

Гюнтер Думски (Günter Dumsky), Kontron

Высоконадёжный встраиваемый сервер для безопасного дистанционного обслуживания

Для обеспечения безопасного дистанционного обслуживания и диагностики технологического оборудования и систем по сети Интернет компания Innominate разработала высоконадёжный 19-дюймовый блок сетевой защиты, который может использоваться в центрах технического обслуживания в качестве брандмауэра верхнего уровня и шлюза виртуальных частных сетей (VPN). Эта система применяется для создания VPN-сетей и поддержания защищённых сетевых соединений с удалёнными промышленными устройствами. Поскольку число одновременно поддерживаемых соединений может достигать 1000 и более, к работоспособности этого узла предъявляются весьма высокие требования. Именно по этой причине в качестве аппаратной платформы был выбран сервер KISS компании Kontron, коэффициент готовности которого соответствует требованиям, обычно предъявляемым к телекоммуникационным платформам операторского класса, но по стандартным для отрасли встраиваемых систем ценам.

Для удобства работы операторов станков и производственного оборудования в них всё чаще и чаще предусматриваются функции дистанционного мониторинга и обслуживания. Взаимодействие операторов на местах и специалистов в удалённых центрах технического обслуживания по сетевым каналам связи устраняет необходимость в дорогостоящих командировках технических экспертов и значительно сокращает простой оборудования. А благодаря тому, что в современные станки обычно встраиваются широкополосные Ethernet-порты, возникают перспективы новых возможностей обслуживания и повышения конкурентоспособности. Это касается, например, использования таких интернет-технологий, как VoIP (Voice over IP, передача речи по IP-каналам) и потоковая передача изображений и видеoinформации.

Вместе с тем, чтобы в полной мере вкушать все радости пребывания в прекрасном новом мире Интернета

Модемы уже устарели

С середины 90-х годов прошлого столетия и до недавнего времени дистанционное обслуживание практически повсеместно осуществлялось с использованием аналоговых телефонных модемов или терминальных ISDN-адаптеров. Наряду с высокой стоимостью телефонной инфраструктуры, дополнительными расходами на установление и поддержание соединений и низкой пропускной способностью, подобные решения характеризуются тем, что каждое такое соединение потенциально играет роль «чёрного входа» (backdoor) в вычислительную сеть предприятия. По этой причине в последнее время набирает силу тенденция использовать для обеспечения дистанционных услуг современные широкополосные интернет-соединения на основе виртуальных частных сетей и соответствующих брандмауэров.

Поскольку большинство современных систем и оборудования уже имеют Ethernet-интерфейсы и входят в состав корпоративных сетей, естественным образом напрашивается выполнять их дистанционное обслуживание по Ethernet-каналам и протоколам TCP/IP. Дистанционное обслуживание промышленного оборудования и систем по интернет-каналам обладает рядом достоинств. Во-первых, отпадает необходимость в прокладке дополнительных телефонных линий к каждой контролируемой единице оборудования и установке дополнительных модемов. Во-вторых, сокращаются расходы на оплату международной связи, при этом пропускная способность каналов обмена данными существенно возрастает. В-третьих, применение таких современных интернет-технологий, как VoIP (Voice over IP, передача речи по IP-каналам) и потоковая передача изображений и видеосигналов, открывает возможность создания новых видов обслуживания и, тем самым, повышения конкурентоспособности соответствующего оборудования.

и использовать интернет-возможности оборудования, необходимо начать с мер предосторожности, чтобы никто из посторонних не смог непосредственно из Интернета получить доступ к вашему станку и не натворить бед. Производители и операторы производственных систем ищут экономически оправданные методы обеспечить защищённый удалённый доступ по каналам TCP/IP к системам, к каждой единице оборудования, к объединённым в сети станкам. Эти методы должны гарантировать аутентификацию пользователя, конфиденциальность и целостность передаваемой информации с помощью различных средств шифрования, а также предотвращение передачи через брандмауэр незатребованного трафика. В идеале подобные средства хотелось бы встраивать в существующие сети максимально легко.

Универсальная система защиты для корпоративных сетей

Компания *Innominate*, которая специализируется на разработке оборудования сетевой защиты, разработала требуемое техническое решение на базе своего портфолио продуктов mGuard. Одна из новинок этого комплексного решения, созданного на базе испытанных стандартных технологий, заключается в реализации нового, «инверсного», подхода к дистанционному обслуживанию. До настоящего времени соединение с требующей обслуживания системой должна была устанавливать техническая служба. Концепция дистанционного обслуживания на базе mGuard предусматривает, что инициатором такого соединения должна выступать обслуживаемая система. То есть соединение со станком теперь устанавливается не по внешней инициативе,

а по инициативе самого станка с предварительно определённым удалённым пунктом обслуживания. Подобный подход позволяет решить многие проблемы, связанные с обеспечением защиты и использованием брандмауэров, поскольку исходящие соединения с явно определёнными партнёрами в VPN-сети гораздо проще организовывать и контролировать. Концепция mGuard, специально разработанная для производственных систем, построена на принципах использования так называемых брандмауэров экспертного уровня (stateful inspection firewall), осуществляющих мониторинг входящих и исходящих пакетов в соответствии с предопределёнными наборами правил, и обеспечения безопасной и конфиденциальной передачи информации по шифрующим соединениям виртуальных частных сетей.

Для каждого случая своё решение

Для защиты производственных сетей, производственных подразделений и отдельных автоматизированных устройств, компания *Innominate* предлагает развитый ассортимент устройств сетевой защиты mGuard, которые без особых усилий интегрируются в существующие на предприятиях Ethernet-сети. Компоненты mGuard, предназначенные для установки на производственных участках, уже допускают интеграцию с децентрализованными системами типа DIN-модулей и PCI-плат. Кроме того, в портфолио входит blade-блок mGuard – очень интересное решение для установки в 19-дюймовую стойку, удовлетворяющее повышенным требованиям к готовности. Это устройство с резервными источниками питания и поддержкой «горячей» замены blade-модулей обеспечивает организацию до 12 защищённых сетевых систем,

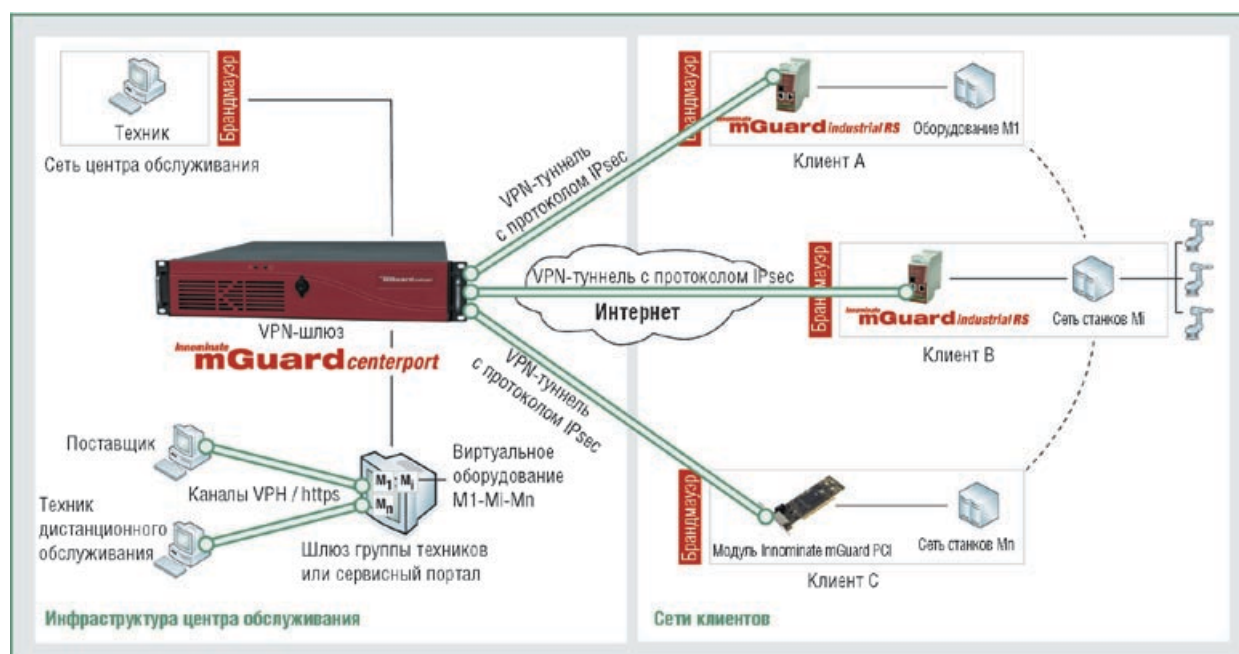


Рис. 1. Инфраструктура эффективного обслуживания. Построенный на основе промышленного сервера Kontron KISS 2U, шлюз mGuard Centerport играет роль центрального шлюза для полевого оборудования mGuard, имеющего специфические требования к построению VPN-сетей и обеспечивающего защищённые VPN-каналы с различными распределёнными промышленными системами.

или подсетей, с увеличением числа VPN-туннелей с 250 до 3000 и может быть использовано в качестве VPN-шлюза.

В дополнение к графическому веб-интерфейсу пользователя (WebGUI) для локального администрирования все устройства имеют встроенные средства, которые позволяют централизованно управлять системой с помощью менеджера устройств Innominate Device Manager (IDM). Менеджер IDM обеспечивает максимально эффективное конфигурирование и мониторинг устройств mGuard, благодаря «шаблонным» процедурам. После того, как эти устройства установлены в нужной производственной точке, они могут создавать как временные («по требованию»), так и постоянные VPN-соединения со службами поставщика услуг дистанционного обслуживания. Как правило, эта операция выполняется оператором станка или оборудования, который может воспользоваться услугами дистанционного обслуживания и проконтролировать состояние соединения в любой момент. Организация VPN-соединения, естественно, требует наличия удалённой станции в центре техобслуживания. Именно для таких удалённых станций компания Innominate и спроектировала совершенно новую систему, применение которой позволяет значительно повысить эффективность конфигурирования большого количества подключённых к центру полевых устройств (рис. 1).

Новый брандмауэр и VPN-шлюз для семейства mGuard

Центральное место в семействе Innominate mGuard для систем 19-дюймового формата занимает устройство mGuard Centerport, выполняющее функции брандмауэра верхнего уровня и VPN-шлюза, необходимых для защиты соединений в приложениях с очень большим числом подключённых полевых устройств. Его главное достоинство заключается в том, что все VPN-соединения имеют

один и тот же IP-адрес. В предшествующем устройстве mGuard bladePack для этого требовалось 12 IP-адресов, по одному адресу на слот. Теперь же необходимости в распределении нагрузки между разными адресами нет, используется всего один публичный IP-адрес, что существенно облегчает задачу конфигурирования и администрирования сети. Кроме того, вместо портов Fast Ethernet (с пропускной способностью 100 Мбит/с) используются порты Gigabit Ethernet (1000 Мбит/с), благодаря чему устройство mGuard Centerport может поддерживать в рабочем состоянии одновременно до 1000 VPN-туннелей с общей производительностью шифрования данных в 300 Мбит/с (в четыре раза выше производительности mGuard bladePack). Шлюз mGuard Centerport полностью совместим со всеми полевыми устройствами mGuard и менеджером IDM, вследствие чего задача его интеграции в рабочую систему значительно упрощается. На аппаратном уровне всё, что нужно сделать, – это подключить к устройству сеть центра обслуживания (к порту локальной сети на тыльной стороне) и канал доступа к сети Интернет (к порту глобальной сети) (рис.2). После включения питания (источники питания дублируются) и начальной настройки при помощи веб-интерфейса управление шлюзом может быть осуществлено с помощью менеджера IDM. Благодаря высокой производительности шлюза реконфигурация 1000 VPN-каналов после перезагрузки системы (по каким-либо причинам) выполняется менее чем за 5 минут, что соответствует высочайшему коэффициенту готовности для приложений дистанционного обслуживания.

Цель – «шесть девяток»

К новым системам для 19-дюймовой стойки, которые являются одним из узлов корпоративной сети центра техобслуживания и обеспечивают доступ к подключённым устройствам и приложениям, предъявляются весьма

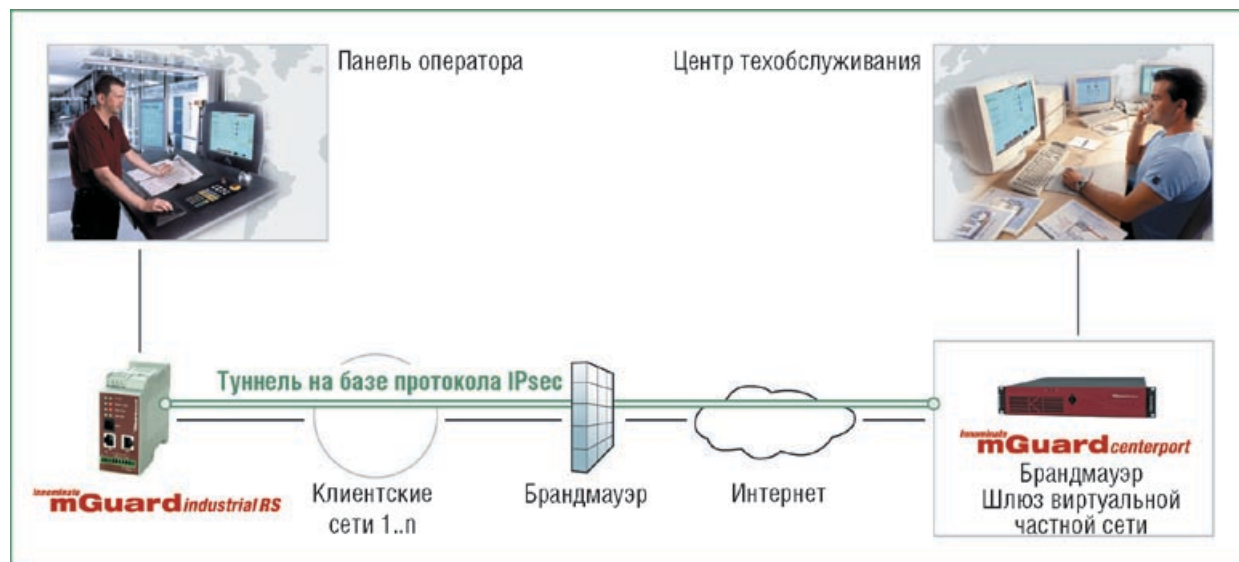


Рис. 2. Схема подключения с возможностью масштабирования. Применение шлюза Innominate mGuard Centerport позволяет центрам обслуживания и приложениям мониторинга подключаться посредством зашифрованных VPN-каналов к 1000 глобально распределённым системам.

высокие требования. Система должна обладать высокой вычислительной мощностью, достаточной для эффективного управления 1000 VPN-каналов без больших задержек. Кроме того, высокопроизводительные системы должны характеризоваться значительной наработкой на отказ (интервал сохранения работоспособности между отказами), поскольку к такому серверу предъявляются требования, сравнимые с требованиями к телекоммуникационным сетям операторского класса. Хотя подобные системы могут и не иметь резервных модулей и не поддерживать «горячую» замену, в их проектах должны быть реализованы решения, обеспечивающие максимально возможный коэффициент готовности. Например, для уменьшения времени простоев и повышения степени отказоустойчивости можно предусмотреть резервирование источников питания или организацию дисковых накопителей в виде RAID-массива. «В идеале коэффициент готовности таких систем должен быть равен 99,9999 %, или по-другому “шести девяток”, – говорит Торстен Россел (Torsten Roessel), директор *Innominate* по развитию бизнеса. – Мы затратили немало времени в поисках нужного решения».

Системные компоненты и оборудование из одного источника

Внимание проектировщиков *Innominate* привлекли серверы *Kontron* семейства KISS (*Kontron Industrial Silent Server* – малозумный промышленный сервер компании *Kontron*), которые широко используются в составе систем управления электростанциями, в железнодорожных и медицинских приложениях и даже на атомных станциях, что свидетельствует о его высокой надёжности. Благодаря поддержке технологии Intel® AMT, они могут оснащаться средствами внутриканального (in-band) и внешнеканального (out-of-band) мониторинга, что обеспечивает выполнение практически всех требований, предъявляемых к телекоммуникационным системам операторского класса (за исключением требования поддержки «горячей» замены модулей). С точки зрения *Innominate*, серверы KISS 2U 19-дюймового формата, имеющие резервные источники питания, порты Gigabit Ethernet, процессоры Intel® Core™ 2 Quad, в настоящее время одни из самых компактных и быстродействующих серверов с высоким коэффициентом готовности, пригодных для применения в системах с повышенными требованиями к непрерывности работы и устойчивости к высоким нагрузкам.

По словам Торстена Россела, причин выбора аппаратной платформы компании *Kontron* было несколько: «Мы очень хорошо знаем эту компанию-производителя надёжных промышленных ПК, которая является одним из поставщиков нашей родительской компании *Phoenix Contact*. На наше решение повлияло также наличие подходящей номенклатуры устройств с возможностью масштабирования как вверх, так и вниз, возможность проектирования системы как OEM-

изделия с собственной торговой маркой, политика долгосрочных поставок указанных аппаратных конфигураций, высокое качество продукции компании и локальная поддержка этого немецкого производителя». Для стандартной конфигурации шлюза *Innominate Centerport* сервер KISS 2U был модифицирован компанией *Kontron* путём изменения клиентской части (front-end), использования компактного модуля слотов PICMG 1.3, высокопроизводительной объединительной панели и реализации 4-х портов Gigabit Ethernet. Кроме стандартной конфигурации, возможно построение заказных версий с изменённым набором аппаратных компонентов. Получение системы и всех её компонентов из единого источника – от компании *Kontron* – гарантирует наивысшую степень их совместимости и надёжности. Средняя наработка на отказ (MTBF) составляет порядка 50000 часов, или около 5,7 лет непрерывной работы. Кроме того компания *Kontron* гарантирует наличие серверов KISS 2U в течение не менее 5 лет. Это позволяет создавать однородные аппаратные структуры, обеспечивающие эффективное оказание услуг и высокую степень защиты инвестиций в заказные клиентские платформы.

OEM-производство устройств обеспечения защиты

Средства обеспечения защиты сетей на основе представленных устройств семейства *Innominate mGuard* и серверов *Kontron KISS*, ориентированные на требования конкретных пользователей, могут быть реализованы в виде дополнительных OEM-вариантов. Заинтересовались? Обращайтесь к нам!

Сервер Kontron KISS 2U: высокая степень конфигурируемости

Промышленный сервер *Kontron KISS 2U* был выбран компанией *Innominate* в качестве специализированной OEM-платформы с высоким коэффициентом готовности для построения брандмауэров верхнего уровня и шлюзов VPN-сетей. Стандартные серверы *Kontron KISS 2U* отдельно оснащаются модулями слотов PICMG 1.3 и PICMG 1.0 либо материнскими платами формата Flex-ATX, что обеспечивает широкие возможности дополнительного расширения системы. Компактные модули PICMG 1.x могут иметь до пяти слотов расширения. В стандартной конфигурации с материнской платой Flex-ATX возможно наличие до 2 плат расширения PCI.

