Сергей Воробьёв

Глубокая защита промышленного сетевого периметра

В статье рассмотрен вариант организации защиты промышленной Ethernet-сети на базе принципа "Defense in Depth", который представляет собой специализированный многоступенчатый подход, позволяющий выстроить оптимальную защиту сетевого периметра промышленного объекта.

Введение

Тенденция последних лет заключается в повышенном внимании к обеспечению безопасности промышленной сети, которая представляет собой очень важный аспект любого индустриального объекта. Ведь переход к концепции Industry 4.0, развитие технологий IoT и создание умного предприятия требуют практически полной взаимосвязи между отдельными объектами, начиная от производственных площадок и заканчивая кластерами управления с облачными хранилищами данных [1, 2]. В связи с этим требуется комплексный подход к организации защиты всей сетевой инфраструктуры. И если решений для обеспечения безопасности IT-сетей достаточно много, то обеспечение безопасности промышленной сети – вопрос более сложный, требующий дополнительного анализа и особого подхода. Многочисленные инциденты с вирусами Stuxnet, Duqu, Flame, которые атаковали промышленные объекты по всему миру, подтолкнули специалистов к комплексному пересмотру политик безопасности сетей АСУ ТП промышленных объектов [3].

Промышленный вирус: что за зверь?

Отличительная особенность промышленных вирусов в том, что их цель – воздействие на оконечные устройства полевого уровня АСУ ТП. Наиболее известный практический пример – атака на крупное предприятие атомной промышленности Ирана в 2010 году. В результате деятельности вируса Stuxnet контроллеры Siemens SIMATIC S7-417/315 [4], отвечающие за управление центрифугами для обогащения урана (рис. 1), стали функционировать некорректно: скорость вращения центрифуг неконтролируемо возросла почти в полтора раза, до 84 600 об./мин. Это привело к значительному повышению риска аварийной ситуации, что вынудило руководство предприятия остановить все технологические процессы. На устранение последствий воздействия вируса ушло достаточно много времени и средств. Тем не менее, эти потери можно считать лёгкими – ведь гипотетические неполадки на атомном предприятии грозят катастрофой глобального масштаба.

После ряда подобных случаев на многих промышленных предприятиях во всём мире были пересмотрены политики безопасности в части дополнительной антивирусной защиты, причём ряд подходов был взят из готовых наработок IT-сферы. Это дало возможность частично

©www.tehrantimes.com

Рис. 1. Центрифуги для обогащения урана на заводе атомной промышленности в Иране

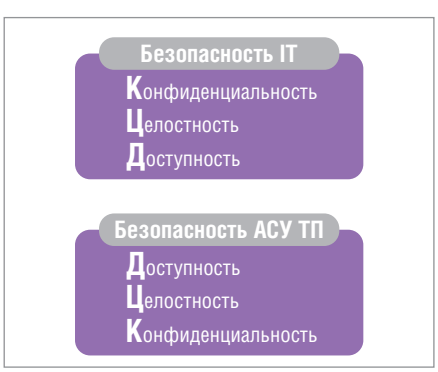

Рис. 2. Подходы к обеспечению безопасности IT-сети и промышленной сети АСУ ТП

повысить уровень защищённости периметра предприятий. Однако, поскольку в промышленных политиках безопасности во главу угла ставится не конфиденциальность, как в IT-сфере, а целостность информации, методы защиты промышленных сетей должны быть принципиально иными (рис. 2). Практика показывает, что на сегодняшний день необходим более глубокий подход к реализации защиты сети АСУ ТП промышленного объекта, нежели для IT-сетей. В частности, необходимо учитывать тот факт, что вирусы, подобные Stuxnet, – это тщательно разработанное вредоносное программное обеспечение, создаваемое злоумышленниками с высокой профессиональной квалификацией.

Industrial Ethernet: в чём особенность построения защиты?

Переход промышленных объектов на сеть Industrial Ethernet (промышленный Ethernet) фактически является свершившимся фактом. Использование единой среды передачи данных позволяет существенно увеличить гибкость сети всего промышленного объекта. На сегодняшний день сеть, построенная по принципу Industrial Ethernet, даёт возможность с лёгкостью провести интеграцию между промышленными и корпоративными сегментами. Это позволяет организовать управление и взаимодействие на качественно новом уровне. В качестве примера можно привести удалённые VPN-соединения, которые могут быть использованы для создания непосредственной

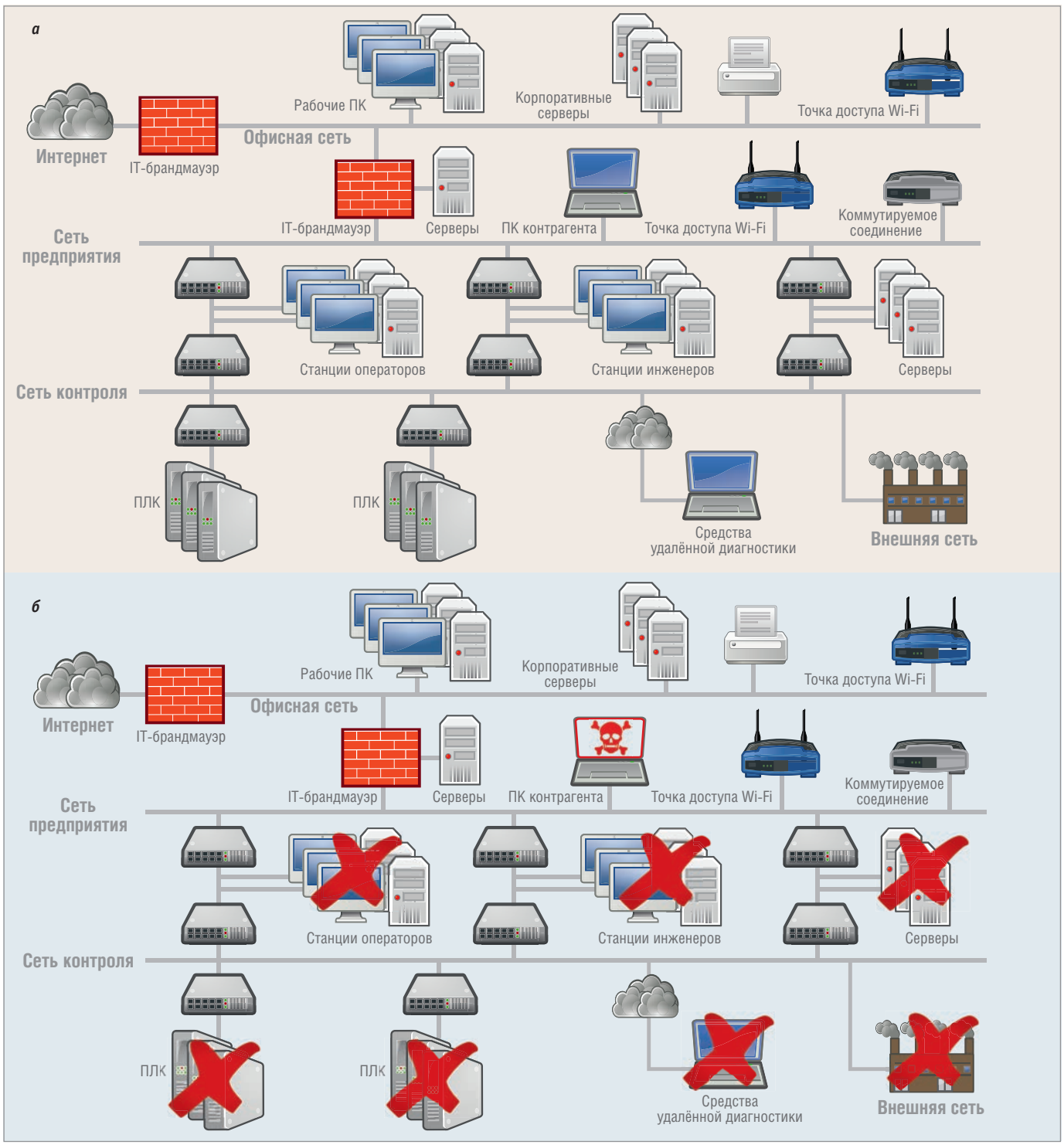

Рис. 3. Пример защиты промышленной сети, перенесённый из IT-сферы: *а* – брандмауэр установлен на границе с сетью Интернет, а также на границе между объединёнными сетями; *б* – последствия работы вирусного ПО, проникшего во внутреннюю сеть изнутри

связи и обмена информацией между головным офисом компании и производством и могут быть расположены даже на разных континентах. Подобные возможности, бесспорно, увеличивают гибкость управления. Однако нередки случаи, когда после подобных объединительных действий организация безопасности всей сети строится по уже известной схеме, справедливой для IT-сферы. На рис. 3*а* изображён пример подобного решения, которое заключается в установке брандмауэра на границе с сетью Интернет, а также на границе между объединёнными сетями. Такой подход позволит обеспечить хорошую конфиденциальность и защиту от внешних атак. Но если угроза появляется в присоединённой промышленной сети, то возникает вероятность воздействия вирусного ПО на все незащищённые объекты (рис. 3*б*). Это связано с тем, что в настоящий момент промышленная сеть, которая частично или полностью была переведена на Ethernet, – фактически лёгкая добыча для любого вирусного ПО. Она, как правило, плохо сегментирована, при этом многие сегменты сделаны открытыми без выделения отдельных подсистем. ПК и ПЛК функционируют в режиме 24/7 без критичных обновлений. Также существуют множественные варианты входа: флэш-накопители, не отключённые порты и т.д. Не стоит забывать, что особенность промышленной сети, в первую очередь, заключается в используемых технологиях, она достаточно сложна и реализуется как распределённая по функциям система, взаимодействующая посредством локальной сети. Основной единицей, обеспечивающей связь, является коммутатор, работающий на уровне L2 модели OSI, оперирующий исключительно MAC-адресами для организации быстрого обмена. Также зачастую применяются узкоспециализированные технологии и компоненты, такие как SCADA-серверы, панели оператора, ПЛК и т.п. Для обеспечения полноценной защиты промышленной сети необходимо контролировать трафик сразу на нескольких уровнях модели OSI. В итоге, учитывая эти моменты, можно сказать, что подход к организации защиты сети промышленного объекта должен быть достаточно специфическим. В особенности это касается тех сегментов, которые задействованы непосредственно в технологических процессах производства. Ведь слабый контроль доступа к критически важным системам может иметь просто катастрофические последствия. В связи с этим необходимо правильно выбрать как аппаратную, так и программную платформу, причём не стоит забывать и про архитектуру построения сети в целом.

Промышленному Ethernet – промышленный брандмауэр

Ни для кого не секрет, что наиболее популярным инструментом, который предлагается для обеспечения безопасности любой Ethernet-сети, в том числе и промышленной, является брандмауэр (нем. *Brandmauer*), он же файрвол (англ. *Firewall*), или межсетевой экран. Как правило, это решение для осуществления контроля и фильтрации проходящего через него сетевого трафика в соответствии с заданными правилами. Но как бы ни называли данный класс программных либо программно-аппаратных элементов Ethernet-сети, 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 неё, 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 учётом развития Ethernet-сетей подобные решения можно разделить на два типа, которые чаще всего применяются. К первому типу можно условно отнести брандмауэры (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, который установлен практически на каждом ПК. Ко второму типу можно отнести 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 её границе, либо между подсетями, или в самом сегменте. Весь трафик при этом проходит через отдельное устройство, подвергаясь глубокому анализу. Именно устройства второго типа (рис. 4) обычно встречаются в промышленных Ethernet-сетях. Это связано с тем, что промышленная сеть АСУ ТП, как правило, разделена на отдельные крупные сегменты, которые осуществляют тот либо иной производственный/технологический процесс. В настоящее время в большинстве случаев, если упомянуто такое устройство, как промышленный брандмауэр/файрвол, или межсетевой экран, то имеется в виду отдельный программно-аппаратный комплекс, который 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 защищённости сети. Например, если в сегменте сети одновременно находятся ПЛК, промышленные ПК и, например, сервер сбора данных, то можно создать ряд правил для промышленного брандмауэра, которые позволят получить доступ к серверу сбора данных ограниченному кругу 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 несанкционированного доступа. Но если исходить из общемировых тенденций и правил, то обычно на промышленных объектах применяется принцип глубокой защиты, или защиты в глубину (англ. *Defense in Depth*), которая также упомянута в стандарте МЭК 62443 [5].

"Defense in Depth" – защищай свою сеть, как свой за́мок

Принцип "Defense in Depth" дословно можно перевести как защита в глубину, он достаточно известен, особенно при построении многоуровневой защиты самых различных объектов. В основе лежит

Рис. 4. Внешний вид промышленного брандмауэра Tofino Xenon от Hirschmann

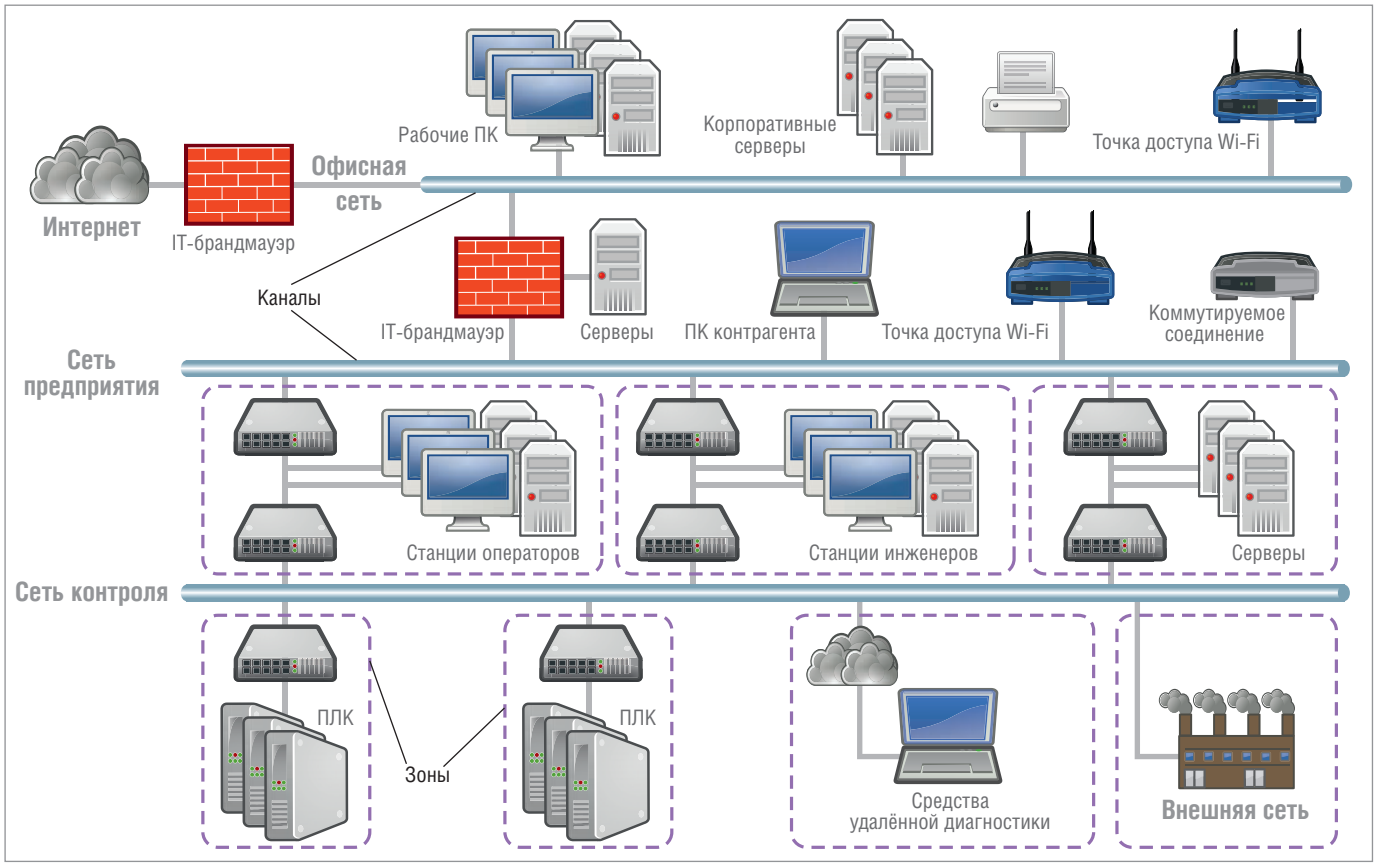

Рис. 5. Концепция зон и каналов для промышленной сети

Модель OSI	Тип информации	Решение, обеспечивающее безопасность
7. Прикладной		
6. Представления	Данные	Глубокая проверка пакетов (DeepPacketInspection)
5. Сеансовый		
4. Транспортный	Сегменты	Шифрование
3. Сетевой	IP-пакеты	Роутер+L3-брандмауэр
2. Канальный	Фреймы	Коммутатор+L2-брандмауэр
1. Физический	Биты	Физическая защита линии

Рис. 6. Решения для обеспечения многоуровневой защиты сети на примере модели OSI

так называемая концепция зон и каналов (англ. *Zones and Conduits*), позволяющая разделить критически важные сегменты. Данная концепция заключается в том, что сеть сперва разделяется на каналы – крупные сегменты, например, сегмент производства, а далее выделяются отдельные зоны, например, отдельные технологические процессы, которые примыкают к каналам. В итоге получается многоуровневая и многозонная сеть с возможностью создания эффективного механизма защиты (рис. 5). Если атака злоумышленника приводит к сбою одного механизма безопасности, то другие механизмы могут по-прежнему обеспечивать необходимую защиту для безопасности сети. Принцип "Defense in Depth" можно сравнить с организацией защиты древнего зáмка: защитные рвы, стены, башни и т.д. Отдельные зоны замка отделены друг от друга контролируемыми и управляемыми препятствиями: ворота, разводные мосты, чтобы сдержать нападающих и затруднить их передвижения. Конечно, разводные мосты и рвы для защиты сети достаточно неэффективны, но правильно организованная иерархия может быть достаточно проста и эффективна одновременно.

Рассмотрим небольшой пример. Возьмём систему контроля и сбора параметров АСУ ТП, как правило, для получения доступа к подобной системе необходимо пройти аутентификацию путём ввода связки логин–пароль. Зачастую, стараясь повысить уровень безопасности, администраторы сети увеличивают требуемую длину пароля вплоть до 15 символов. Данный факт, с одной стороны, несомненно, увеличит устойчивость системы к атакам при помощи перебора типа Brute Force, но с другой, приведёт к тому, что работники будут записывать свои пароли для аутентификации, что создаст возможность их кражи третьими лицами. А если добавить дополнительный уровень в процесс аутентификации и разбить его на 2 этапа, это позволит избежать обозначенной ранее проблемы. Например, идентификация при помощи смарт-карты и ввода 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. По той же аналогии рекомендуется выстраивать и одноимённый принцип защиты для сетей Industrial Ethernet. При этом стоит выделить критически важные уровни модели OSI (рис. 6) и исходя из них реализовать несколько уровней защиты при помощи промышленных брандмауэров/файрволов.

Разные уровни – разные задачи фильтрации

Как было отмечено ранее, основная задача промышленного брандмауэра – это контроль и фильтрация проходящего через него сетевого трафика. При этом существуют различные механизмы для его анализа. Требования формируются, исходя из тех задач, которые ставятся пе-

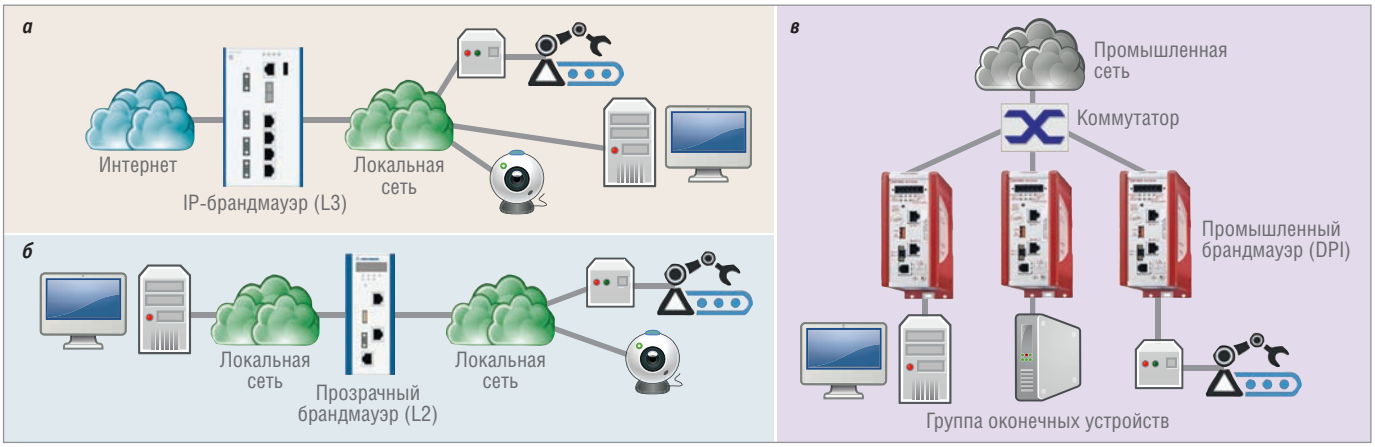

Рис. 7. Варианты применения промышленных брандмауэров: *а* – брандмауэр установлен между промышленной и общедоступной сетью (IP-брандмауэр); *б* – брандмауэр установлен в сети производственного сегмента (прозрачный брандмауэр); *в* – брандмауэр установлен в непосредственной близости к оконечным устройствам (DPI-брандмауэр)

ред брандмауэром. И если на границе сети это в первую очередь быстрая работа по спискам доступа, то ближе к оконечным устройствам необходимо обеспечить более глубокую фильтрацию на уровне промышленных протоколов.

При выборе брандмауэра важно знать, насколько глубоко он может анализировать связь между различными устройствами. Это обусловлено тем, что установка связи и последующее взаимодействие между устройствами может происходить в различных фазах. Например, связь устанавливается в первой фазе. Активная связь и обмен информацией ведётся на второй фазе, и соединение завершается в третьей фазе. При этом могут быть задействованы различные уровни модели OSI. Таким образом, если, например, брандмауэр функционирует на уровне L3, модели OSI, то он может быстро на скорости 1 Гбит/с отследить взаимодействие между двумя управляемыми устройствами, например маршрутизаторами. Но с другой стороны, подобный брандмауэр не может распознавать или предотвращать любые атаки, вызванные ненормальным поведением протоколов верхних уровней, например Modbus TCP. Для данных задач необходим более глубокий анализ передаваемого трафика, который, в свою очередь, может существенно увеличить степень защищённости, но повлечёт уменьшение скорости передачи до 100 Мбит/с. В связи с этим необходимо формировать сбалансированную многоуровневую защиту промышленной сети, как на границе сети, так и внутри ядра сети, что в итоге позволит обеспечить более тщательную проверку и фильтрацию проходящего трафика. В настоящий момент можно выделить 4 уровня, или границы, которые необходимо контролировать.

Уровень 1: граница сети, анализ IP-пакетов

Промышленные брандмауэры, установленные на границе сети, выполняют достаточно широкий круг задач, в основе которых находится разделение и сегментирование 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 удалённый производственный сегмент к общей корпоративной сети, например посредством сотовой 3G/4G-сети, анализируя при этом весь проходящий через него трафик. Подобный класс устройств называется IP-брандмауэрами, поскольку он представляет собой управляемую границу, например, между сетью предприятия и внешней сетью – сетью провайдера или Интернет (рис. 7*а*). Как правило, функциональность подобных устройств требует наличия функционального фильтра IP-пакетов, возможности маршрутизации, создания VPN-туннелей, списков доступа, а также механизмов трансляции сетевых адресов (NAT – Network Address Translation).

Уровень 2: внутренняя сеть, анализ фреймов

Как было упомянуто ранее, Industrial Ethernet становится единой средой для передачи данных на промышленных объектах. При этом угрозы, связанные с безопасностью промышленной сети, могут исходить как из внешней сети, так и из внутренней, в которой находятся устройства, функционирующие исключительно на уровне L2 и передающие данные на основе MAC-адресов. И если от внешних угроз может защитить правильно настроенный промышленный IP-брандмауэр (согласно “Defense in Depth” это лишь первый защитный контур), то от внутренних угроз из собственной сети нужно защищаться иначе. И для этого хорошо бы знать, что происходит внутри, на уровне L2. Поводом к некорректной работе может послужить, например, не только вирусная активность, но и некорректная работа собственного внутреннего программного обеспечения.

Если в целом рассматривать промышленную сеть, то множество устройств работают на уровне L2, и, например, неконтролируемый broadcast (широковещательный пакет) может заполонить всю сеть, при этом IP-брандмауэр, который функционирует на уровне L3 и работает исключительно с IP-адресами, будет работать в штатном режиме и никак не будет сигнализировать о наличии некорректно работающих устройств. Для решения данной проблемы в дополнение к IP-брандмауэру необходим так называемый прозрачный брандмауэр (рис. 7*б*). Данное устройство функционирует исключительно на уровне L2 модели OSI и становится следующим защитным звеном. Оно устанавливается в разрыв внутренней сети и анализирует трафик на уровне фреймов. При этом брандмауэр уровня L2 прозрачен для протоколов верхнего уровня.

Уровень 3: WLAN

Беспроводные сети (WLAN) всё чаще встречаются в промышленных сетях, при этом для подвижных объектов передача данных при помощи Wi-Fi-радиоканала зачастую является оптимальным реше-

HIRSCHMANN
A BELDEN BRAND

Clear Space® — запатентованная технология получения чистого сигнала в шумных средах

Серия Hirschmann OpenBAT

Беспроводное оборудование стандарта IEEE 802.11n (Wi-Fi)

- 1 или 2 радиомодуля IEEE 802.11a/b/g/h/n
- Скорость передачи до 450 Мбит/с
- Технологии MIMO 3×3, MESH, WDS
- –40…+75°C, конформное покрытие
- Внутреннее и внешнее исполнение IP40/IP67

Вся необходимая инфраструктура:

BAT-C – простой и компактный клиент сети
Антенны, кабели, грозозащита
BAT-Controller – аппаратный централизованный контроллер точек доступа
BAT-Planner – ПО для расчёта зон покрытия и скоростей передачи на плане объекта

ProSoft® WWW.PROSOFT.RU
ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

МОСКВА	(495) 234-0636	info@prosoft.ru
С.-ПЕТЕРБУРГ	(812) 448-0444	info@spb.prosoft.ru
АЛМА-АТА	(727) 321-8324	sales@kz.prosoft.ru
ВОЛГОГРАД	(8442) 260-048	volgograd@prosoft.ru
ЕКАТЕРИНБУРГ	(343) 376-2820	info@prosoftsystems.ru
КАЗАНЬ	(843) 203-6020	info@kzn.prosoft.ru
КРАСНОДАР	(861) 224-9513	krasnodar@prosoft.ru
Н. НОВГОРОД	(831) 215-4084	n.novgorod@prosoft.ru
НОВОСИБИРСК	(383) 202-0960	info@nsk.prosoft.ru
ОМСК	(3812) 286-521	omsk@prosoft.ru
ПЕНЗА	(8412) 49-4971	penza@prosoft.ru
САМАРА	(846) 277-9166	info@samara.prosoft.ru
УФА	(347) 292-5216	info@ufa.prosoft.ru
ЧЕЛЯБИНСК	(351) 239-9360	chelyabinsk@prosoft.ru

нием. Если клиент подключён к WLAN посредством точки доступа Wi-Fi, то появляется возможность напрямую общаться со всеми устройствами, расположенными в одной сети. Фактически точка доступа Wi-Fi становится неким порталом доступа. Даже с учётом того, что современные точки доступа в большинстве случаев используют технологии защиты беспроводных сетей WPA и WPA2, которые пришли на смену устаревшему стандарту WEP, всё равно может возникнуть ряд дополнительных угроз для остальных устройств в сети.

Злоумышленник либо вредоносное ПО может провести успешную атаку на клиента, подключённого к WLAN, и на любое другое устройство в сети Ethernet. В качестве решения данной проблемы рекомендуется использовать промышленный брандмауэр, который будет функционировать совместно с точкой доступа Wi-Fi. Но наибольшей эффективности можно достичь, если брандмауэр будет реализован непосредственно в точке доступа, так как её можно разместить как на границе сети, за несколькими уровнями защиты, так и непосредственно в ядре сети, рядом с производственным сектором. Поскольку точка доступа является теми воротами, через которые можно получить доступ к информации, то данный брандмауэр должен производить анализ трафика, как на уровне L3, так и на уровне L2 для обеспечения защиты как внутренней Ethernet-сети, так и подключённых WLAN-клиентов. Сконфигурировав подобный брандмауэр, можно ограничить пересылку сообщений между клиентами непосредственно в точке доступа WLAN. Например, связь планшета, подключённого к устройству через WLAN, может быть ограничена, так что он может получать доступ только к данным через пользовательский интерфейс, но не к дополнительным подсистемам или к другим подключённым к нему устройствам.

Уровень 4: полевой, глубокая проверка данных

Глубокая проверка и инспекция пакетов является следующим барьером, который предназначен для защиты непосредственно оконечных устройств. Как было упомянуто, Industrial Ethernet становится стандартом для промышленных сетей, но, как правило, сами оконечные устройства (ПЛК, контроллеры и т.д.) функционируют на базе хорошо известных промышленных протоколов Modbus, CAN и др. При этом информация, с которой будет работать, например, ПЛК, размещена непосредственно в передаваемом IP- пакете.

Возьмём, к примеру, популярный протокол Modbus TCP, он используется, чтобы обеспечить взаимодействие между устройствами, подключёнными к сети Ethernet, но работающими при помощи протокола Modbus. Фактически на 7-м (прикладном) уровне модели OSI используются данные Modbus RTU, которые впоследствии упаковываются в сегменты, далее в пакеты, и получается Modbus TCP [6]. Если злоумышленник или вредоносное ПО, используя узкоспециализированные шаблоны атаки, смогут получить доступ к возможности корректировать эти данные, то возникает опасность полной потери контроля над оконечными устройствами.

Промышленные брандмауэры, описанные ранее, в этом случае бессильны, так как они проверяют только заголовок в начале пакета (IP-брандмауэр) либо фрейма (прозрачный брандмауэр). И если при формировании данных на прикладном уровне запишутся некорректные данные, то оконечное устройство, например ПЛК, запишет их в свои ре-

гистры, что в дальнейшем может привести к аварии и даже катастрофе. Решением, которое сможет защитить оконечное устройство, является глубокая проверка пакетов (англ. *Deep Packet Inspection*, DPI), осуществлять её необходимо непосредственно на верхних уровнях модели OSI при помощи специализированных брандмауэров (DPI-брандмауэр). В данном случае каждый пакет данных необходимо полностью распаковывать и осуществлять проверку передаваемых данных на уровне протоколов и полезной нагрузки (рис. 7*в*). При этом желательно, чтобы устройство, осуществляющее данную операцию, оставалось невидимым для остальных участников сети.

Заключение

Применение сетей Industrial Ethernet на промышленных объектах, безусловно, положительно влияет на эффективность их работы. Сеть предприятия становится более гибкой, скоростной, возникают новые возможности централизованного управления. Однако у данного факта есть и обратная сторона – появление потенциальных уязвимостей. При этом, с учётом специфики промышленных сетей АСУ ТП, обеспечение её защиты является комплексной и достаточно сложной задачей. Появление вирусов, подобных Stuxnet, которые способны добраться до оконечных устройств, даёт понять, что необходим более тщательный подход к созданию защиты. Один из таких подходов – "Defense in Depth", защита в глубину. Данный подход основывается на многоступенчатой защите, которая должна анализировать передаваемый трафик на критически важных уровнях модели OSI. При этом базой, теми устройствами, которые способны проводить подобный анализ, могут выступать промышленные брандмауэры. На сегодняшний день промышленный брандмауэр – это отдельный узкоспециализированный программно-аппаратный комплекс, который устанавливается на разных уровнях доступа к промышленной сети, позволяющий фильтровать передаваемый трафик, начиная от фреймов (L2) и заканчивая уровнем промышленных протоколов (L7). Установка подобных комплексов в критически важные места промышленной сети позволит создать многоуровневую защиту объекта, позволяющую не только обеспечить защиту от внешних и внутренних угроз, но и вовремя локализировать возникшую опасность. ●

Литература

1. Швецов Д. Условия и факторы неоиндустриального развития и их влияние на мировую экономику // Современные технологии автоматизации. – 2017. – № 3.
2. Косов М. Индустрия осваивает промышленный Интернет вещей // Современные технологии автоматизации. – 2017. – № 3.
3. Пищик Б.Н. Безопасность АСУ ТП // Вычислительные технологии. – 2013. – Том 18, Специальный выпуск.
4. Ralph Langner. To Kill a Centrifuge [Электронный ресурс] // Сайт Langner Communications GmbH/ – Режим доступа : https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.
5. Understanding Firewall Technology for Industrial Cybersecurity [Электронный ресурс] // Сайт Belden Inc. – Режим доступа : http://info.belden.com/iit/understanding_firewall_technology_industrial_cybersecurity-bc-lp.
6. Денисенко В. Протоколы и сети Modbus и Modbus TCP // Современные технологии автоматизации. – 2010. – № 4.

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru