



# МЕТОДЫ ЗАЩИТЫ ОТКРЫТЫХ ПРОМЫШЛЕННЫХ СЕТЕЙ ETHERNET

ТИМ ПИТТЕРЛИНГ (TIM PITTERLING)  
ДЖОНАС ЛДЖАНБЕРГ (JONAS LJUNGBERG)

Удаленный доступ к сети — полезная функция, однако она несет потенциальный риск несанкционированного входа в сеть. В статье рассмотрены способы обеспечения защиты данных.

Применение Ethernet на производстве обеспечивает множество преимуществ, наиболее значимым из которых является открытость архитектуры, то есть наличие доступа к промышленным устройствам и инструментам управления практически из любой точки как на территории предприятия, так и за его пределами. В то же время эта открытость несет в себе угрозу потери безопасности.

По сути, если автоматизированная система подключена к сети, она подключена к Интернету, поскольку с очень высокой степенью вероятности где-то на предприятии найдется узел, имеющий выход в Интернет. Соответственно, система становится подвержена типичным киберугрозам, в частности атакам хакеров и проникновению вредоносных программ («троянов», «червей» и пр.), поэтому должны быть предприняты меры защиты, аналогичные тем, что используются при подключении к глобальной Сети.

Инструменты защиты офисной и промышленной сетей, по сути, одинаковы, хотя последние учитывают особенности работы в промышленной среде. Они должны обеспечивать авторизованный доступ к среде предприятия из любой точки производственного комплекса и вне его. Сетевой администратор получает возможность удаленно выполнять такие задачи, как конфигурирование и диагностика сети, инициализация узлов.

В набор инструментов входят аппаратные и программные средства, практические наработки, такие как межсетевые экраны (firewall), виртуальные приватные сети (VPN), средства пре-

образования сетевых адресов (NAT) и соответствующие политики.

Итак, при осуществлении удаленного управления или обмена данными с внешними сетями необходимо обеспечить защиту от типичных для глобальных сетей угроз. Ниже рассмотрены некоторые инструменты, используемые для выполнения данной задачи.

## **FIREWALL — ПЕРВАЯ ЛИНИЯ ЗАЩИТЫ**

Межсетевой экран, хотя и является одним из наиболее старых инструментов защиты, не теряет позиции до сих пор. Как следует из названия, он контролирует потоки данных между сетями. Его задача заключается в подтверждении прохождения данных.

Если межсетевой экран предназначен для защиты ячейки, объединяющей несколько подключенных к Ethernet автоматических устройств, таких как промышленные ПК или программируемые логические контроллеры (ПЛК), рекомендуется устанавливать модуль безопасности. Он представляет собой простое устройство, один вход которого подключен к внутренней сети предприятия, а второй — ко внешней глобальной сети. Данные, проходящие между сетями, проходят через межсетевой экран в соответствии с правилами, прописанными в нем для каждого узла.

Существует несколько режимов работы межсетевого экрана. В промышленных сетях, как правило, используется проверка с учетом состояния, которая предоставляет устройству доступ только к контекстным данным. Экран

пропускает только те данные, которые были высланы в ответ на зафиксированный внутри сети запрос. Если внешний источник пытается отправить данные, которые не были запрошены, передача блокируется.

Для подтверждения потока данных используются предустановленные правила фильтрации. Например, если внутренний узел высылает данные внешнему устройству, межсетевой экран разрешит принять ответный пакет только в течение ограниченного промежутка времени. Когда отведенное временное окно закончится, доступ будет снова заблокирован.

## **NAT И NAPT**

Следующей технологией, обеспечивающей безопасность автоматизированной среды, является NAT. Она реализована на уровне узлов. NAT скрывает IP-адреса внутренних узлов от публичных устройств, имеющих доступ к внешним сетям. Публичным узлам видны только публичные IP-адреса, отличающиеся от адресов, используемых внутри сети.

В методике преобразования адресов и портов (NAPT) делается на один шаг больше: помимо IP-адреса, ставится в соответствие номер порта. Публичным узлам сообщается только один IP-адрес, а устройство назначения определяется по номеру порта.

Таблица NAPT, как правило, хранится в памяти маршрутизатора. По ней происходит преобразование внутренних IP-адресов портов в публичные. Если устройство из внешней сети попытается переслать пакет во внутренний узел сети, оно использует публичный адрес

устройства и номер порта в качестве адреса назначения. IP-адрес преобразуется во внутренний по таблице портов, хранящейся в маршрутизаторе.

Адрес источника в заголовке пакета данных остается без изменений. Однако, поскольку адрес отправителя не принадлежит той же подсети, что адрес получателя, ответный пакет проходит через маршрутизатор. Он передает его во внешнюю сеть, защищая реальный IP-адрес внутреннего устройства от публичных узлов.

### ВИРТУАЛЬНЫЕ КАНАЛЫ БЕЗОПАСНОСТИ

Рассмотрим еще один способ обеспечения безопасного соединения через незащищенную сеть — использование виртуальных частных сетей (VPN). VPN представляет собой канал передачи, защищенный цифровым сертификатом. По аналогии с цифровыми идентификационными номерами (ID), по сертификату устройства распознают друг друга и определяют метод шифрации, используемый для передачи пакета через Интернет. Данные расшифровываются на приемном конце канала и передаются конечному узлу. Модули безопасности на основе цифровых сертификатов могут создавать частные сети двух конфигураций: на основе мостов и на основе маршрутизаторов.

Мостовая конфигурация используется для обеспечения безопасной передачи данных между территориально разнесенными устройствами либо узлами, связь между которыми не может быть обеспечена в рамках сети предприятия и осуществляется с использованием незащищенных участков сети. Данная конфигурация используется также в тех случаях, когда связь не может быть обеспечена маршрутизатором либо ограничена пределами одной подсети.

Режим маршрутизации используется для создания виртуальной частной сети между устройствами, принадлежащими разным подсетям. Маршрутизатор работает на третьем уровне модели OSI. Он оснащен интеллектуальными функциями, осуществляющими сбор информации о доступных внешних сетях, которые можно использовать для передачи пакетов по адресу назначения. В этом случае, как и в предыдущем, пакет проходит по защищенному тоннелю в зашифрованном виде, что гарантирует защиту данных даже в публичной сети.

### ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ

Инструменты защиты, доступные в производственной среде, можно сочетать различными способами в зависимости от требуемого типа доступа и расположения устройства-получателя. Рассмотрим несколько примеров.

#### Пользовательский межсетевой экран

Допустим, что на предприятии работает подрядчик, использующий часть производственного оборудования. Когда его нет на рабочем месте, он должен иметь возможность удаленного подключения для устранения неисправностей. В этом случае следует создать пользовательское правило, обеспечивающее доступ к сети только для этого пользователя. Можно также назначать разные уровни авторизации, чтобы удаленные пользователи получали доступ только к тем устройствам, для которых они авторизованы.

Наиболее простой процедурой аутентификации удаленного пользователя является проверка имени пользователя и пароля. Пользователь входит в свой профиль или учетную запись через IP-адрес модуля. По умолчанию ему открывается доступ на предустановленный промежуток времени, по истечении которого производится автоматический выход. Это сделано для обеспечения защиты в том случае, если пользователь покидает рабочее место на длительное время и не разрывает соединение. Если для работы требуется больше времени, пользователь должен обновить соединение до того, как оно разорвется, используя соответствующую веб-форму.

#### Межобъектный VPN-канал

В случае, когда на предприятии имеется один центральный объект или, например, количество объектов мало, целесообразно использовать объектные виртуальные каналы, обеспечивающие защищенное шифрованное соединение между двумя объектами. В зависимости от параметров конфигурации обеспечиваются различные типы доступа, например пользователь, расположенный на одном объекте, может обмениваться данными с абонентами или узлами сети, расположенной на другом объекте. Требуется только пройти авторизацию.

При таком подходе все объекты должны быть оснащены модулями связи, между которыми устанавливается

защищенный виртуальный коридор. Допустимо применение меж сетевого экрана для тонкого управления доступом и ограничения доступа к ресурсам объекта.

#### Точечные VPN-каналы

Виртуальная частная сеть «точка-точка» открывает пользователю доступ к устройствам на любом производственном объекте с любого другого производственного объекта, имеющего выход в Интернет. Эту конфигурацию удобно использовать сетевому администратору для удаленного подключения к сети предприятия и устранения неполадок во внеурочное время.

Для реализации данного подхода на каждом объекте должен быть модуль связи, подключенный к сети предприятия, и соответствующее клиентское программное обеспечение (ПО), установленное на компьютере или ноутбуке администратора. ПО выстраивает защищенный виртуальный канал до любого объекта, оснащенного модулем связи. Возможность доступа к тому или иному устройству на объекте определяется политикой разрешений.

#### Многоточечные VPN-каналы

Теперь рассмотрим ситуацию, когда сетевой администратор удаленно обслуживает несколько объектов. Вместо установления отдельных VPN-каналов с каждым из них он может создать одно соединение с центральным модулем, который в свою очередь уже имеет VPN-связи с каждым объектом. Это избавляет сетевого администратора от необходимости проводить много времени в пути от одного объекта к другому, обеспечивая тот же уровень безопасности, что и в случае межобъектных или точечных VPN-связей.

\* \* \*

Мы рассмотрели несколько инструментов, обеспечивающих уровень защиты данных в сети Ethernet предприятия, не уступающий уровню защиты FieldBus или офисных сетей. Хотя межсетевой экран и виртуальные частные сети являются важными средствами обеспечения защиты данных при удаленном доступе, действительно всесторонне защищенная модель подразумевает использование дополнительных мер защиты. Необходимо помнить, что безопасность должна быть во всем. Это не просто проверка пароля, это стиль жизни. ●