Новые межсетевые экраны компании Phoenix Contact

И. Хильгенкамп (Phoenix Contact Electronics GmbH),
М.Б. Линеенко, Д.С. Зозуля (ООО «Феникс Контакт РУС»)

Представлены устройства удаленного доступа к объектам автоматизации - межсетевые экраны FL MGuard RS2000 и RS4000 с функцией маршрутизации и поддержкой защищенного соединения.

Ключевые слова: удаленный доступ, межсетевые экраны, маршрутизация, поддержка защищенного соединения, антивирусная защита.

На современных промышленных предприятиях встречается большое число автоматизированных систем управления от различных производителей. Наладка и последующее сервисное обслуживание таких систем требуют привлечения высококвалифицированных специалистов. Использование устройств для организации удаленного доступа к объекту позволяет оперативно решать многие вопросы по настройке и сервисному обслуживанию систем автоматизации без выезда мастера на место установки оборудования.

У конечных потребителей систем автоматизации существует потребность в сокращении стоимости обслуживания оборудования и в повышении эффективности его использования. Отключения и отказы в работе приводят к значительным убыткам. В то же время обслуживание автоматизированных систем только собственными силами сопряжено со значительными затратами. Поэтому наиболее эффективным является взаимодействие собственных сервисных служб предприятия и специалистов производителя оборудования или инженерных компаний. Благодаря широкой доступности сети Internet, высоким скоростям передачи данных и низкой стоимости такой вид взаимодействия является предпочтительным для многих заказчиков.

Основные характеристики маршрутизаторов

При выборе системы удаленного обслуживания всегда рассматриваются: стоимость оборудования, безопасность, пропускная способность, надежность и стабильность работы, простота настройки. Отвечая на эти запросы, компания Phoenix Contact расширила свою серию межсетевых экранов FL MGuard двумя устройствами с различными классами производительности (рис. 1). Новые устройства безопасности выпускаются в надежных металлических корпусах. Карты памяти в формате SD позволяют сохранять конфигурацию системы и полезны при необходимости быстрой замены устройства. Межсетевые экраны разделены по функционалу и цене на две группы. Модули FL MGuard RS2000 – это устройства базовой серии, предназначенные для простых задач маршрутизации и удаленного доступа с поддержкой до двух VPN-туннелей, что гарантирует высокий уровень безопасности. В случае необходимости может быть задействован встроенный межсетевой экран. При этом настройка устройства максимально упрощена и не требует специальных знаний в области информационных технологий.

Рис. 1. Новые межсетевые экраны от Phoenix Contact

Модули FL MGuard RS4000 в дополнение к функциям маршрутизации предлагают полный функционал межсетевого экрана и VPN. Гибко конфигурируемые фильтры межсетевого экрана гарантируют пропускание только авторизованного пользователем трафика. Для каждого устройства доступно до 10 VPN-туннелей. Имеется возможность расширения до 250 туннелей с помощью дополнительной лицензии.

Три основные причины эффективности использования систем удаленного сервиса

1. *Низкие затраты на гарантийное обслуживание.* В случае поставки системы конечному пользователю может потребоваться выполнение гарантийных обязательств по обслуживанию системы. В этом случае расходы, связанные с выявлением причины неисправности, и последующий ремонт ложатся на производителя. Командировочные расходы и время, необходимое для проведения работ, могут быть сокращены как минимум вдвое при использовании FL MGuard, так как такой подход ускоряет диагностику неисправностей и позволяет оперативно заказать запасные части. Если выявляются проблемы в программной части системы, то их решение может быть осуществлено удаленно. При этом сокращается общий простой оборудования заказчика.

2. *Сервисное обслуживание.* Современные производства насыщены сложным оборудованием. При этом невозможно держать штат специалистов под различные системы. Поэтому многие компании предпочитают сфокусироваться на основном виде своей деятельности, а сервисное обслуживание передать специализированным сервисным компаниям. Такой подход экономически эффективен, так как участие сервисных специалистов требуется только в момент ремонта или планового обслуживания. Но данный вид работы может привести к увеличению времени простоя в случае отказов из-за медленного реагирования сервисной компании. В этом

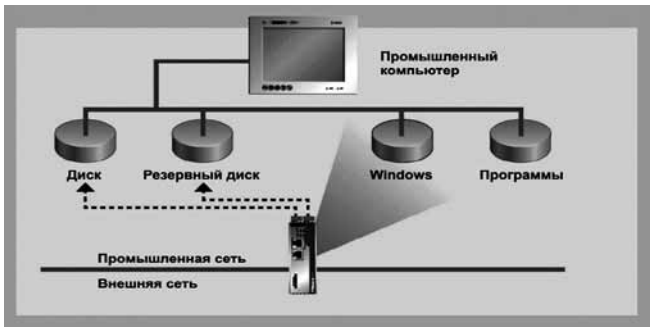

Рис. 2. Принцип работы CIM (CIFS Integrity Monitoring)

случае использование функции VPN-маршрутизаторов FL MGuarg для удаленного подключения через Internet может ускорить выявление неисправностей со стороны сервисной компании и, как следствие, решить проблему длительного простоя оборудования заказчика.

3. *Гарантийные соглашения*. В случае поставки сложного оборудования, требующего соблюдения определенных условий эксплуатации и периодического обслуживания, производитель оборудования может обговорить необходимость удаленного контроля за установкой и возможность проверки периодичности проводимых сервисных операций с помощью защищенного VPN-соединения.

Мониторинг целостности системы

Со времени появления вируса Stuxnet, созданного для атак на системы автоматизации, средства мониторинга целостности системы были значительно усовершенствованы. Была разработана антивирусная защита CIFS (Common Internet File System) Integrity Monitoring (CIM), предназначенная для промышленного применения и доступная в качестве дополнительной лицензии для устройств RS4000 серии FL MGuard. CIM работает как антивирусный сканер, не требуя перезагрузки антивирусных баз, определяет вредоносное ПО, которое поражает системы управления, системы операторского интерфейса и промышленные ПК под управлением ОС Windows (рис. 2).

Таким образом, при параллельной работе встроенного межсетевого экрана и антивирусного ПО достигается максимальная защита систем, ранее не доступная. Такая защита наиболее актуальна для:

• операционных систем, для которых более не предоставляются обновления безопасности, такие как Windows 2000 и др.;

• систем, установленных производителем, обновление или изменение ПО которых может привести к неработоспособности системы и потере гарантии. Например, обновление ОС Windows может вызвать несовместимость установленного ПО, которое было протестировано на более ранних версиях;

• систем реального времени промышленного применения, в которые не может быть установлена антивирусная защита без потери real-time совместимости;

• систем, в которых отсутствует возможность периодической загрузки обновленных антивирусных баз;

• систем, в которых ПО, установленное производителем, распознается антивирусными программами как вредоносное.

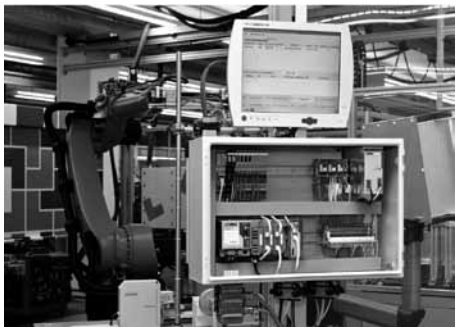

Рис. 3. Пример установки новых устройств FL MGuard

Высокая безопасность во всех сферах применения

Новое поколение промышленных межсетевых экранов безопасности привлекает внимание благодаря компактному металлическому корпусу для установки на DIN-рейку без системы активного охлаждения (рис. 3).

Эти устройства имеют слот для установки SD-карт, а также контакты для удаленного управления VPN-подключениями и контакты для отображения статуса этих подключений. Все соединения выполнены с помощью разъемов, что делает установку и замену устройства очень простой. Серия RS4000, основанная на ОС Embedded Linux, имеет четыре компонента, идеально сочетающихся друг с другом:

• двунаправленный межсетевой экран с анализом структуры;

• гибкий NAT-маршрутизатор;

• VPN-шлюз с максимальной безопасностью;

• опциональная антивирусная защита на основе технологии CIFS Integrity Monitoring.

Модули RS2000 разработаны как удаленные «полевые» устройства и могут быть установлены в качестве VPN-маршрутизатора непосредственно в удаленной или в локальной распределенной системе. Они поддерживают до двух VPN-подключений, имеют простой в настройке межсетевой экран, а также гибкие функции маршрутизации и безопасности.

Таким образом, новые RS2000 и RS4000 устройства серии FL MGuard созданы для обеспечения безопасных, надежных и доступных по цене систем удаленного контроля и сервиса. В сочетании с антивирусной защитой CIFS Integrity Monitoring (CIM), доступной для RS4000, пользователи могут управлять системой автоматизации с использованием VPN-подключений и защититься от атак вредоносного ПО (рис. 3).

Хильгенкамп Инго *– специалист по сетевым технологиям в маркетинге, Phoenix Contact Electronics GmbH,*
Линеенко Михаил Борисович *– канд. техн. наук, инженер по продажам,*
Зозуля Денис Сергеевич *– менеджер по продукции AUTOMATION Systems ООО “Феникс Контакт РУС”.*
Контактный телефон (495) 933-85-48, факс 931-97-22.
E-mail: info@phoenixcontact.ru Http://www.phoenixcontact.ru