ВОЗМОЖНОСТИ ЧЕЛОВЕКО-МАШИННОГО ИНТЕРФЕЙСА С УДАЛЕННЫМ ДОСТУПОМ

ДЖОНАТАН ГРИФФИТ (JONATHAN GRIFFITH)
ПЕРЕВОД: ВЛАДИМИР РЕНТЮК

Доступ к мобильному человеко-машинному интерфейсу (англ. human-machine interface, HMI) это не прихоть, а насущная необходимость для многих приложений промышленной автоматизации. В этом плане существует два типичных метода реализации такого соединения: с маршрутизаторами (роутерами) и виртуальными частными сетями, известными как VPN1. Доступ может быть осуществлен через стандартный маршрутизатор без VPN и облачный VPN-маршрутизатор. Рассмотрим особенности обоих подходов.

Первый вариант доступа к мобильному HMI — стандартный маршрутизатор (роутер), и хотя он не является безопасным, данное решение все еще применяется во многих существующих приложениях мобильных HMI и даже используется в некоторых уже более современных. Главное преимущество подобной реализации — ее низкая стоимость, но такой подход не рекомендуется, поскольку, когда в межсетевом защитном экране (брандмауэре, файерволе) включена переадресация портов, он создает значительные риски в части кибербезопасности, соответственно, подвергает внешним угрозам корпоративную сеть или сеть предприятия.

Сложность информационных технологий упрощает облачный VPN-маршрутизатор, создающий поверх привычного интернет-соединения зашифрованное соединение от локального VPN-маршрутизатора до облачного VPN-маршрутизатора. Благодаря такому подходу удаленные пользователи могут получить безопасный доступ к локальным компонентам и системам через облачный VPN-маршрутизатор. Это не только снижает риски в части кибербезопасности, но и облегчает конфигурирование и обслуживание.

Третий тип подключения маршрутизатора с традиционной реализацией VPN-маршрутизатора здесь не рассматривается, поскольку он включает открытие входящих подключений и создает сложности и риски, аналогичные стандартной реализации маршрутизатора.

СТАНДАРТНЫЙ МАРШРУТИЗАТОР

Стандартный маршрутизатор используется во многих промышленных приложениях, при этом для защиты корпоративной и промышленной сети применяется межсетевой защитный экран. Такое решение требует от пользователей ручной настройки (конфигурирования) и управления как всеми настройками маршрутизации, так и настройками межсетевого защитного экрана. Маршрутизаторы этого типа обычно не имеют VPN для шифрования данных, и, как следствие, для того чтобы получить доступ к определенным приложениям и компонентам в сети предприятия, для переадресации портов для удаленных пользователей в межсетевом защитном экране создаются «дыры».

Однако большинство пользователей HMI хотят иметь и удаленный, и локальный доступ. Для локального подключения обычно предназначаются ноутбуки, которые подключаются к веб-серверу HMI для мониторинга данных и внесения изменений в заданные значения и другие параметры, либо они подключаются к HMI с программным обеспечением для устранения неполадок или внесения изменений в программу.

Для удаленного подключения с использованием стандартного маршрутизатора переадресация портов обычно настраивается таким образом, чтобы разрешить доступ к HMI или локальному ПК, на котором запущено программное обеспечение для удаленного доступа. Этот локальный ПК и разрешает удаленному пользователю запускать программное обеспечение HMI.

Однако мобильные приложения HMI типа apps (для того чтобы удаленный пользователь мог получить доступ к локальному HMI для управления или просмотра данных) также требуют переадресации портов. Эти приложения обычно предоставляют ту же функциональность, что и удаленный доступ через браузер, но он осуществляется непосредственно через приложение.

Основной проблемой этого подхода становится риск нарушения безопасности, связанный с переадресацией портов в мобильных приложениях и приложениях для ПК. Хакеру легко определить, какие порты открыты в межсетевом защитном экране, и через них, пользуясь маршрутизатором, получить доступ к корпоративной сети или сети предприятия.

Хотя переадресация портов может быть чрезвычайно эффективной и полезной в корпоративной или заводской сети, все

[1] Virtual Private Network, VPN («виртуальная частная сеть») — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). — Прим. пер.

же использовать эту функцию в корпоративном интернет-интерфейсе крайне опасно, и придется делать это на свой страх и риск. Предприятия и компании должны избегать подхода с использованием маршрутизатора для новых установок и преобразовывать существующие стандартные установки маршрутизатора в более безопасное соединение, например в облачный VPN-маршрутизатор.

VPN-МАРШРУТИЗАТОР В ОБЛАКЕ

Облачные виртуальные частные сети обеспечивают безопасное соединение с простой настройкой и конфигурацией сети. Типичные варианты VPN-хостинга в облаке включают локальный VPN-маршрутизатор, VPN-сервер в облаке, VPN-клиент и подключенные компоненты автоматизации (рис. 1).

Безопасное соединение устанавливается после того, как локальный маршрутизатор в сети предприятия/управления и VPN-клиент (программное обеспечение на ноутбуке или мобильном устройстве пользователя) устанавливают соединение с облачным VPN-сервером. Локальный маршрутизатор устанавливает это соединение непосредственно сразу после запуска, но VPN-клиент подключается только после подтвержденного запроса от удаленного пользователя. Как только оба соединения реализованы, все данные, проходящие через этот VPN-туннель, являются безопасными.

Большинство VPN-хостов, размещенных в облаке, имеют бесплатное ежемесячное распределение полосы пропускания для базового трафика, а затем, после достижения этого уровня, провайдеры ограничивают доступ к данным и предлагают премиальный план для доступа к дополнительной полосе пропускания. Например, один провайдер предлагает продукт VPN с 5 Гбайт бесплатного обмена данными в месяц, что достаточно для большинства задач по устранению неполадок, мониторингу и программированию. Далее уже придется раскошелиться.

Риск для безопасности уменьшается, когда локальный маршрутизатор инициирует связь с сервером, осуществляя соединение через стандартные открытые порты, такие как HTTPS. Это обычно позволяет избежать изменений в корпоративном ИТ-брандмауэре и удовлетворяет требованиям по ИТ-безопасности. Чтобы добавить уверенности, пользователи могут искать облачные VPN, которые имеют сертифицированную в отрасли систему управления информационной безопасностью, например ISO/IEC 27001:2013[2]. Такая сертификация указывает на то, что поставщик внедрил комплексные программы безопасности и контроля.

Еще одно преимущество облачного VPN — более простая настройка маршрутизатора. Поскольку защищенный локальный маршрутизатор будет подключен к предопределенному облачному серверу, маршрутизатор поставляется с уже предварительно настроенными сложными сетевыми настройками VPN, что позволяет устанавливать его лицам, не являющимся продвинутыми ИТ-специалистами. Все, что здесь требуется, — знать IP-адреса компонентов автоматизации, подключенных к локальной сети. Динамические или статические IP-адреса присваивает поставщик интернет-услуг (провайдер) или маршрутизатор корпоративной сети (не облачный маршрутизатор VPN).

Другие дополнительные параметры могут включать регистрацию

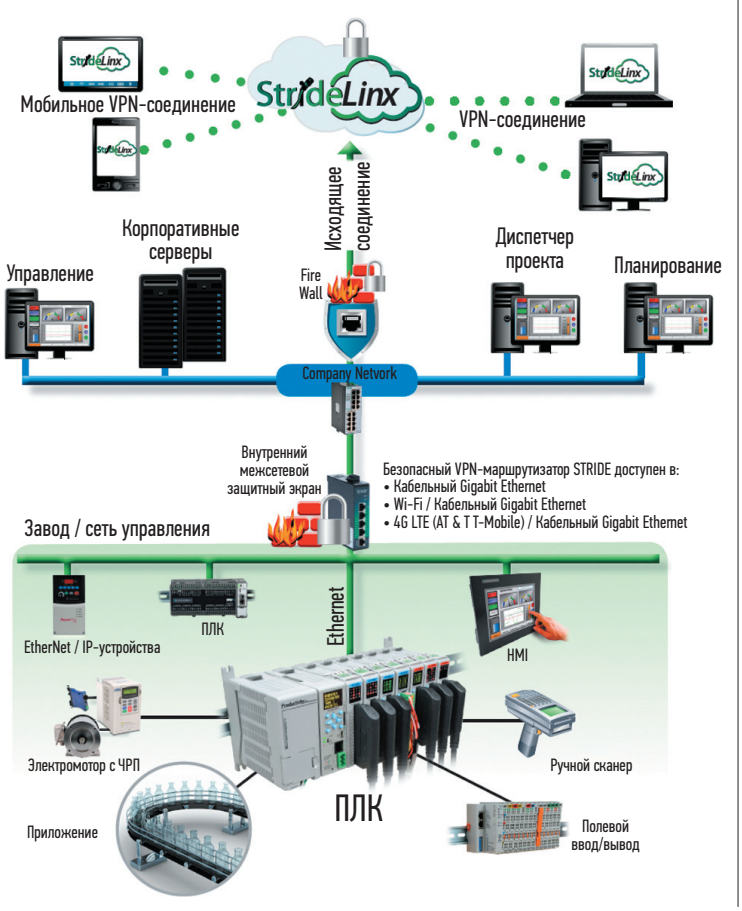

РИС. 1. ◄ Облачная виртуальная частная сеть StrideLinx от компании AutomationDirect обеспечивает безопасное подключение для мобильных приложений HMI, размещенных на ноутбуках, смартфонах и планшетах. Изображения предоставлены компанией AutomationDirect

[2] ISO/IEC 27001 — международный стандарт по информационной безопасности, разработанный совместно Международной организацией по стандартизации и Международной электротехнической комиссией. Подготовлен к выпуску подкомитетом SC27 Объединенного технического комитета JTC. Стандарт содержит требования в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности (СМИБ). В стандарте ISO/IEC 27001 (ISO 27001) собраны описания лучших мировых практик в области управления информационной безопасностью. ISO 27001 устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы. В этом направлении в РФ действует стандарт ГОСТ Р ИСО/МЭК 27013-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1», который идентичен международному стандарту ИСО/МЭК 27013:2012* «Информационная технология. Методы обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1». — Прим. пер.

данных в облаке и оповещение о тревоге, которое обеспечивает подмножество функций HMI, что также является более простым в применении, чем пользовательское программирование. Эти сервисы позволяют пользователям регистрировать системные данные и получать уже настроенные критические сигналы тревоги на своих мобильных устройствах или ноутбуках, используя доступную и удобную, основанную на веб-протоколе историю производительности системы — так называемые исторические данные.

УДАЛЕННЫЙ ДОСТУП НА ОСНОВЕ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

В настоящее время компоненты промышленного HMI и программируемого логического контроллера (ПЛК) все чаще поддерживаются мобильными приложениями. Это обеспечивает пользователям удаленный доступ с возможностями мониторинга и управления в любое время из любого места. Однако для безопасного доступа к промышленному оборудованию мобильное устройство также должно использовать технологию VPN для шифрования данных, передаваемых с мобильного устройства в сеть предприятия. Без мобильной VPN необходимо будет открыть порты брандмауэра на предприятии, создав сценарий, аналогичный стандартному маршрутизатору, и оставив сеть предприятия уязвимой для кибератаки.

Использование VPN-хоста обеспечивает безопасное VPN-соединение для ноутбуков и мобильных устройств. Последнее — через полностью поддерживаемое мобильное приложение с VPN. После безопасного подключения к сети предприятия через мобильное приложение VPN можно открыть стороннее приложение HMI или ПЛК и подключить его к локальным компонентам HMI и ПЛК, причем так, как если бы мобильный пользователь находился на месте, поскольку фактически он там и присутствует.

Некоторые маршрутизаторы уже предоставляют VPN-хост с подключениями для ноутбуков и мобильных устройств. Кроме того, приложения для мобильных устройств на PC Apple iOS и Google Android также предоставляют пользователям безопасное подключение к сети предприятия.

Некоторые поставщики VPN с размещением в облаке также предлагают доступ к работающему в облаке программному обеспечению на основе приложений для регистрации данных наряду с виджетами для настройки панелей мониторинга для удаленного просмотра (рис. 2).

Это встроенное облачное ведение журнала (лога) может быть особенно эффективным для производителя оригинального оборудования (original equipment manufacturer, OEM) с тысячами машин, установленных по всему миру в сотнях местоположений, каждая из которых имеет несколько пользователей. OEM-производитель может предоставить VPN-маршрутизатор для каждой машины, предварительно настроенный для регистрации данных и включающий настраиваемые панели мониторинга для удаленного просмотра в мобильном приложении. Заказчикам такого оборудования, за исключением установки приложения на смартфон или планшет, уже не потребуются какие-либо усилия для его настройки, конфигурирования, установки или обслуживания программного обеспечения для удаленного доступа.

Для более полного доступа, помимо панелей мониторинга, удаленные пользователи могут получать доступ к локальным HMI и ПЛК через приложения, использующие мобильный VPN от поставщика VPN-хоста. Некоторые мобильные программы HMI работают надежно при использовании с VPN-маршрутизатором конкретного поставщика. Локальное оборудование также может быть безопасно удаленно доступно ПК для программирования, мониторинга или устранения тех или иных неисправностей в его функционировании. ⬢

РИС. 2. ▶ Мобильное приложение в виде графической панели HMI C-more компании AutomationDirect безопасно функционирует при использовании с защищенным маршрутизатором StrideLinx VPN. Оно также доступно и для ОС Google Android