ОБЗОР РЕШЕНИЯ

Платформа Aruba ESP — модель безопасности “нулевое доверие”

Безопасность сетевой инфраструктуры

В последние годы требования к сетевой безопасности значительно изменились: пользователям необходима децентрализация, а атаки участились и стали более изощренными. Традиционные подходы к сетевой безопасности, которые были направлены на защиту периметра сети, стали неэффективными без вспомогательных стратегий. Современная система сетевой безопасности должна работать с постоянно меняющимся набором пользователей и устройств и учитывать угрозы, от ранее считавшихся безопасными элементов сетевой инфраструктуры.

Модель нулевого доверия стала эффективным ответом на новые требования к безопасности современного предприятия. Согласно этой модели, все пользователи, устройства, серверы и сегменты сети считаются небезопасными и потенциально вредоносными. Благодаря использованию более строгих мер безопасности и средств контроля платформа Aruba ESP на основе модели нулевого доверия повышает общую безопасность сети.

ПЛАТФОРМА ARUBA ESP: КЛЮЧЕВЫЕ ПРИНЦИПЫ МОДЕЛИ НУЛЕВОГО ДОВЕРИЯ

Реализация модели нулевого доверия может значительно отличаться в зависимости от сферы, безопасность которой требуется обеспечить. Средства контроля на уровне приложений являются ключевой точкой модели нулевого доверия, но необходим комплексный подход с учетом сетевой безопасности, увеличивающегося количества подключенных устройств и удаленной работы сотрудников. Платформа Aruba ESP на основе модели нулевого доверия включает принципы микросегментации для ограничения доступа, полной видимости сети и функции непрерывного мониторинга сетевого поведения и реагирования на его изменение. Благодаря использованию унифицированных средств контроля для кампусных сетей и сетей филиалов, а также отдельных удаленных сотрудников, можно улучшить даже традиционные решения VPN.

В век Интернета вещей бывает сложно реализовать базовые принципы надлежащей сетевой безопасности. По возможности все устройства и пользователи должны быть идентифицированы и пройти надлежащую аутентификацию перед получением доступа к сети. При этом должен действовать принцип минимальных привилегий: пользователи и устройства получают доступ только в том объеме, который необходим для выполнения важных для организации задач. Необходимо определить, к каким сетевым ресурсам и приложениям пользователь или устройство могут обращаться. Кроме того, обмен данными между пользователем и приложением должен быть зашифрован.

НЕОБХОДИМОСТЬ ПОЛНОЙ ВИДИМОСТИ

С повсеместным внедрением Интернета вещей обеспечение полной видимости устройств и пользователей сети усложнилось. Без достаточного уровня видимости затруднительно применять средства контроля, необходимые для реализации на практике модели нулевого доверия. Ключевое значение имеют автоматизация, машинное обучение с использованием ИИ и быстрое определение типа устройства.

В решении Aruba ClearPass Device Insight используется сочетание технологий активного и пассивного определения типа сетевого устройства и его профилирования. Это позволяет установить профиль любого устройства, уже находящегося в сети или

только подключающегося к ней. Такими устройствами, например, могут быть обычные ноутбуки и планшеты. В отличие от традиционных технологий, ClearPass Device Insight позволяет профилировавть разнообразные устройства Интернета вещей, которые подключаются к современным сетям.

РЕАЛИЗАЦИЯ ПРИНЦИПОВ МИНИМАЛЬНЫХ ПРИВИЛЕГИЙ И МИКРОСЕГМЕНТИРОВАНИЯ

Следующим шагом после обеспечения видимости в модели нулевого доверия является надлежащая реализация принципов минимальных привилегий и микросегментирования. Для конечных точек сети используются наилучший из возможных метод аутентификации (т. е. 802.1X и многофакторная аутентификация для пользовательских устройств) и сетевая политика, разрешающая доступ пользователя или устройства только к необходимым ресурсам.

Решение Aruba ClearPass Policy Manager позволяет создавать политики доступа на основе ролей. Отдел ИТ-безопасности может создать роль с правами доступа один раз, а затем использовать ее в любой точке сети — проводной или беспроводной, на уровне кампуса или филиала. После определения профиля устройства оно автоматически получает права доступа и подключается в собственный сегмент с помощью решения Aruba Dynamic Segmentation. За ограничение отвечает Aruba Policy Enforcement Firewall (PEF) — полнофункциональный сетевой экран, встроенный в сетевую инфраструктуру Aruba. Инфраструктура Aruba также поддерживает самые безопасные протоколы шифрования, например WPA3 для подключения по беспроводной локальной сети.

Решение ClearPass Policy Manager также включает набор средств аутентификации, позволяющий использовать многофакторную аутентификацию и принудительную повторную аутентификацию для ключевых ресурсов сети. В экосистеме ClearPass можно легко реализовать и другие принципы модели нулевого доверия, связанные с обработкой контекстной информации и телеметрических данных, необходимых для обеспечения безопасности.

Платформу ClearPass можно интегрировать с решением для защиты безопасности конечных устройств, которое позволит учитывать их состояние для управления сетевой политикой. Политику можно изменять в зависимости от типа устройства, местоположения пользователя и других контекстных данных.

НЕПРЕРЫВНЫЙ МОНИТОРИНГ СЕТЕВОГО ПОВЕДЕНИЯ И РЕАКЦИЯ НА ЕГО ОТКЛОНЕНИЕ ОТ НОРМАЛЬНОГО

Для эффективного использования модели нулевого доверия с микросегментированием и политикой контроля доступа на основе ролей необходим постоянный мониторинг сетевого поведения пользователей и устройств. Эта мера предотвращает недопустимые действия персонала, вмешательство сложных вредоносных программ и устойчивые угрозы, преодолевшие основную защиту периметра.

Защита от угроз с помощью IDS/IPS

Защитные возможности Aruba эффективны против различных угроз, включая фишинговые атаки, DoS-атаки и участившиеся атаки вирусов-вымогателей. Шлюзы Aruba 9000 SD-WAN в сочетании с системой Aruba Central, ClearPass Policy Manager и Policy Enforcement Firewall позволяют реализовать систему обнаружения и предотвращения вторжений (IDS/IPS) на основе пользовательских данных. Система IDS/IPS проверяет передаваемые пользователями данные с помощью сигнатур и шаблонов. Проверяются входящие и исходящие данные внутри центрального сегмента, а также передаваемые между центральным сегментом и

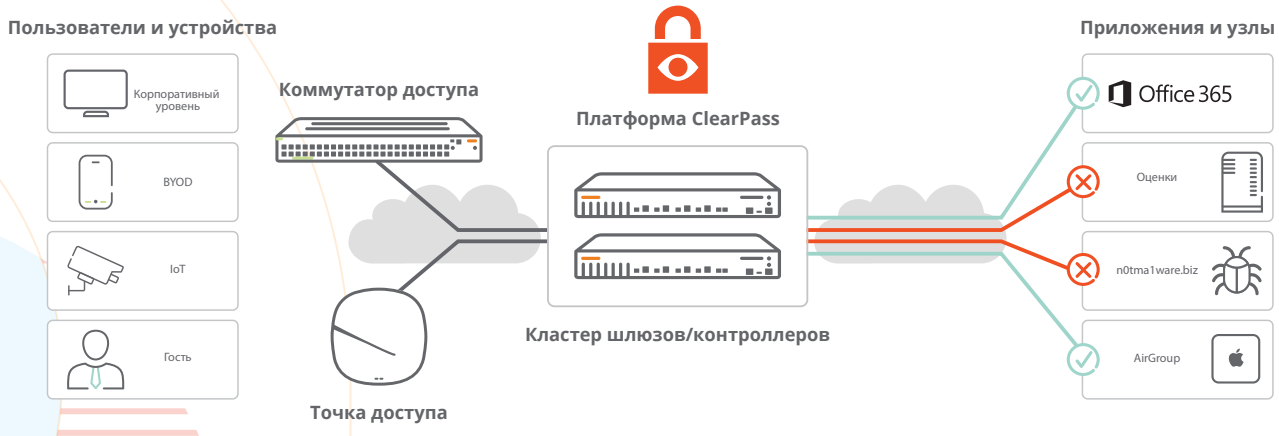

Рис. 1. Платформа Aruba ClearPass автоматически назначает сетевые политики, реализуемые с помощью решения Dynamic Segmentation

ARUBA ESP — СЕТЕВАЯ ПЛАТФОРМА

Первая в мире сетевая платформа, обладающая искусственным интеллектом со сверхчеловеческими способностями в областях автоматизации и безопасности

Рис. 2. Модель нулевого доверия — основа платформы Aruba ESP

сетью филиала. Инновационная система управления средствами безопасности Aruba Central обеспечивает ИТ-отделы полной видимостью, многомерными метриками угроз, корреляционными и аналитическими данными и средствами управления в чрезвычайных ситуациях. Сигналы о происшествиях отправляются в системы SIEM и ClearPass для исправления ситуации.

Полная интеграция

Доступны более 150 вариантов интеграции с лучшими системами безопасности, включая системы обработки событий безопасности и автоматического реагирования (SOAR). Решение ClearPass Policy Manager может динамически управлять доступом в зависимости от данных телеметрии угроз. Права доступа можно изменять в режиме реального времени по сигналам, которые поступают от сетевых экранов нового поколения (NGFW), систем управления информацией о безопасности и событиями безопасности (SIEM) и из других источников. Можно полностью настроить действия платформы ClearPass — от ограничения доступа (например, только интернет) до полного удаления устройства из сети для исправления ситуации.

ARUBA ESP — СЕТЕВАЯ ПЛАТФОРМА

Мы разработали платформу Aruba ESP, чтобы помочь клиентам использовать новые возможности сетевой инфраструктуры. Это первая в отрасли сетевая платформа, основанная на искусственном интеллекте, которая обеспечивает безопасность на границе сети, а так же автоматизирует и унифицирует сетевые подключения. Модель нулевого доверия — основа платформы Aruba ESP. В сочетании с унифицированной инфраструктурой и AIOps это позволяет организации сократить расходы, упростить работу и обеспечить безопасность.

ЗАКЛЮЧЕНИЕ

Современные сети и угрозы требуют нового подхода. Стратегия безопасности, ориентированная на защиту периметра, создавалась без учета возможности удаленной работы сотрудников и использования Интернета вещей. Платформа Aruba ESP на основе модели нулевого доверия содержит полный набор средств для обеспечения видимости, управления и контроля. Она позволяет создать децентрализованную сетевую инфраструктуру, поддерживающую подключение устройств Интернета вещей.

SO_ZeroTrustSecurity_051120 a00097694enw