Краткий обзор

Платформа Cisco Identity Services Engine

Корпоративная сеть больше не ограничивается «четырьмя стенами», защищающими ее безопасность. Она должна быть везде, куда направляются сотрудники и данные. Постоянно увеличивается число устройств и сетей, с помощью которых работники хотят получать доступ к рабочим ресурсам. Мобильность и Всеобъемлющий Интернет (IoE) изменяют привычный ход работы и жизни. Предприятия вынуждены обеспечивать поддержку растущего числа устройств с доступом к сети, и при этом множество угроз безопасности и утечки данных, о которых мы часто слышим, явно указывают на необходимость защищать доступ к развивающейся корпоративной сети.

По мере расширения современной сети становится все сложнее распределять ресурсы, управлять разнородными решениями безопасности, контролировать риски. Прибавьте к этому доступ из любой точки благодаря Всеобъемлющему Интернету и уже перегруженные ИТ-ресурсы, и потенциальные последствия неспособности идентифицировать и нейтрализовать угрозы безопасности становятся чрезвычайно ощутимыми.

Требуется другой подход к управлению развивающейся корпоративной мобильной средой и ее защите. Это платформа Cisco® Identity Services Engine (ISE).

Преимущества

- **Централизация и унификация контроля безопасного доступа** на основе бизнес-роли для обеспечения единообразной политики управления сетевым доступом конечных пользователей, подключающихся по проводным и беспроводным сетям и VPN.
- **Более точный контроль и идентификация устройств** благодаря платформе Cisco® Identity Services Engine (ISE) с функциями создания и передачи профилей устройств, которые в сочетании друг с другом сокращают число неизвестных оконечных устройств.
- **Упрощение среды для гостевых пользователей** для снижения сложности подключения и администрирования устройств через настраиваемые фирменные гостевые порталы в мобильных и настольных версиях, которые можно создать за минуты с помощью динамических наглядных процедур, позволяющих вам без проблем управлять удобством работы гостей.

Расширяйте защиту и снижайте риски

Опережайте угрозы с помощью возможностей контроля и управления. Это и тщательный контроль пользователей и устройств, получающих доступ к вашей сети, и динамическое управление, которое открывает доступ к корпоративным услугам только проверенным пользователям с проверенных устройств.

С перестроенной платформой ISE 2.0 поддерживать стабильный контроль безопасного доступа по проводным и беспроводным сетям, а также удаленным VPN-подключениям становится еще проще. Благодаря масштабным интеллектуальным функциям создания профилей и обнаружения платформа Cisco ISE проникает вглубь сети, обеспечивая максимальный контроль доступа пользователей и устройств к ресурсам. За счет обмена ключевыми контекстуальными данными с интегрированными партнерскими экосистемами и внедрения политики Cisco TrustSec для программно определяемой сегментации платформа Cisco ISE преобразует сеть из обычного канала передачи данных в центр безопасности, сокращающий время обнаружения и устранения сетевых угроз.

- **Ускорение внедрения BYOD и корпоративной мобильной среды** благодаря простым готовым настройкам, самообслуживанию в процессе подключения и контроля устройств, внутреннему управлению сертификатами устройств, а также интегрированному партнерскому ПО для управления корпоративной мобильной средой, обеспечивающему подключение устройств на территории предприятия и за ее пределами.
- **Построение политики программно определяемой сегментации для сдерживания сетевых угроз** с помощью технологии Cisco TrustSec®, обеспечивающей управление доступом на основе ролей на уровне маршрутизации и коммутации. Динамическое сегментирование доступа без сложных сетей VLAN и без необходимости перестраивать сеть.
- **Обмен подробными контекстными данными с партнерской сетью и решениями информационной безопасности** с целью повышения их общей эффективности, а также сокращения времени обнаружения и времени устранения сетевых угроз.
- **Автоматическая блокировка угроз** за счет интеграции с центром управления Cisco Firepower, так как ISE может блокировать зараженные оконечные устройства для восстановления, наблюдения или удаления.

Версия ISE 2.0 включает в себя следующие обновления и улучшения:

- Интеграция с платформой сервисов мобильности Cisco Mobility Services Engine (MSE), позволяющая предоставлять данные о местоположении для создания и применения локальных политик доступа, чтобы, например, медицинские работники могли получать доступ к истории болезни пациентов только в приемном отделении.
- Усовершенствование нашей открытой архитектуры для определенных партнерских экосистем ISE, позволяющее заказчикам использовать существующие решения по обеспечению информационной безопасности в сочетании с ISE, что дает возможность обнаруживать угрозы в сети, а также способствует быстрой блокировке и восстановлению.
- Поддержка устройств сетевого доступа (NAD) и оконечных устройств IPv6 сторонних производителей с целью расширения возможностей ISE для обеспечения соответствия оконечных устройств нормативным требованиям в более широком диапазоне сетей.
- Оптимизированное управление политиками, включая упрощенное администрирование устройств с аутентификацией, авторизацией и учетом (AAA) и возможностями доступа TACACS+ и RADIUS, что в значительной степени облегчает развертывание политики контроля безопасного доступа для проводных сетей.
- В комплекте с Cisco AnyConnect 4.2 поставляется модуль контроля состояния сети (NVM), предоставляющий такой уровень контроля потоков трафика приложений, какой ранее был недоступен для внешних оконечных устройств.

Кроме того, ISE использует технологию Cisco Platform Exchange Grid (pxGrid) для обмена подробными контекстными данными с интегрированными решениями экосистемы партнеров. Эта технология расширяет возможности идентификации и отражения угроз безопасности в вашей распределенной сети, а также устранения последствий атак. Централизовано и упрощено управление безопасным доступом, что позволяет надежно предоставлять доступ к основным бизнес-сервисам, усиливать безопасность инфраструктуры, контролировать соответствие нормативным требованиям и оптимизировать операции обслуживания.

Благодаря интеграции с ведущими решениями для управления информацией и событиями об информационной безопасности (SIEM), высокому уровню контроля состояния сети и функциям контроля безопасного доступа, ISE является неотъемлемой частью решений Cisco Cyber Threat DEfense, Network-as-a-Sensor и Network-as-an-Enforcer. ISE обеспечивает контроль, контекст и динамическое управление, эффективно поддерживая высокий уровень информационной безопасности до, во время и после атаки, — управление сетевым доступом до атаки, контроль и сдерживание угроз во время атаки, сокращение времени обнаружения и времени устранения после атаки.

Дальнейшие шаги

Для получения более подробной информации о платформе Cisco ISE перейдите на страницу http://www.cisco.com/go/ise или свяжитесь с вашим региональным представителем.

C45-654884-13, октябрь 2015 г.