации, а также соблюдении политик конечных устройств.

Инновации TrustSec

Решение TrustSec предоставляет множество инноваций от Cisco. Режимы мониторинга и низкого влияния 802.1X обеспечивают управляемый и полностью настраиваемый сетевой доступ до аутентификации. Это способствует повышению уровня контроля, более гибкому развертыванию и улучшенной эксплуатационной поддержки. Профилировщик Cisco NAC Profiler, сервер гостевого доступа и интеграция IP-телефонии со средствами коммутации Cisco в среде 802.1X значительно увеличивают производительность ИТ и сотрудников. Списки управления доступом (ACL) групп безопасности упрощают управление политиками безопасности благодаря включению конечных пользователей в состав группы безопасности и назначению соответствующих прав для ресурсов вместо ACL на основе IP-адресов. Решение TrustSec предоставляет клиентам усовершенствованные технологии обеспечения безопасности, такие как 802.1X-REV и MACSec.

Почему Cisco?

Решение Cisco TrustSec — это комплексное решение, гибкое и удобное в использовании и эффективное при развертывании. Оно обеспечивает безопасность инфраструктуры для поддержки управляемых, неуправляемых и неизвестных активов, а также сотрудников, гостей и поставщиков.

Сети Cisco с защитой TrustSec обеспечивают полный контроль и управление. Решение TrustSec улучшает гибкость, согласованность и масштабируемость сети.

Компания Cisco и ее партнеры предоставляют профессиональные сервисы для помощи клиентам в обеспечении необходимого соответствия требованиям и безопасности.

Более подробную информацию см. на web-сайте <http://www.cisco.com/go/trustsec>.