EagleOne – первый защитник сетевого периметра

С.С. Воробьев (Компания ПРОСОФТ)

Рассмотрен вариант организации защищенной сети Industrial Ethernet на базе промышленного брандмауэра EagleOne от Hirschmann, описана основная функциональность и приведены практические рекомендации по его применению.

Ключевые слова: защищенная сеть, Industrial Ethernet, промышленный брандмауэр, многоуровневая защита, безопасность, киберугрозы.

Введение

За последнее время подходы к организации безопасности сети промышленного объекта пережили существенные изменения. Инциденты с вирусами Stuxnet, Duqu, Flame, которые атаковали множество промышленных объектов по всему миру, подтолкнули к комплексному пересмотру политики безопасности сетей АСУТП промышленных объектов [1, 2]. При этом атаке были подвержены оконечные устройства на полевом уровне, примером могут служить обогатительные центрифуги на одном из заводов в Иране, который стал жертвой вируса Stuxnet. После подобных случаев на многих промышленных предприятиях была пересмотрена политика безопасности в части антивирусной защиты, часть решений была взята из ИТ-среды и заключалась в установке дополнительной антивирусной защиты. Это позволило повысить общий уровень локальной защиты. Но тенденции последних лет показывают, что подход, который справедлив для ИТ-среды, в основе которой находится конфиденциальность, а не целостность информации, становится не всегда приемлемым для сети промышленного объекта. И на сегодняшний день необходимо более серьезное решение в реализации защиты АСУТП.

Зачем необходима специализированная защита сети Industrial Ethernet?

Переход промышленных объектов на сеть Industrial Ethernet (промышленный Ethernet) фактически является свершившимся фактом. Использование единой среды для передачи данных позволяет существенно увеличить гибкость сети всего промышленного объекта и позволяет организовать доступ к технологическим и информационным данным извне. На сегодняшний день сеть, построенная по принципу Industrial Ethernet, дает возможность с легкостью провести интеграцию между технологическими и корпоративными сетями, что позволяет организовать управление и взаимодействие на качественно новом уровне. Для примера приведем удаленные соединения, которые могут быть использованы для создания непосредственной связи и обмена информацией между головным офисом компании и производством, которые могут быть расположены даже на разных континентах. Подобные возможности увеличивают гибкость управления, но также уменьшают устойчивость всей сети к внешним угрозам. При этом для промышленных объектов решение должно быть очень надежным. Ведь слабый контроль доступа к критически важным системам контроля технологических процессов может иметь просто катастрофические последствия. И решения, которые справедливы для ИТ-среды, из которой пришел стандарт Ethernet, просто не смогут обеспечить должный уровень безопасности. Между типовыми сценариями администрирования защиты ИТ-среды и промышленной инфраструктуры есть ряд отличий. В первую очередь это заключается в используемых технологиях, промышленная сеть АСУТП достаточно сложна, она реализуется как распределенная по функциям система, взаимодействующая посредством локальной сети. При этом зачастую применяются узкоспециализированные технологии и компоненты, такие как серверы SCADA, АРМ, ПЛК. Часто используется возможность удаленного доступа к ранее полностью закрытым объектам, например, сеть АЭС с использованием общедоступных линий связи [3]. Подобная линия связи, ее протяженность и независимость от государственных и большинства естественных границ приводит к потенциальной уязвимости промышленной сети объекта и возможности получения несанкционированного доступа на значительном удалении.

К такой сети и должна быть адаптирована система безопасности. При этом долгий (иногда до 50 лет) жизненный цикл оборудования АСУТП, использование уникальных промышленных протоколов, непрерывный цикл производства на многих предприятиях, в том числе критически важных, часто конфликтуют с решениями в области информационной безопасности, разработанными на самых современных платформах, требующими модернизации, по крайней мере, части оборудования и регулярного обновления ПО. При организации защиты промышленной сети Industrial Ethernet необходимо иметь многоуровневый инструментарий, который позволит организовать не только защитный контур для объектов со своей спецификой, но и внутренний анализ процессов на уровне промышленных протоколов.

Брандмауэр, файрвол, межсетевой экран...

Наиболее популярным инструментом, который предлагается для обеспечения безопасности любой Ethernet сети, в том числе и промышленной, является брандмауэр (Brandmauer), он же файрвол (Firewall) или же межсетевой экран. Как правило, это решение, которое осуществляет контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. В существующих реалиях

это незаменимый инструмент сетевой безопасности. Другими словами, это своего рода комплекс, который предоставляет возможность защитить не только саму сеть, но и оконечных пользователей, входящих в нее, таких как ПЛК, промышленные ПК, системы управления, камеры и т. п., от несанкционированного доступа, фильтруя входящий и исходящий сетевой трафик. Как правило, подобный комплекс становится первой и обязательной линией защиты промышленной сети.

С учетом развития Ethernet сетей подобные решения можно разделить на два типа. К первому типу условно отнесем брандмауэры и файрволы, которые представляют собой только программные решения и устанавливаются на оконечных устройствах, обеспечивая их непосредственную защиту. Самый простой пример — это встроенный брандмауэр («защитник») ОС Windows. Ко второму типу отнесем более сложные и комплексные механизмы, которые являются программно-аппаратным решением. Их условно можно назвать сетевыми брандмауэрами либо межсетевыми экранами. Основное отличие от первого типа заключается в том, что они устанавливаются в разрыв сети, например, на ее границе либо между подсетями. Весь трафик при этом проходит непосредственно через отдельное устройство, подвергаясь глубокому анализу. Именно устройства второго типа обычно встречаются в промышленных Ethernet сетях. Это связано с тем, что промышленная сеть АСУТП, как правило, разделена на отдельные сегменты, которые осуществляют тот либо иной производственный/технологический процесс. Да и с учетом специфики подобной сети намного проще и быстрее устанавливать правила именно на границе сети, производя анализ трафика для всего сегмента в целом.

В настоящее время в большинстве случаев, если упомянуто устройство типа промышленный брандмауэр/файрвол или межсетевой экран, то имеется в виду отдельный программно-аппаратный комплекс, который устанавливается на границе сети и осуществляет анализ каждого полученного пакета на соответствие установленным правилам и в дальнейшем принимает решение пропустить или отбросить полученные данные. Настроив правила входящего и исходящего трафика для промышленного брандмауэра, можно существенно повысить степень защищенности сети. Например, если в сегменте сети одновременно находятся ПЛК, промышленные ПК и сервер сбора данных, то можно создать ряд правил для промышленного брандмауэра, которые позволят получить доступ к серверу сбора данных ограниченного круга лиц и запретить доступ из внешней сети к ПЛК и промышленным ПК. В итоге, используя подобные правила, можно реализовать контур защиты, который позволит обезопасить промышленную сеть от возможного несанкционированного доступа. Но если исходить из общемировых тенденций и правил, то, как правило, на промышленных объектах применяется принцип «глубокой» защиты или защиты в глубину (Defense in Depth), которая также упомянута в стандарте МЭК62443. Согласно Defense in Depth установка промышленного брандмауэра на границе сети — это лишь первый защитный контур.

Принцип Defense in Depth

Данный принцип достаточно известен, особенно при построении многоуровневой защиты сети передачи данных промышленного объекта. В его основе находится так называемая концепция «зон и каналов» (Zones and Conduits). Принцип «глубокой» защиты заключается в том, что многоуровневые механизмы безопасности повышают безопасность системы в целом. Если атака приводит к сбою одного инструмента, обеспечивающего безопасность сети, другие могут по-прежнему обеспечивать необходимую защиту для системы. Рассмотрим небольшой пример. Возьмем систему контроля и сбора параметров АСУТП. Как правило, для получения доступа к подобной системе необходимо пройти аутентификацию путем ввода связки логин-пароль. Зачастую, стараясь повысить уровень безопасности, администраторы сети увеличивают требуемую длину пароля вплоть до 15 сим-

а)

б)

Рис. 1. Варианты применения промышленных брандмауэров: а) брандмауэр установлен между промышленной сетью и общедоступной; б) брандмауэр установлен в сети производственного сегмента

волов. Данный факт увеличит устойчивость системы к атакам при помощи перебора типа Brute Force, но при этом работники будут записывать свои пароли для аутентификации, что приведет к возможности их кражи третьими лицами. Добавление дополнительного уровня в процесс аутентификации и разбиение его на два этапа позволит избежать обозначенной выше проблемы. Например, идентификация при помощи смарт-карты + ввод простого пароля позволит повысить общий уровень безопасности доступа к подобной системе. Принцип «глубокой» защиты как раз и заключается в том, что многоуровневые механизмы безопасности повышают безопасность системы в целом. Если атака злоумышленника приводит к сбою одного механизма безопасности, другие механизмы могут по-прежнему обеспечивать необходимую защиту для безопасности сети.

Defense in Depth можно также сравнить с организацией защиты древнего замка: защитные рвы, стены, башни и т.д. При этом отдельные зоны замка отделены друг от друга контролируемыми и управляемыми препятствиями: ворота, разводные мосты. Они призваны задержать нападавших и затруднить их передвижения. Аналогично рекомендуется выстраивать и одноименный принцип защиты для сетей Industrial Ethernet, исходя из которого необходимо реализовать несколько уровней защиты при помощи промышленных брандмауэров/файрволов, установленных как на границе сети, так и внутри ядра сети, что в итоге позволит обеспечить более тщательную проверку и фильтрацию проходящего трафика.

Промышленные брандмауэры на границах сети (IP-брандмауэры)

Промышленные брандмауэры выполняют достаточно широкий спектр задач, в основе которых находится разделение и сегментировании сети предприятия на отдельные части с последующей фильтрацией трафика. Согласно принципу Defense in Depth, это позволяет создать защиту как от угроз извне, так и отделить производственный сегмент от корпоративного. При этом, если промышленный брандмауэр обладает возможностью работы на уровне L3 (согласно модели OSI), осуществляя при этом маршрутизацию, то становится возможным подключить удаленный производственный сегмент к общей корпоративной сети, например, посредством сотовой 3G/4G сети, анализируя при этом весь проходящий через себя трафик. Подобный класс устройств называется IP-брандмауэрами, поскольку он представляет собой управляемую границу между, например, сетью предприятия и внешней сетью — сетью провайдера или Internet (рис. 1а). Поскольку данные устройства часто устанавливаются близко к производственному объекту, необходимо также учитывать эксплуатационные характеристики, такие как диапазон рабочих температур, степень защищенности, возможность работы при повышенных вибрациях и т.д.

Промышленные брандмауэры на «полевом» уровне (прозрачные брандмауэры)

Сеть Industrial Ethernet становится единой средой передачи данных на промышленных объектах. При этом угрозы, связанные с безопасностью промышленной сети, могут возникать как из внешней сети, так и исходить из внутренней. И если от внешних угроз может защитить правильно настроенный промышленный IP-брандмауэр, а согласно Defense in Depth это лишь первый защитный контур, то внутренние угрозы могут исходить из собственной сети. Поводом может служить, например, не только вирусная активность, но и некорректная работа собственного внутреннего программного обеспечения. Если рассматривать промышленную сеть, то множество устройств работают на уровне L2 и, например, неконтролируемый broadcast может заполонить всю сеть, при этом IP брандмауэр, который функционирует на уровне L3 и работает исключительно с IP адресами, будет работать в штатном режиме, от него не поступит сигнала о наличии некорректно работающих устройств. Для решения данной проблемы в дополнение к IP-брандмауэру необходимо добавить так называемый «прозрачный» брандмауэр (рис. 1 б). Данное устройство функционирует исключительно на уровне L2 модели OSI и становится следующим защитным звеном. Подобное устройство устанавливается в разрыв внутренней сети и анализирует трафик на уровне фреймов. При этом брандмауэр уровня L2 прозрачен для верхних уровней протокола.

Орлиная защита от Hirschmann

Hirschmann – это компания с более чем 90-летней историей, которая является локомотивом на рынке устройств Industrial Ethernet. В настоящий момент Hirschmann входит в состав концерна Belden, продолжая успешно развивать направление, связанное с коммуникационным оборудованием. В настоящий момент в линейке Hirschmann представлено множество решений, таких как коммутаторы, Wi-Fi точки доступа, решения для встраиваемых систем и т.д. Для многих инженеров Hirschmann ассоциируется с управля-

Рис. 2. Решения для обеспечения безопасности промышленной сети от Hirschmann

емыми и функциональными коммутаторами, на основе которых можно сформировать качественную сеть Industrial Ethernet. Однако это далеко не все, для защиты сети у Hirschmann присутствует линейка промышленных брандмауэров Eagle [4] (в переводе — орел), которые обладают достаточно богатой функциональностью и способны анализировать трафик как на уровне L3, осуществляя при этом маршрутизацию, так и на уровне L2 модели OSI (рис. 2).

Рис. 3. Внешний вид брандмауэра EagleOne от Hirschmann

Таблица. 1 Характеристики промышленных брандмауэров серии Eagle от Hirschmann

Наименование	EagleOne	Eagle 20/30
Место применения	Граница сети/ внутренняя сеть/ полевой уровень	
Функциональность		
Фильтр пакетов	+	+
Режим работы: IP-брандмауэр (L3)	+	+
Режим работы: Прозрачный брандмауэр (L2)	+	-
Глубокая проверка пакетов (DPI)	-	Modbus/TCP
NAT	+	+
VPN	+	+
Маршрутизация	+	+
L3 резервирование	+	+
Порты	2 FE	2GE, 4FE
Режим обучения	+	+

Таблица 2: Сравнение механизмов NAT

Свойства	IP Masquerading	1:1 NAT	Port Forwarding
Инициализация соединения изнутри	Да	Да	Нет
Инициализация соединения извне	Нет	Да	Да

Hirschmann EagleOne

Самой младшей в линейке Eagle является модель EagleOne (табл. 1), которая на первый взгляд не отличается внушительными габаритами и наличием большого числа коммуникационных коннекторов, она содержит на борту всего пару портов RJ45 и разъем питания. Но на самом деле внутри скрывается достаточно богатая и полезная функциональность: устройство может работать в режиме роутера, позволяет создавать VPN туннели, списки доступа, оснащено фильтром пакетов, а также механизмом трансляции сетевых адресов (NAT) (рис. 3). EagleOne способен функционировать как в режиме IP-брандмауэра, так и в режиме прозрачного брандмауэра. Ко всему прочему в устройстве предусмотрен встроенный инструмент самообучения. Рассмотрим более подробно функциональность EagleOne.

Фильтр пакетов

Фильтр пакетов позволяет производить управление трафиком данных путем проверки содержимого передаваемых пакетов. EagleOne предоставляет возможность задания параметров анализа и фильтрации как входящих/исходящих IP-пакетов, так и входящих MAC-пакетов (фреймов). Брандмауэр проверяет каждый пакет данных по установленным правилам, начиная с первого. После анализа данных устройство принимает решение отбросить (drop), отклонить (reject) либо принять (accept) данные. При этом существенно облегчить задачу создания очередного фильтра может функция создания шаблона адресов. Она может быть использована для быстрого и простого создания и изменения записей фильтра пакетов, если, например, применяются одни и те же диапазоны IP-адресов для адреса источника или назначения в нескольких правилах. Другими словами, можно определить эти адреса в качестве шаблонов. Шаблон адреса состоит из одной или нескольких записей с одинаковым именем. При желании можно ввести индивидуальный адрес с маской, отдельно активировать или деактивировать отдельные адреса шаблона.

При конфигурации фильтра пакетов рекомендуется использовать шаблон адреса в форме переменной. Это реализуется путем помещения символа $ перед именем. Переменные можно использовать для исходных адресов и адресов назначения.

Режим обучения (FLM)

Режим обучения (FLM) — это удобный помощник по настройке, который помогает анализировать трафик и создавать необходимые правила для его анализа. Режим обучения брандмауэра позволяет:

— определить трафик, который существующие правила еще не охватывают;

— анализировать трафик на основе различных задаваемых критериев;

— создавать новые значения из анализа трафика;

— изменять правила, если это необходимо, и визуализировать их зону охвата.

FLM применяется только к пакетам, которые проходят через брандмауэр. Он не применяется к пакетам, которые отправляются самому устройству и тем, которые оно создает.

Пример применения режима обучения брандмауэра

На рис. 4 показан пример установки нового производственного сегмента на предприятии. В качестве первоначальной настройки рекомендуется разделить общую (10.115.0.0/19) и производственную (10.0.1.0/24) сети. Разделение реализовано с помо-

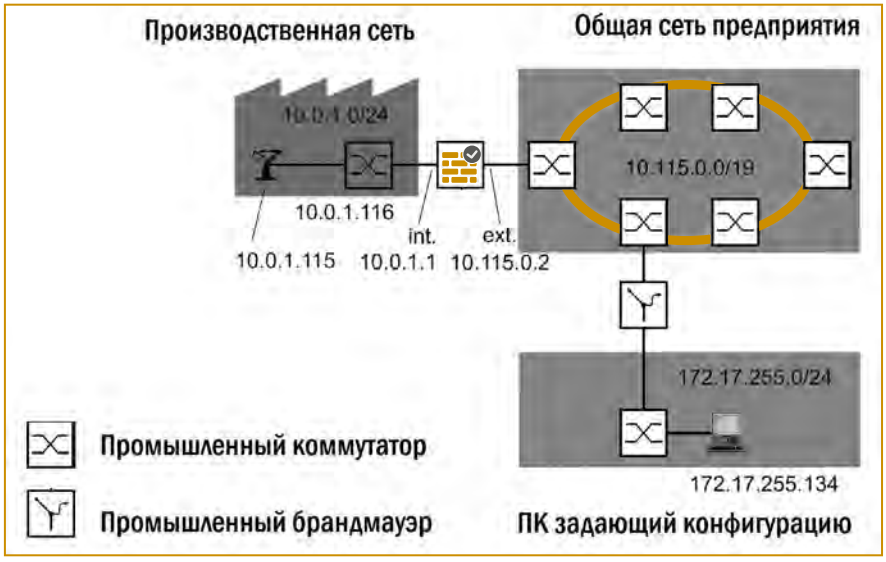

Рис.4. Режим обучения брандмауэра, пример использования

щью промышленного брандмауэра EagleOne, который функционирует в режиме IP-брандмауэра и дополнительно осуществляет маршрутизацию. Внутренний интерфейс «int» расположен в производственной сети, а внешний «ext» — в общей с соответствующей установкой IP-адресов. Далее необходимо настроить ряд фильтров, которые позволят обеспечить пропуск необходимого трафика (как для задания конфигурации, так и служебного) к устройствам, расположенным в производственном сегменте. В противоположном же направлении от производственного сегмента к общей сети компании поток данных должен проходить свободно. Трафик от других сетей передачи данных должен быть отброшен брандмауэром. Но предусмотреть весь возможный трафик и установить для него правила бывает достаточно непросто. Для этого как раз и предназначен режим обучения. В этом режиме устройство анализирует только трафик, для которого не было настроено ни одного правила. Таким образом, на этапе обучения устройство игнорирует трафик, для которого уже были настроены явные правила. Во время работы режима обучения брандмауэр позволяет скорректировать правила пропуска трафика.

На рис. 5 представлен графический интерфейс промышленного брандмауэра EagleOne. Здесь цветом выделены строки для проходящего трафика. В светло-сером цвете отображены строки трафика, для которых правила были уже созданы. Темно-серым цветом отображены строки, которые охватывает новое созданное правило. Данные правила вступят в силу, когда будет закрыт помощник режима обучения брандмауэра. Белым же цветом выделены строки проходящего трафика, который был удален, исходя из принятых ранее правил.

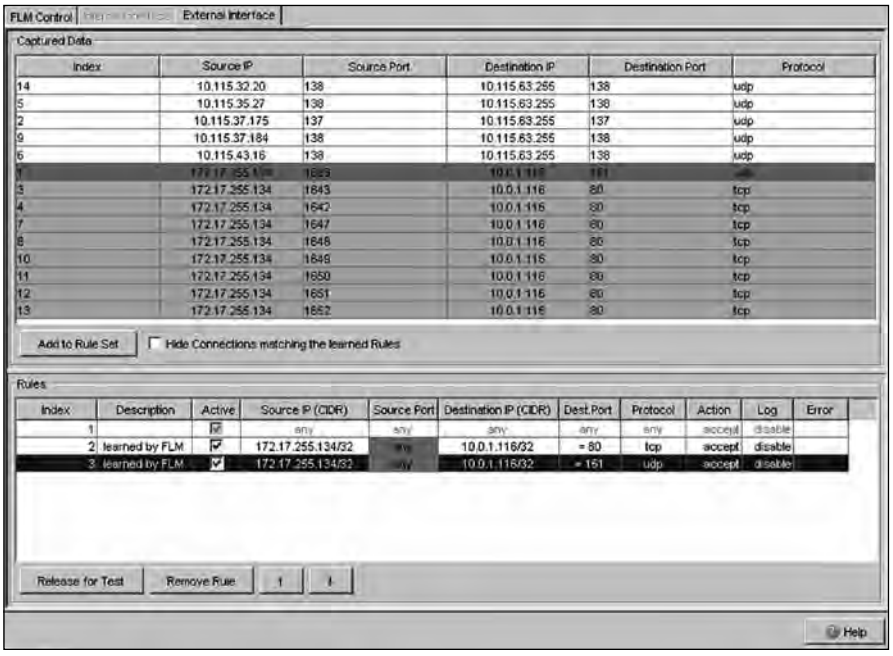

Рис. 5. Режим обучения брандмауэра, графический интерфейс EagleOne, внешний интерфейс (int)

Защита от DoS (Denial of Service) атак

Защита от DoS (Denial of Service) атак помогает оградить сеть и сервер от несанкционированного доступа, который может быть получен вследствие чрезмерного «наводнения» сети TCP-соединениями, ping или ARP-пакетами. Для ее запуска необходимо настроить значения, которые будут определены параметрами по умолчанию, на TCP соединения, Ping-пакеты и ARP-пакеты, которые необходимы в сети. При превышении каждого из пороговых значений EagleOne создает запись в log-журнале.

NAT — трансляция сетевых адресов

Протокол трансляции сетевых адресов (NAT) описывает процедуру автоматического изменения информации об IP-адресах в пакетах данных с последующей передачей их в точное место назначения. NAT используется, например, чтобы IP-адреса внутренней сети не были видны извне. Причины этого могут быть различными от использования IP-адресов несколько раз и до желания сохранить структуру внутренней сети, скрытой для внешних источников. В зависимо-

Каждый достоин лишь того мира, который он способен защитить сам.
Сергей Лукьяненко

сти от необходимых параметров и свойств существуют различные типы NAT (табл. 2)

IP Masquerading используется, чтобы скрыть внутреннюю структуру сети извне за маской. С помощью механизма IP Masquerading брандмауэр заменяет исходный IP-адрес пакета данных из внутренней сети внешним IP-адресом брандмауэра. Для определения внутреннего IP-адреса NAT добавляет логический номер порта соединения к информации об адресе.

Добавление данной информации также дало данному механизму имя Network Address Port Translation (NAPT). Преобразуя IP-адреса и используя информацию о портах, устройства могут устанавливать коммуникационные соединения снаружи из внутренней сети. Однако, поскольку устройствам во внешней сети известны только внешний IP-адрес брандмауэра, они не могут настроить коммуникационное соединение с устройством во внутренней сети.

1:1 NAT используется при необходимости создать идентичные производственные сегменты с одинаковыми IP-адресами, при этом требуется подключить их к внешней сети. При данной схеме брандмауэр назначает устройствам во внутренней сети различные IP-адреса для внешней сети. При работе механизма NAT 1:1 брандмауэр заменяет исходный IP-адрес пакета данных из внутренней сети на IP-адрес внешней сети.

Посредством преобразования IP-адресов 1:1 устройства могут устанавливать коммуникационные соединения с внешней сетью из внутренней сети, а устройства во внешней сети могут устанавливать коммуникационные соединения с устройством во внутренней сети. В связи с этим NAT 1:1 также называют двунаправленным NAT.

Также при использовании механизма NAT 1:1 предусмотрена возможность объединения устройств путем создания резервированного L3 соединения. При этом два физических устройства образуют виртуальный маршрутизатор NAT с высокой доступностью 1:1. Однако стоит учитывать, что механизм NAT 1:1 изменяет IP-адреса только в IP-заголовках пакетов.

Инверсный NAT 1:1 используется при необходимости обмениваться данными устройствам из внутренней и внешней сети, как например, если бы устройства из внешней сети находились во внутренней сети. Для данной реализации брандмауэр назначает устройствам во внешней сети различные IP-адреса из внутренней сети. Для инверсного NAT 1:1 брандмауэр заменяет IP-адрес назначения в пакете данных с внутренней сети на IP-адрес внешней сети.

Double NAT, называемый также Twice NAT, используется при необходимости обмениваться данными устройствам во внутренней и внешней сети, как если бы устройства во внешней сети находились во внутренней сети и наоборот. Механизм работы подразумевает, что устройствам из внутренней сети присваивается IP-адрес из внешней сети (NAT 1:1), а к устройствам из внешней сети — IP-адрес из внутренней сети (инверсная функция NAT 1:1). При использовании Double NAT для пакета данных из внутренней сети брандмауэр заменяет исходный IP-адрес на IP-адрес из внешней сети, а IP-адрес назначения на IP-адрес внешней сети.

Port Forwarding — это механизм, позволяющий скрыть внутреннюю структуру сети для устройств из внешней сети, но при этом сохраняется возможность доступа устройствам из внешней сети к устройствам из внутренней. При данном механизме одно или несколько устройств из внешней сети настраивает коммуникационное соединение с внутренней сетью. При этом устройство из внешней сети адресует пакеты данных конкретному порту с внешним IP-адресом брандмауэра. Пакеты данных с разрешенным исходным IP-адресом, который брандмауэр получает по определенному порту, перенаправляются брандмауэром на порт внутреннего устройства в сети, введенного в таблицу NAT. Отсюда и название Port Forwarding. Так же данная процедура известна как Destination NAT. Преобразуя IP-адреса и информацию о портах, устройства могут настраивать внутренние сетевые коммуникационные соединения из внешней сети.

Типовым применением в промышленном секторе является порт 5631 для удаленного обслуживания ПК в производственном секторе.

Брандмауэр для определенного пользователя (User Firewall)

Данная функциональность позволяет управлять потоком данных для конкретного пользователя. Для каждого пользователя можно создать различные правила, на основе которых брандмауэр будет анализировать полученные пакеты данных и принимать дальнейшее решение. Порядок работы достаточно прост и схож с авторизацией на любом сайте или форуме. После регистрации пользователя в Web-интерфейсе брандмауэра устройство идентифицирует его и в дальнейшем проверяет пакеты данных для этого конкретного пользователя на основе правил, определенных для него. Если ни одно из этих правил не применяется, брандмауэр проверяет пакеты данных на основе общих фильтров пакетов.

Данная функция позволяет предоставить определенным пользователям доступ к внутренней или внешней сети в течение ограниченного периода времени, доступ при этом осуществляется на основе правил. Это может быть полезно, например, при удаленном сервисном обслуживании устройств, находящихся в промышленном сегменте сети.

Создание защищенных соединений

Данная функция реализована посредством создания виртуальной частной сеть (Virtual Private Network, VPN) между двумя устройствами. Фактически это

часть общедоступной сети, которая используется для передачи данных. Особенность VPN, как следует из названия private, заключается в том, что соединение закрыто от общедоступной сети. Создание защищенного соединения посредством VPN позволяют защитить данные от шпионажа, фальсификации данных и других атак от внешних источников. В промышленной среде VPN, как правило, используется для соединения двух секций предприятия друг с другом через общедоступную сеть Internet. Для реализации этого механизма в промышленном брандмауэре EagleOne используются следующие механизмы и протоколы.

1) IPsec (Internet Protocol Security) является наиболее часто используемым протоколом VPN, точнее группой протоколов. IPsec регулирует настройку VPN-соединения и меры по безопасной передаче данных в виртуальной частной сети. Безопасная передача данных в VPN включает:

— *защиту целостности соединения*, гарантирующую подлинность переданных данных, то есть их поступление от надежного отправителя;

— *шифрование,* гарантирующее запрет на просмотр данных без разрешения. Процедуры шифрования кодируют данные, которые должны передаваться, используя код (ключ), который доступен исключительно для авторизованных абонентов;

— *конфиденциальность потока трафика* помогает гарантировать, что никто из неавторизованных лиц не сможет получить информацию о фактическом получателе и отправителе пакета данных.

IPsec выполняет все перечисленные функции, шифруя полный IP-пакет. Для согласования параметров безопасности, которые должны использоваться между двумя конечными точками VPN-соединения, IPsec предоставляет два режима — транспортный и туннеля.

В транспортном режиме два терминальных устройства определяют подлинность друг друга, затем устанавливают параметры, необходимые для подписи и шифрования. Поскольку связь происходит между двумя определенными терминальными устройствами, адреса получателя и отправителя остаются видимыми.

В туннельном режиме два устройства удостоверяют подлинность друг для друга, затем устанавливаются параметры, необходимые для подписи и шифрования.

С двумя устройствами VPN-соединение имеет две адресуемые оконечные точки, но связь осуществляется между абонентами сети, подключенными к шлюзам. Это позволяет шифровать передаваемые данные, включая адреса получателей и отправителей. Адреса шлюзов используются для адресации конечных точек VPN-соединения. Режим туннеля может также использоваться для VPN-соединения между терминальным устройством и шлюзом. Таким образом, адресные данные в сети, подключенной к шлюзу, остаются скрытыми.

2) IKE (Internet Key Exchange) используется для обмена ключами, дальнейшей аутентификации и обеспечения безопасности VPN-соединения. Аутентификация используется как часть соглашения о безопасности. Во время аутентификации соединяемые устройства предоставляют друг другу свои идентификационные данные, которые могут состоять из предварительного общего ключа (символьной строки, ранее передаваемой по другому каналу связи), а также цифрового сертификата. Сертификат содержит достаточно большой объем информации. Например, сертификаты, основанные на стандарте X.509, содержат:

— информацию о сертификационном органе,

— срок действия сертификата,

— информацию о разрешенном использовании,

— личность, которой присваивается сертификат (X.500 DN),

— открытый ключ, принадлежащий данной идентификации,

— цифровая подпись для проверки связи между этим идентификатором и связанным открытым ключом.

Крупные компании обычно имеют свои собственные центры сертификации. Также возможно получение сертификата от компании Hirschmann Automation and Control GmbH.

Для защиты данных IKE использует различные криптографические алгоритмы для шифрования данных. Как правило, конечные точки VPN-подключения требуют, чтобы ключ кодировал и декодировал данные. На первом этапе для настройки механизма безопасности IKE между конечными точками VPN-подключения, оконечные устройства соглашаются на криптографический алгоритм, который впоследствии будет исполь-

Рис. 6. Защищенное соединение при помощи создания VPN-туннеля

зовать ключ для кодирования и декодирования сообщений протокола IKE. Далее, оконечные устройства согласуют периоды времени, в течение которых происходит обмен ключами, и сообщают конечные точки, на которых происходит кодирование и декодирование. Администратор при этом заранее определяет конечные точки в настройках VPN-соединения. На втором этапе конечные точки VPN-соединения согласовывают ключ для кодирования и декодирования данных.

В большой корпоративной сети, как правило, подсети соединены друг с другом через сеть передачи данных. При этом сегменты производства и управления могут быть географически разнесены между собой. Пример подключения двух сетей, соединенных через общую сеть, изображен на рис. 6. Две из этих сетей, например, корпоративная (10.0.1.0/24) и сеть производственного цеха (10.0.3.0/24), подключены через защищенное VPN соединение. В качестве сети передачи данных выступает сеть 10.0.2.0/24. Поскольку внутренние IP-адреса должны оставаться скрытыми, VPN соединение должно работать в режиме туннеля с использованием всех описанных выше механизмов IPsec, IKE и шифрование.

Заключение

Несмотря на то, что промышленные брандмауэры являются лишь одним из многих способов обеспечения безопасности и защищенности промышленной сети АСУТП, в основе которой находится сеть передачи данных Industrial Ethernet, они по-прежнему являются ключевым элементом, без которого не может обойтись никакая модель безопасности. На сегодняшний день промышленный брандмауэр — это полноценный комплекс, оснащенный разнообразным набором функций, которые реализованы как на программном, так и на аппаратном уровне. Примером подобных устройств могут служить промышленные брандмауэры от Hirschmann серии Eagle, которые обеспечат необходимую и требуемую функциональность для построения защиты промышленной сети согласно Defense in Depth.

Список литературы

1. *Пищик Б.Н.* Безопасность АСУТП // Вычислительные технологии. Т. 18. Спец. выпуск. 2013.
2. *Ralph Langner.* To Kill a Centrifuge. Langner. 2013.
3. *Жарко Е.Ф., Промыслов В.Г.* Использование концепции и моделей безопасности iec 62443 для систем промышленной автоматики и контроля атомных электрических станций // XII Всероссийское совещание по проблемам управления – ВСПУ-2014. М. ИПУ РАН. 2014.
4. *Зойферт Ф.* Концепция защиты промышленного ИТ-контура на основе брандмауэра Hirschmann серии Eagle//Современные технологии автоматизации 2013. № 3.

Воробьев Сергей Сергеевич *– специалист компании ПРОСОФТ.*
Контактный телефон +7(495) 234-06-36.
E-mail: vorobyev.s@prosoft.ru

Cisco представила сеть будущего, способную обучаться, адаптироваться и развиваться

Компания Cisco представила комплекс интенционно-ориентированных (intent-based, основанных на намерениях) сетевых решений. Появление этих решений стало возможным благодаря разработкам Cisco, направленным на создание интуитивной системы, способной предвидеть действия, нейтрализовать в зародыше угрозы безопасности, а также непрерывно совершенствоваться и обучаться. В эпоху роста числа подключений и развития распределенных технологий такая система поможет бизнесу открывать новые перспективы и решать проблемы, считавшиеся ранее неразрешимыми.

Новая сеть стала результатом многолетней работы научных сотрудников и инженеров Cisco, которые создавали решение для инфраструктуры будущего, когда сетевые инженеры, управляющие сотнями устройств, станут управлять миллионами.

Сегодня для управления своими сетями компании задействуют традиционные ИТ-процессы, которые станут анахронизмом в наступающей эпохе. Подход Cisco дает возможность создать интуитивную систему, которая постоянно обучается, адаптируется, автоматизирует и защищается, а также позволяет оптимизировать эксплуатацию сети и противостоять нарастающим атакам злоумышленников.

Решение Cisco Encrypted Traffic Analytics (ETA) решает проблему сетевой безопасности, долго считавшуюся неразрешимой. Используя интеллектуальные средства Cisco Talos, Cisco ETA находит известные сигнатуры атак даже в зашифрованном трафике, помогая обеспечивать безопасность при сохранении конфиденциальности.

Львиная доля мирового интернет-трафика передается по сетям Cisco, и компания воспользовалась своим уникальным положением, чтобы проанализировать эти чрезвычайно ценные данные и предоставить ИТ-специалистам информацию, которая позволила бы выявлять аномалии и предвидеть проблемы в реальном времени, сохраняя при этом конфиденциальность. Автоматизируя границу сети и встраивая технологии машинного обучения и аналитики в базовый уровень, Cisco делает неуправляемое управляемым и дает ИТ-отделам возможность сосредоточиться на стратегических потребностях бизнеса.

Уже сегодня предварительные полевые испытания сетевых решений следующего поколения проводят 75 ведущих международных предприятий и организаций, среди которых DB Systel GmbH, Высшая школа прикладных наук Яде (Jade University), NASA, Royal Caribbean Cruises Ltd., Scentsy, UZ Leuven и Wipro.

Http://www.cisco.com