Сергей Воробьёв

“Defense in Depth” в действии. Уровень 1: защита границы сети

В статье рассмотрен вариант организации защиты границы промышленной сети Industrial Ethernet при условии построения её по принципу “Defense in Depth”. В качестве возможного инструментария описан промышленный брандмауэр EAGLE One компании Hirschmann.

Введение

Принцип построения защиты промышленной Ethernet-сети “Defense in Depth” является одним из наиболее популярных [1]. Многоуровневая структура позволяет создать высокоэффективную многоступенчатую защиту, которая будет отвечать самым современным требованиям. Фактически согласно “Defense in Depth” для разных областей промышленной сети необходимо решать разные задачи. Для организации защиты границы сети, условно назовём это уровнем 1, необходимо в первую очередь обеспечить защиту от внешних угроз. Решается это путём установки промышленного брандмауэра на границе сети, который должен функционировать на уровне L3 модели OSI [1]. Такой подход является классикой и позволяет как осуществить контроль проходящего трафика, так и предоставить дополнительную полезную функциональность.

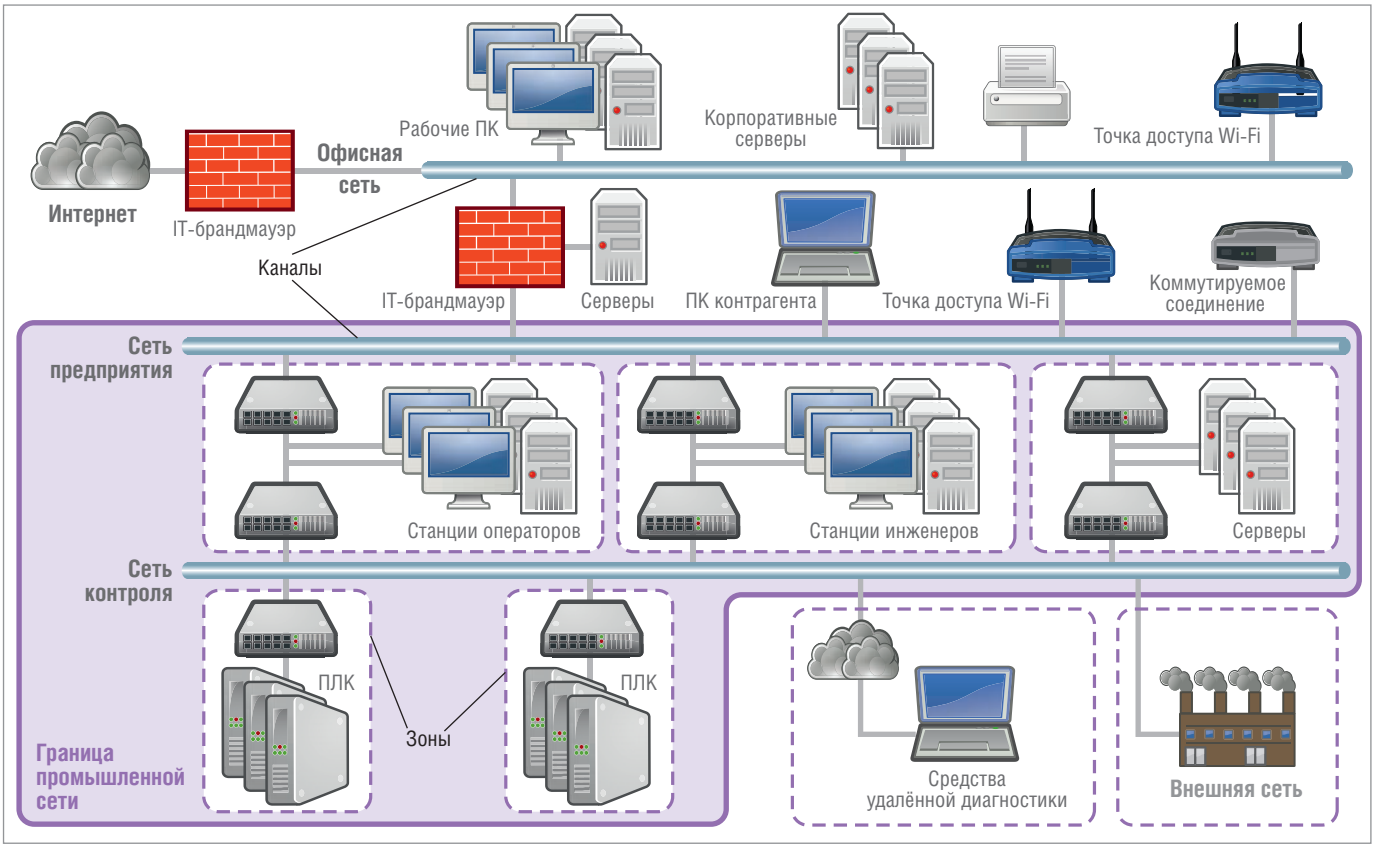

Рис. 1. Пример сети промышленного объекта

Рис. 2. Брандмауэр EAGLE One

Таблица 1

Характеристики промышленного брандмауэра EAGLE One от Hirschmann

Функциональность	Поддержка функциональности (да/нет, описание)
Фильтр пакетов	Да
Режим работы «IP-брандмауэр» (L3)	Да
Режим работы «прозрачный брандмауэр» (L2)	Да
NAT	Да
VPN	Да
Маршрутизация	Да
L3-резервирование	Да
Порты	2×Fast Ethernet
Режим обучения	Да

Функциональность: что же необходимо на границе сети

Граница сети является логическим барьером, отделяющим два её сегмента. В разрезе промышленного предприятия это может быть граница между сетью промышленного сегмента и корпоративной сетью (рис. 1). И чем более продвинутой будет её защита, тем сложнее проникнуть в неё извне. При этом важно помнить, что на границе сети реализован её раздел на внешнюю и внутреннюю сеть и все основные действия происходят на уровне IP-пакетов. И чтобы понять всю происходящую на границе сети картину, нужно знать, что устройство, которое будет осуществлять контроль, должно функционировать на уровне L3 и выше. Соответственно подобный класс устройств можно определить, как IP-брандмауэры. Набор функций не должен ограничиваться только анализом информации, содержащейся в IP-пакетах, а должен включать различные утилиты для защиты сети и подключений извне. Например, наличие дополнительной функциональности в виде создания защищённых соединений позволит увеличить защищённость ключевых объектов сети. А возможность предотвращения DoS-атак (Denial of Service – отказ в обслуживании) поможет защитить сеть и сервер от несанкционированного доступа. Рассмотрим в качестве примера подобного устройства промышленный брандмауэр EAGLE One компании Hirschmann, которая известна своими управляемыми промышленными коммутаторами для сетей Industrial Ethernet.

EAGLE One – классическое решение для границы сети

Брандмауэр EAGLE One (рис. 2) является самой младшей моделью в линейке Hirschmann, и представляет собой базовое решение. На первый взгляд, это совсем небольшая металлическая коробочка, предназначенная для монтажа на DIN-рейку, на которой расположены пара портов RJ-45, контактная группа с дежурным реле, да, в общем-то, и всё. Но на самом деле внутри скрывается достаточно богатая и полезная функциональность, которая позволяет создать мощный барьер для защиты промышленной сети. Устройство может работать в режиме роутера и осуществлять маршрутизацию, позволяет создавать VPN-туннели, списки доступа, оснащено гибким фильтром пакетов, а также механизмом трансляции сетевых адресов NAT (табл. 1) [2, 3]. Далее рассмотрим более подробно ту функциональность, которую предлагает брандмауэр EAGLE One, и назначение функций.

Фильтр пакетов

Данная функциональность является базовой для любого брандмауэра, в том числе и промышленного, она позволяет производить управление трафиком путём проверки содержимого передаваемых пакетов данных [1]. Промышленный брандмауэр предоставляет возможность задания параметров для анализа входящих/исходящих IP-пакетов. В процессе проверки каждый пакет данных проверяется по установленным правилам, их ещё называют фильтрами, начиная с первого. Далее брандмауэр принимает решение: отбросить (drop), отклонить (reject) либо принять (accept) данные. При создании фильтра необходимо указать такие параметры, как IP-адреса отправителя и точки назначения, информацию по используемым портам, а также тип протокола: TCP, UDP, ICMP (рис. 3). Однако при создании правил обычно возникает вопрос, как предугадать весь возможный трафик и создать все необходимые параметры для фильтра пакетов. В идеальной ситуации создаваемые правила должны охватывать весь возможный трафик, который будет проходить через брандмауэр. Но на практике предусмотреть весь возможный трафик и установить для него правила бывает достаточно непросто. Существенно облегчить данную задачу может дополнительный инструментарий, предназначенный для анализа трафика. В устройстве EAGLE One он называется режимом обучения (Firewall Learning Mode – FLM). Режим обучения – это удобный помощник по настройке, который помогает анализировать трафик и создавать необходимые дополнительные правила для его проверки. Режим обучения брандмауэра позволяет выполнить следующее:

- определить трафик, который существующие правила ещё не охватывают;
- анализировать трафик на основе различных задаваемых критериев;
- создавать новые правила, исходя 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 как самому устройству, так и тем, которые оно само создаёт. В режиме обучения устройство анализирует только трафик, не охваченный текущими правилами (рис. 4), то есть трафик, для которого не было настроено ни одного правила. Таким образом, в режиме обучения брандмауэр игнорирует трафик, для которого уже были настроены

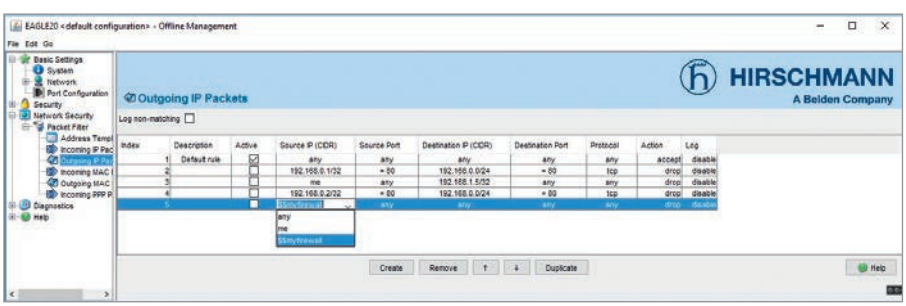

Рис. 3. Указание параметров фильтра пакетов

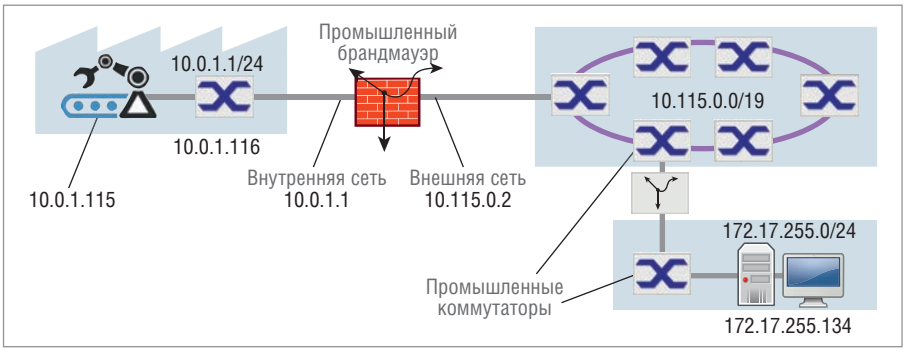

Рис. 4. Пример использования режима обучения

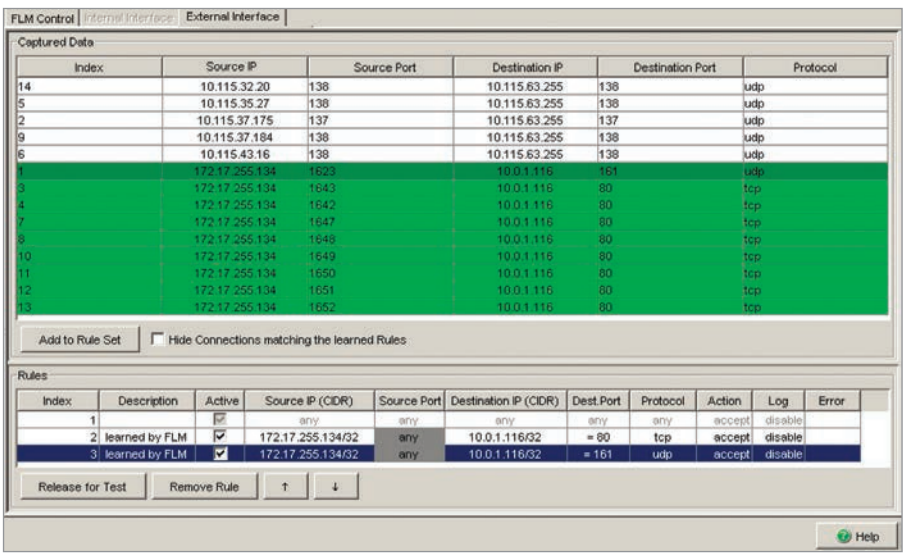

Рис. 5. Режим обучения брандмауэра, графический интерфейс EAGLE One, внешний интерфейс

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

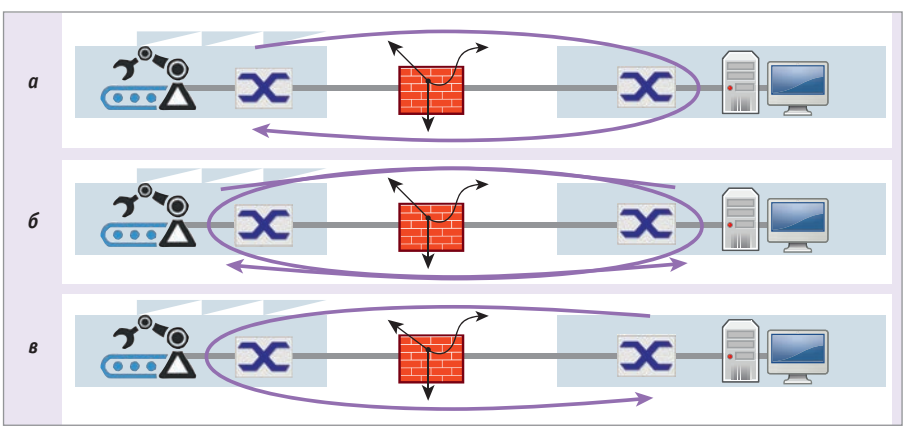

Рис. 6. Построение соединения при помощи различных режимов NAT:
***а* – IP Masquerading, *б* – NAT 1:1, *в* – Port Forwarding**

явные правила, и позволяет скорректировать существующие.

На рис. 5 представлен графический интерфейс режима обучения EAGLE One, где цветом выделены строки для проходящего трафика. Светло-зелёным цветом показаны строки трафика, для которых правила были уже созданы. Тёмно-зелёным цветом показана строка, которая описывает новое правило. Данные правила вступят в силу после того, как будет закрыт режим FLM. Белым цветом выделены строки проходящего трафика, который был удалён, исходя из принятых ранее правил.

Защита от DoS-атак

Атаки типа DoS являются достаточно популярным и, главное, простым инструментом, позволяющим создать такие условия, при которых пользователи сети не могут получить доступ к предоставляемым ресурсам. Смысл данной атаки заключается в том, что на сетевое устройство поступает большое количество однотипных запросов, например, многочисленные ping- или ARP-пакеты, с целью довести его до отказа. Однозначной защиты от DoS-атак не существует, но возможность зафиксировать атаку и предотвратить её дальнейшее развитие есть.

В брандмауэре EAGLE как раз и предусмотрена подобная функциональность. Для её запуска необходимо настроить значения, которые будут определены как параметры по умолчанию, для TCP-соединений, ping- и ARP-пакетов, которые необходимы в сети. При превышении каждого из пороговых значений EAGLE One создаёт запись в журнале (log), что позволяет зафиксировать подобную атаку.

Трансляция сетевых адресов

Механизм трансляции сетевых адресов NAT (Network Address Translation) описывает процедуру автоматического изменения информации об IP-адресах в пакетах данных с дальнейшей передачей их в место назначения. NAT используется, когда, например, необходимо, чтобы IP-адреса внутренней сети не были видимыми извне. Причины этого могут быть различными, начиная от использования IP-адресов несколько раз, заканчивая желанием сохранить структуры внутренней сети скрытыми для внешних источников. Как правило, реализация данного механизма ложится на устройство, которое установлено на границе сети, в нашем случае это промышленный IP-брандмауэр. Принцип работы механизма NAT может быть различным в зависимости от конкретной ситуации. Например, где-то надо скрыть внутреннюю сеть, где-то внешнюю, а в каких-то случаях обе. На примере EAGLE One разберём различные типы NAT (табл. 2).

IP Masquerading

IP Masquerading используется, чтобы скрыть за маской сети внутреннюю структуру сети извне. С помощью механизма IP Masquerading брандмауэр заменяет исходный IP-адрес пакета данных из внутренней сети внешним IP-

адресом брандмауэра. Чтобы определить внутренний IP-адрес, NAT добавляет логический номер порта соединения к информации об адресе (рис. 6*а*).

Добавление указанной информации также дало этому 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 известен только внешний IP-адрес брандмауэра, они не могут настроить коммуникационное соединение с устройством во внутренней сети.

NAT 1:1

NAT 1:1 используется, когда необходимо создать идентичные производственные сегменты с одинаковыми IP-адресами, при этом необходимо их подключить 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 (рис. 6*б*). 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 есть возможность объединения путём создания резервированного L3-соединения. При этом два физических устройства образуют виртуальный NAT-маршрутизатор с высокой доступностью 1:1. Однако стоит учитывать то, что механизм NAT 1:1 изменяет IP-адреса только в IP-заголовках пакетов.

Инверсный механизм NAT 1:1

Инверсный механизм NAT 1:1 используется, если необходимо, чтобы устройства из внутренней сети обменивались данными с устройствами из внешней сети, как если бы устройства из внешней сети находились во внутренней сети.

Для реализации механизма 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

Механизм Double NAT, известный также как Twice NAT, используется, если необходимо, чтобы устройства во внутренней сети обменивались данными с устройствами во 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 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 и IP-адрес назначения на IP-адрес внешней сети.

Port Forwarding

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 (рис. 6*в*). При этом устройство из внешней сети адресует пакеты данных конкретному порту с внешним IP-адресом брандмауэра. Пакеты данных с разрешённым исходным IP-адресом, который брандмауэр получает по определённому порту, перенаправляются брандмауэром на порт внутреннего устройства в сети, введённого в таблицу NAT. Отсюда и название Port Forwarding. Также 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 удалённого обслуживания ПК в производственном секторе.

Защищённые соединения

Создание защищённых соединений является очень нужным и востребованным механизмом. Возможность построения канала связи, который будет обладать дополнительной защитой, между разными объектами инфраструктуры промышленного предприятия позволяет без опасения обмениваться информацией и при необходимости получать доступ к нужным устройствам.

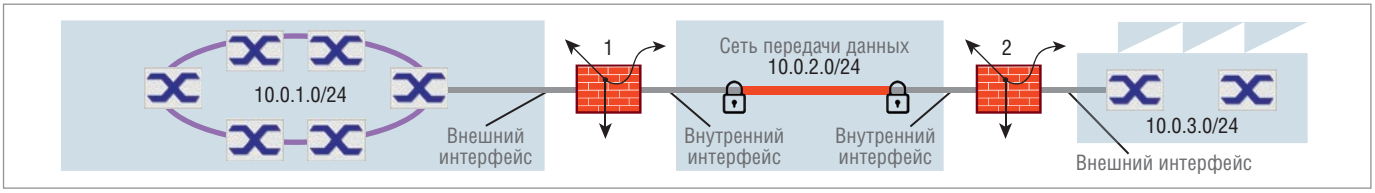

Рис. 7. Защищённое соединение на основе VPN-туннеля: 1, 2 – промышленные брандмауэры

Примером может служить организация канала связи между головным офисом компании и производственным кластером предприятия, которые могут быть расположены на значительном расстоянии. Обычно данная функция реализуется посредством создания виртуальной частной сети (Virtual Private Network, VPN) между двумя устройствами. Фактически это часть общедоступной сети, которая используется для передачи данных. Особенность VPN, как следует из термина "private", заключается в том, что соединение закрыто от общедоступной сети. Создание защищённого соединения посредством VPN позволяет защитить данные от шпионажа, фальсификации и других атак от внешних источников. В промышленной среде VPN, как правило, используется для соединения двух секций предприятия друг с другом через общедоступный Интернет. Для реализации в промышленном брандмауэре EAGLE One используются следующие механизмы и протоколы.

IPsec – Internet Protocol Security

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 в себя следующие аспекты.

Защита целостности соединения гарантирует, что переданные данные являются подлинными, то есть что они исходят от надёжного отправителя.

Шифрование помогает гарантировать, что никто без разрешения не сможет просматривать данные. 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 указанные функции, шифруя полный IP-пакет. Для согласования параметров безопасности, которые должны использоваться между двумя конечными точками VPN-соединения, IPsec предоставляет два режима: транспортный и туннельный.

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

В туннельном режиме два шлюза (в нашем случае данную роль выполняет EAGLE One) удостоверяют подлинность друг 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, подключёнными 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, подключённой к шлюзу, остаются скрытыми.

IKE – Internet Key Exchange

IPsec использует протокол IKE 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. Эти идентификационные данные могут состоять из предварительного общего ключа, который является символьной строкой, ранее переданной по другому каналу связи, а также цифрового сертификата. Сертификат содержит в себе достаточно большое количество информации. Например, сертификаты, основанные на стандарте X.509, содержат:

- информацию о сертификационном органе;
- срок действия сертификата;
- информацию о разрешённом использовании;
- личность лица, которому присваивается сертификат (X.500 DN);
- открытый ключ, принадлежащий данной идентификации;
- цифровую подпись для проверки связи между этим идентификатором и связанным открытым ключом.

Шифрование

Чтобы защитить данные, 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 использовать ключ для кодирования и декодирования сообщений протокола IKE. Далее оконечные устройства согласуют периоды времени, в течение которых происходит обмен ключами, и 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 и сети соединены друг с другом через общую сеть передачи. При этом сегменты производства и управления могут быть географически разнесены между собой. Пример подключения двух сетей через VPN, которые соединены через общую сеть, изображён на рис. 7. Для скрытия внутренних IP-адресов VPN-соединение должно работать в режиме туннеля с использованием всех описанных механизмов IPsec, IKE и шифрования.

Брандмауэр для определённого пользователя

Этот брандмауэр (User Firewall) позволяет управлять потоком данных для

EtherWAN

EX77900

28-портовый управляемый коммутатор L3
Промышленное исполнение
Кольцевое резервирование с быстрым восстановлением (<15 мс)

ПРОМЫШЛЕННОЕ СЕТЕВОЕ ОБОРУДОВАНИЕ

для АСУ ТП, сетей безопасности и видеонаблюдения

- Многопортовые коммутаторы Gigabit Ethernet, в том числе PoE
- Резервирование линий связи для отказоустойчивости
- Оптимизированная передача промышленных протоколов и IP-видео
- Удлинители Ethernet до 2,6 км (cat. 3, 5, телефонный провод)
- Преобразователи сред Ethernet
- Диапазон рабочих температур –40...+75°C для монтажа вне помещений
- Грозозащита Ethernet и VDSL

ED3575

Управляемый коммутатор
6×Fast Ethernet + 2×1 GbE SFP
2×VDSL-удлинитель Ethernet
Резервирование RSTP, α-Ring

EX73900

Управляемый коммутатор L3
12×1 GbE + 4×1 GbE SFP
Резервирование RSTP, α-Ring
Маршрутизация динамическая, статическая

PD3041

Модуль искро- и грозозащиты для VDSL

конкретного пользователя. Можно создать различные правила для каждого пользователя, 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 пользователя и в дальнейшем проверяет пакеты данных для конкретного пользователя на основе правил, определённых для него. Если ни одно из этих правил не применяется, брандмауэр проверяет пакеты данных на основе общих фильтров пакетов. Данная функция позволяет предоставить определённым 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 удалённом сервисном обслуживании устройств, находящихся в промышленном сегменте сети.

Заключение

Обеспечение защиты сети промышленного объекта – достаточно непростая задача, решить которую возможно лишь при помощи грамотно выстроенного подхода. Один из них – это принцип "Defense in Depth", который является многоуровневой и многоступенчатой схемой защиты сети. Согласно данной схеме защита от внешних угроз должна быть реализована при помощи установки промышленного брандмауэра на границе сети, который будет функционировать на уровне L3 (IP-брандмауэр) и пропускать через себя проходящий трафик, анализируя его по установленным правилам. Хорошим примером подобного брандмауэра может служить устройство EAGLE One компании Hirschmann. Брандмауэр EAGLE One отличается компактными габаритами и помимо фильтрации проходящих пакетов может обеспечивать такие функции, как трансляцию сетевых адресов (NAT), защиту от DoS-атак, создание защищённых соединений, шифрование, маршрутизацию и т.д. ●

Литература

1. Understanding Firewall Technology for Industrial Cybersecurity [Электронный ресурс] // Сайт Belden Inc. – Режим доступа : http://www.belden.com/docs/upload/Different-Types-of-Firewalls-WP-EMEA.pdf
2. Зойферт Ф. Концепция защиты промышленного IT-контура на основе брандмауэра Hirshmann серии Eagle 20 // Современные технологии автоматизации. – 2013. – № 3.
3. Configuration Industrial Ethernet Firewall EAGLE One : User Manual [Электронный ресурс] // Сайт Belden Inc. – Режим доступа : https://www.e-catalog.beldensolutions.com/download/managed/pim/2b8c1e5e-d34b-4057-bd0f-2e68d20303db/UM_Config_EAGLE_Rel51_en.pdf?type=attachment

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

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

FASTWEL I/O на объектах газомоторной инфраструктуры

Компания FASTWEL получила положительный отзыв от «Газпром газомоторное топливо» – специализированного подразделения ПАО «Газпром» по развитию рынка газомоторного топлива.

В отзыве отмечается, что в рамках мероприятий по локализации и унификации технических решений, используемых при создании АСУ ТП новых газозаправочных станций, компания «Газпром газомоторное топливо» приняла за стандарт построение систем автоматизации на базе отечественных компьютеров и контроллеров линейки FASTWEL I/O. Дана высокая оценка надёжности, доступности и функциональности решений FASTWEL, отмечается снижение затрат на приобретение оборудования и уменьшение номенклатуры ЗиП. Также в письме говорится, что с начала 2015 года в эксплуатацию были введены объекты (АГНКС), оснащённые АСУ ТП на платформе FASTWEL, в Томске, Южно-Сахалинске, Орске, Перми, Уфе, Нижнекамске, Великом Новгороде, Казани, Зеленодольске, Бугульме, Набережных Челнах, Азнакаево, Лениногорске, Елабуге, Кирове, Санкт-Петербурге и других городах.

В настоящее время для строящихся объектов газомоторной инфраструктуры поставлено ещё 13 комплектов АСУ ТП АГНКС, построенных на базе контроллеров FASTWEL. ●

Семинар ICONICS: индустриальный Интернет вещей в свободной связке с оборудованием

В Москве в Технологическом центре Microsoft состоялся семинар ICONICS, который стал частью мирового турне ICONICS-IoT-World-Tour, проходящего более чем в 10 странах мира. Слушателями семинара стали более 40 человек, а его главный герой – компания ICONICS – представила свою новую технологию IoTWorX, созданную в полном соответствии с тенденциями Industry 4.0 в условиях стремительного проникновения Интернета вещей и облачных решений в системы управления современными предприятиями.

Участники узнали, как с помощью продуктов ICONICS добавить IoT-решение в существующую систему управления предприятием и оптимизировать производственные и бизнес-процессы, в частности, максимизировать энергоэффективность зданий и других объектов, снизить количество поломок и отказов оборудования благодаря аналитическим прогнозам относительно выхода его из строя и т.д. Важно, что презентации иллюстрировались конкретными примерами внедрений ПО ICONICS на объектах самого разного масштаба. При этом открыто демонстрировалась свобода и гибкость подключения ICONICS к любому промышленному оборудованию.

На примере IoT-маршрутизатора ADLINK была продемонстрирована связка подключения IoTWorX к облачному сервису Azure с настройкой и визуализацией через мобильных клиентов. Рассмотрены были также варианты подключения к облачным технологиям сторонних производителей (российских локальных центров обработки данных).

В рамках семинара специалисты обсудили перспективы промышленного Интернета вещей в России, в частности, существующие ограничения законодательства РФ. Представители компаний – системных интеграторов (самая заинтересованная часть аудитории) поделились своими размышлениями о том, какие полезные возможности IoT-решение ICONICS способно привнести во внедряемые ими проекты.

В целом слушатели были единодушны в своей оценке семинара как чрезвычайно полезного мероприятия: они из первых рук получили самую свежую информацию о современных технологиях в сфере индустриального Интернета вещей и сервисов уровня Business Intelligence. ●

Industrial Ethernet высокого напряжения

Коммуникационное оборудование для промышленных условий эксплуатации

УПРАВЛЯЕМЫЙ ПРОМЫШЛЕННЫЙ МОДУЛЬНЫЙ КОММУТАТОР GREYHOUND (СЕРИЯ GRS)

До 28 портов Gigabit Ethernet и до 4 портов 2,5G

HIRSCHMANN

Octopus II – промышленный коммутатор IP67

- Герметичные разъемы M12 100Base-TX/FX
- Резервирование, удаленное управление

HiVision Industrial – ПО для управления промышленной сетью

- Мониторинг и диагностика сети
- Управление большим количеством коммуникационного оборудования

Серия RSP – промышленные коммутаторы МЭК 61850

- Параллельное и «бесшовное» резервирование
- Синхронизация PTP IEEE 1588 v2

EAGLE30-0402 – промышленный межсетевой экран

- Конфигурируемый стационарный сетевой экран и маршрутизатор
- Оптимизирован для промышленных протоколов

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