Управляемые коммутаторы Hirschmann: безопасность превыше всего

Михаил Дормаков

В статье на примере продукции Hirschmann описываются основные возможности управляемых коммутаторов, используемых для обеспечения сетевой безопасности. Рассматриваемые функции и способы их применения помогут оперативному персоналу промышленных предприятий эффективнее обеспечивать защиту промышленного IT-контура.

Введение

Разработка глубоко эшелонированной системы сетевой безопасности является одним из ключевых аспектов создания защищённых промышленных сетей. В отличие от простого одностороннего подхода, например, применения только межсетевого экрана на границе между сетью предприятия и глобальной сетью WAN (Wide Area Network), такой подход предполагает использование нескольких средств и методик обеспечения безопасности, позволяющих создать многоуровневую систему защиты сети.

Какими могут быть первые практические шаги на пути к реализации этой концепции? Прежде всего необходимо провести оценку и классификацию по степени опасности возможных угроз и рисков и разработать систему контрмер для их нейтрализации.

Одновременно с этим нужно проанализировать уже существующие возможности сети, которая должна иметь как минимум межсетевой экран, выполняющий функцию разделения защищённого и незащищённого сегментов сети, а также оценить возможности используемых сетевых устройств – насколько эффективно используются встроенные в них механизмы защиты.

Аппаратная часть современных коммутаторов достаточно функциональна и производительна, что позволяет реализовать во встроенном ПО ещё и функции сетевой безопасности без риска снижения скорости обработки трафика. Подавляющее большинство управляемых коммутаторов имеют встроенные защитные механизмы, способные защитить как сами устройства, так и всю сетевую инфраструктуру, причём это не потребует дополнительных материальных затрат эксплуатирующей организации.

Рассмотрим некоторые подходы к обеспечению сетевой безопасности, доступные для реализации с применением коммутаторов компании Hirschmann (рис. 1) – признанного мирового лидера в производстве надёжного и безопасного сетевого оборудования.

Следует отметить, что все управляемые коммутаторы Hirschmann можно настраивать как при помощи удобного Web-интерфейса, так и через консоль, используя текстовые команды. Настройки графического интерфейса полностью дублируют текстовые команды, и выбор того или иного способа администрирования полностью зависит от предпочтений пользователя.

Новейшие коммутаторы Hirschmann обладают собственной операционной системой реального времени HiOS, в полной мере реализующей все механизмы сетевой безопасности.

Ограничения протоколов

Один из прямых методов защиты сетевых устройств – ограничиться использованием только тех протоколов, которые действительно нужны для управления коммутаторами и сетевой инфраструктурой. В табл. 1 приведены рекомендуемые ограничения по применению ряда протоколов управления, используемых в сетях АСУ ТП. Их применение должно быть ограничено или исключено вовсе для эффективной защиты сети.

Рис. 1. Управляемый коммутатор Hirschmann GREYHOUND 1040 с ПО HiOS 6.0

Таблица 1

Ограничения по применению протоколов управления

Протокол	Ограничение
SNMP	Отключить версии v1 и v2
Telnet	Отключить
HTTP	Отключить
HTTPS	Изменить используемый сертификат
	Изменить порт, используемый по умолчанию
SSH	Использовать алгоритм RSA
	Генерировать новые ключи
	Задать время закрытия соединения после простоя

Ограничение диапазона IP-адресов, имеющих доступ к функциям управления

Следующий уровень защиты сети – ограничить IP-адреса, с которых может осуществляться доступ к управлению сетевым устройством. Для этого следует создать список IP-адресов, которым разрешён доступ к интерфейсам управления устройством, а также определить, какой протокол может быть использован для доступа с каждого из адресов.

На рис. 2 условно показаны разрешённые и запрещённые IP-адреса (выделены зелёным и красным цветом соответственно), а также доступные для каждого из разрешённых адресов протоколы управления.

В этом случае злоумышленник будет вынужден подменить IP-адрес рабочей станции управления для получения доступа к сетевым устройствам, что потребует от него дополнительных усилий и знаний в области IT.

Несмотря на то что использование этих двух приёмов (ограничение по IP-адресу и протоколу управления) кажется элементарным, их совместное применение весьма эффективно для предотвращения нежелательного доступа к сетевой инфраструктуре.

Ограничение доступа персонала

Чтобы исключить риски, связанные с возможностью получения доступа к сетевым устройствам персонала, не имеющего прав или необходимых компетенций для осуществления манипуляций с настройками узлов, следует предоставить каждому сотруднику индивидуальный логин и пароль, а также строго соответствующий его обязанностям уровень доступа. Пользователи с гостевым уровнем доступа имеют доступ только по чтению. Управляющий персонал получает доступ как по записи, так и по чтению конфигурации, однако следует исключить его доступ к управлению функциями безопасности. А вот администратор сети, конечно же, должен получить полный доступ по чтению и записи ко всем функциям управления сетевых устройств, включая функции безопасности (рис. 3).

Это предъявляет особые требования к такому сотруднику, и к подбору персонала на должность администратора сети следует подойти более ответственно.

Персонал должен получить уникальные пароли с высокой стойкостью к подбору. При этом коммутатор позволяет задавать минимальные требования к паролю, которые можно сформулировать следующим образом:

- ограничение минимальной длины;
- минимальное число прописных символов;
- минимальное число строчных символов;
- минимальное число цифр;
- минимальное число специальных символов.

Следует также ограничить максимальное число попыток ввода пароля (рис. 3).

Использование процедуры аутентификации пользователей

Аутентификация – это процедура проверки подлинности пользователя путём сравнения введённых учётных данных (логина и пароля), с сохранёнными в базе данных сетевого коммутатора или сервера аутентификации пользователей. Не следует путать *аутентификацию* с *авторизацией*. Последняя представляет собой процедуру предоставления пользователям определённых прав, в соответствии с политиками, определёнными для каждого из пользователей, и их ролями.

Трудно переоценить важность процедуры аутентификации. В последние го-

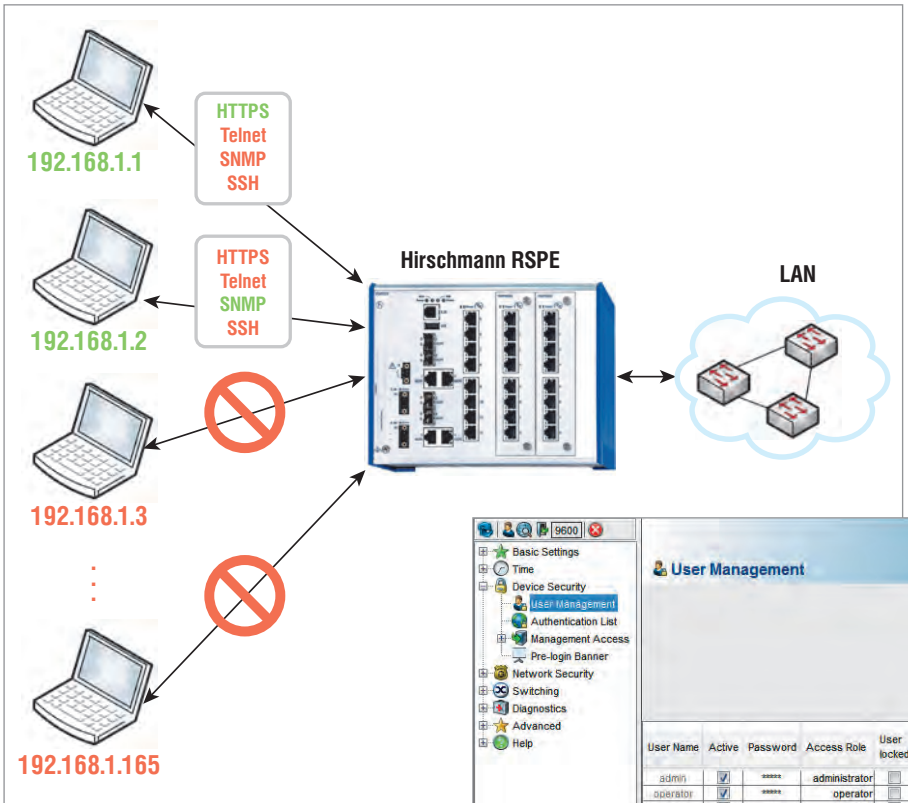


Рис. 2. Визуальное представление правил безопасности

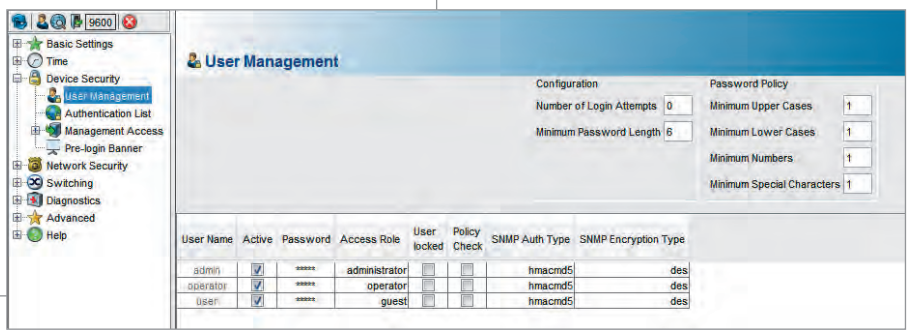
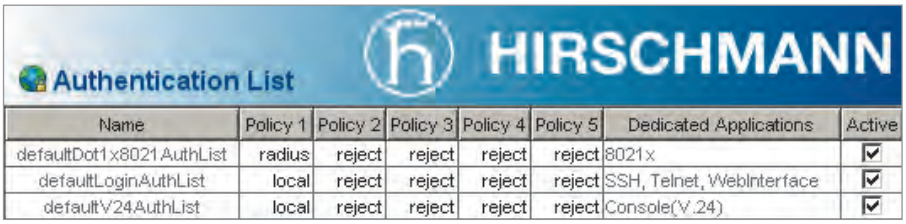


Рис. 3. Страница настроек коммутатора с распределением уровня доступа



Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated Applications	Active
defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	☑
defaultLoginAuthList	local	reject	reject	reject	reject	SSH, Telnet, WebInterface	☑
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	☑

Рис. 4. Списки аутентификации пользователей и политик доступа в коммутаторах Hirschmann

ды число промышленных систем управления с высокой степенью уязвимости существенно увеличилось за счёт устройств, имеющих пароль для доступа к управлению, заданный по умолчанию. Причины, по которым пароль и логин остаются неизменными, – это простота обслуживания, лёгкость управления и восстановления системы при неполадках и интеграции с другими системами. С точки зрения удобства управления, это упрощает жизнь пользователям, но угрожает сетевой безопасности.

Правильным решением будет создание списка имён пользователей и паролей, который может храниться как локально на сетевом устройстве, так и удалённо на сервере авторизации (например, на сервере RADIUS – Remote Authentication in Dial-In User Service), и организация процедур аутентификации и авторизации пользователей (рис. 4).

Рассмотрим процедуру аутентификации на примере стандарта 802.1x [1] и протокола RADIUS [2]. Стандарт 802.1x определяет следующие элементы:

- субъект или клиент – устройство, которое должно получить доступ к сети;
- хозяин системы аутентификации (аутентификатор) – сетевое устройство, например, управляемый коммутатор, которое принимает или блокирует запросы от субъекта;
- сервер аутентификации, который хранит учётные данные и осуществляет аутентификацию пользователя.

Аутентификатор использует информацию от сервера аутентификации (например, RADIUS-сервера), чтобы определить, давать доступ клиенту или нет. RADIUS-сервер даёт доступ на основе проверки учётных данных клиента или его физического (MAC) адреса. Диаграмма, показывающая этапы процесса аутентификации по протоколу RADIUS, показана на рис. 5.

Если использование учётных данных (логина и пароля) невозможно – используется простейшее устройство ввода-вывода без человеко-машинного интерфейса, сетевой накопитель или другое устройство без возможности установки 802.1x-клиента и ввода логина и пароля, – тогда для аутентификации используется MAC-адрес такого устройства. Чтобы облегчить процесс замены вышедшего из строя оборудования, для аутентификации можно использовать лишь первые три байта MAC-адреса, идентифицирующие производителя устройства. Все устройства с интерфейсом Ethernet, производимые определённой компанией, имеют одинаковые значения первых трёх байтов MAC-адреса.

В случае выхода из строя конечного устройства, например ПЛК, его можно просто заменить новым того же производителя из комплекта ЗИП, и оно продолжит работать в сети без ограничений. Если же поставить устройство другого производителя, трафик от него будет блокирован.

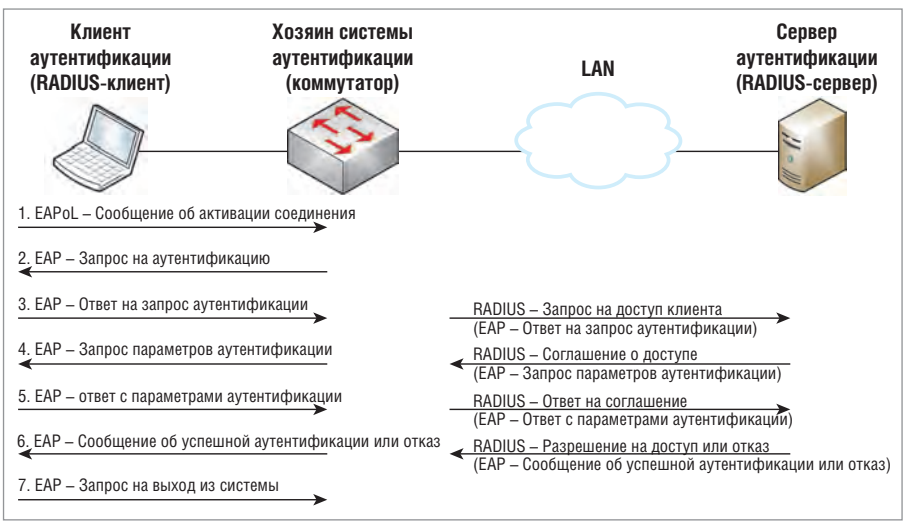


Рис. 5. Аутентификация пользователей в соответствии с 802.1x, протокол RADIUS

Дополнительную степень защиты сетевой инфраструктуры можно обеспечить, если зашифровать файл, в который записывается конфигурационная информация для сохранения на внешнем носителе (переносной флэш-накопитель или адаптер ACA производства Hirschmann). Это несколько усложнит замену коммутатора в случае выхода его из строя, но затруднит доступ к файлу и конфигурационной информации возможному злоумышленнику.

Обнаружение конфликтов IP-адресов

Обнаружение двух одинаковых IP-адресов в сети может означать, что злоумышленник пытается обойти ограничение доступа к сети по IP-адресам или организовать DoS-атаку (Denial of Service – отказ в обслуживании), в результате которой рабочая станция оператора промышленной сети может потерять возможность контроля над сетевым устройством.

Конфликт IP-адресов также может быть результатом ошибки управляющего персонала (человеческий фактор), что само по себе является угрозой безопасности сети.

Есть два способа выявить ситуацию, когда IP-адрес коммутатора совпадает с адресом конечного устройства в сети или терминала управления. Первый – заставить устройство (коммутатор) активно сканировать сеть с целью обнаружения такого же IP-адреса. Второй – настроить устройство на пассивный анализ сетевого трафика с целью поиска устройств с адресом, совпадающим с его собственным IP-адресом. Оба способа реализованы в виде соответствующего алгоритма в коммутаторах Hirschmann, настройка производится на странице Web-интерфейса (рис. 6) или при помощи текстовых команд.

В случае обнаружения другого устройства с таким же адресом коммутатор попытается защитить свой адрес, сделав запрос конечному устройству на смену адреса, который оно использует. Если устройство откажется менять адрес, тогда коммутатор перестаёт использовать конфликтный IP-адрес и выдаёт в систему мониторинга сообщение о конфликте.

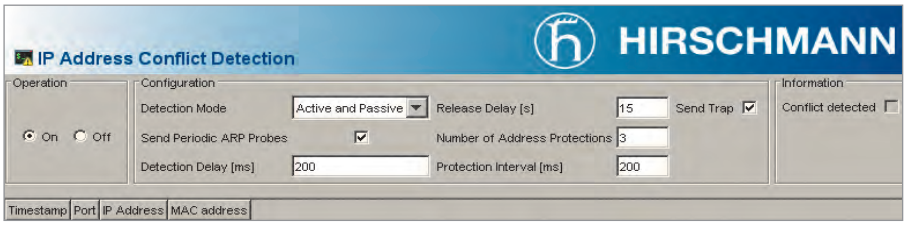


Рис. 6. Настройка механизма обнаружения конфликта IP-адресов

Ограничение доступа к портам коммутатора

Ещё один способ повысить безопасность сети – использовать возможности такого инструмента, как ограничение доступа к портам сетевого коммутатора. Администратор сети создаёт список IP- и MAC-адресов устройств, которым разрешено подключаться к определённому порту. Список может состоять как из набора отдельных адресов, так и из диапазонов (упомянутый диапазон MAC-адресов, задаваемый тремя первыми байтами, либо диапазон IP-адресов, сформированный линейно или при помощи инверсной маски). Использование диапазонов адресов позволяет легко заменять вышедшее из строя устройство на аналогичное либо без труда развёртывать новый сегмент сети. При подключении к порту коммутатора другого устройства или группы устройств (коммутаторов, терминалов, ПЛК и др.) он сверяет адрес нового устройства с имеющимся в памяти списком. В случае обнаружения несоответствия передача данных блокируется, а в систему аварийного оповещения выдаётся сигнал тревоги (замыкается сигнальное реле и/или передаётся SNMP-трап).

Кроме того, не стоит забывать, что наиболее лёгкий способ предотвратить несанкционированное подключение к сети – просто отключить или деактивировать неиспользуемые порты управляемого коммутатора.

Применение средств мониторинга безопасности

В идеальном мире инженер, который делает настройки сетевых устройств, никогда не совершит ошибки. В реальности же при настройке функций безопасности легко недоглядеть и упустить маловажную на первый взгляд деталь. И маленькая оплошность может стать тем заветным ключиком, в котором так нуждался злоумышленник, чтобы получить доступ к сети.

Новейшие управляемые коммутаторы и специальное программное обеспечение для комплексной настройки и диагностики сети (рис. 7) имеют в своём арсенале возможность проанализировать текущие настройки безопасности каждого из устройств и сформировать отчёт с указанием имеющихся недостатков и возможных прорех в сетевой защите.

Так, например, в пакете Hirschmann Industrial HiVision, имеющем удобный графический интерфейс с отображением топологии сети и значков сетевых устройств, можно навести указатель мыши на изображение коммутатора и в окне всплывающей подсказки получить информацию о статусе настроек безопасности. Перейдя во вкладку свойств проекта, можно посмотреть отчёт о наличии тревожных оповещений и их причинах (рис. 8). Даже если вы не специалист по сетевой безопасности, такая

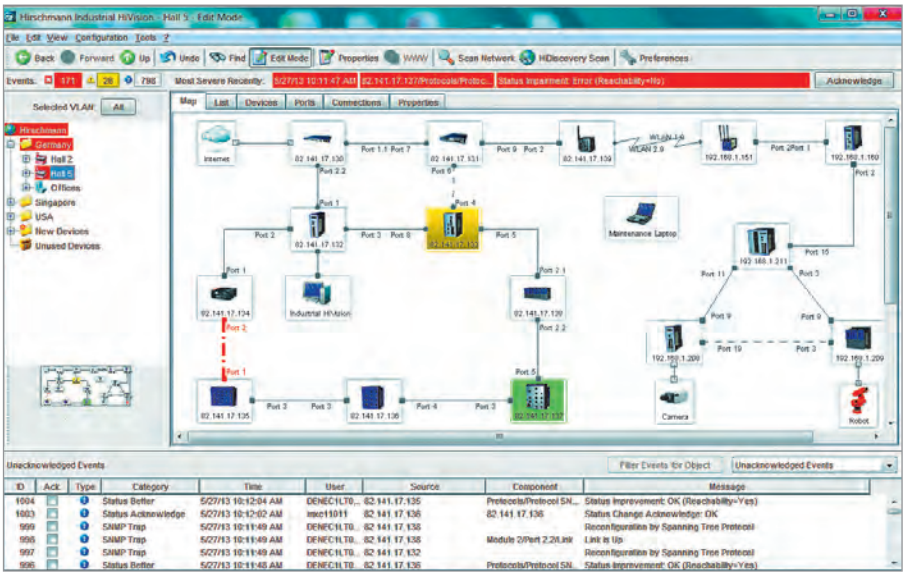


Рис. 7. Специальное ПО для комплексного мониторинга и администрирования сети Hirschmann Industrial HiVision

функциональность позволит вовремя обнаружить слабые места в обороне ещё до того, как ими воспользуется злоумышленник.

Грамотно используя отчёт о состоянии системы безопасности, администратор сети (специалист по информационной безопасности) может вовремя провести нужные настройки и устранить выявленные недостатки.

Предотвращение атак на протокол DHCP

DHCP-серверы (Dynamic Host Configuration Protocol — протокол динамической настройки узла) предназначены для автоматического распределения параметров сети, таких как IP-адреса, по сетевым устройствам. Далее приведён ограниченный список типичных видов атак на сеть, основанных на манипуляциях с протоколом DHCP.

- Подмена DHCP-сервера, добавление в сеть ещё одного сервера DHCP, распределяющего ложные IP-адреса.
- DHCP Exhaustion Attack, или DHCP Starvation – получение злоумышленником всех доступных на текущий момент IP-адресов в рамках подсети, достигается путём присвоения всего пула IP-адресов ложным MAC-адресам, имитированным злоумышленником. Впоследствии вновь подключаемые устройства не могут получить адреса, выдаётся отказ в обслуживании. Далее злоумышленник включает в сеть подменный DHCP-сервер, которому и достаются легальные устройства сети.
- Перехват IP-адреса устройства, уже зарегистрированного в сети.

Противостоять этим атакам можно следующим образом:

- принимать пакеты от DHCP-сервера, подключённого только к доверенному порту;
- сравнивать физический адрес устройства, записанный в таблицу DHCP-сервера, с MAC-адресом отправителя пакета;
- сравнить данные из запросов на получение IP-адреса с недоверенного порта с данными таблицы соответствия параметров соединения (Bindings table).

В таблице Bindings table задаются соответствия между MAC- и IP-адресами устройств сети. В случае перехвата злоумышленником IP-адреса таблица покажет, что MAC-адрес подключённого устройства изменился, перехватчик выдаёт себя за легальное устройство, а в систему аварийного оповещения будет выдан сигнал тревоги.

Некоторые управляемые сетевые коммутаторы обладают собственными механизмами защиты от подмены или перехвата IP-адреса. Например, некоторые коммутаторы Hirschmann с операционной системой HiOS версии L2A имеет функцию IP Source Guard. Суть её работы в следующем. Когда коммутатор получает пакет на недоверенный порт, его параметры сравниваются с занесёнными в таблицу Bindings table. Если IP- и/или MAC-адрес отправителя не соответствует установленному для данного порта, пакет блокируется.

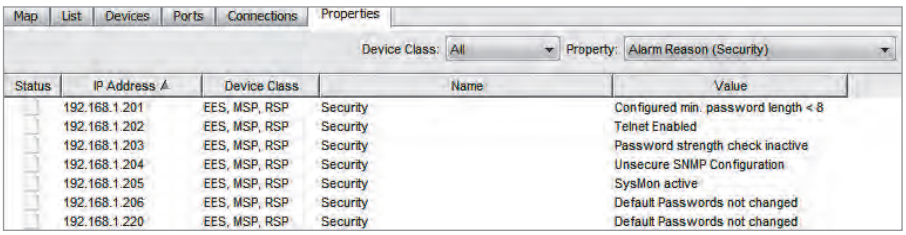


Рис. 8. Пример отчёта о состоянии настроек безопасности сетевых устройств в пакете Industrial HiVision

Применение списков доступа ACL

Списки доступа ACL (Access Control List) используются в коммутаторах и маршрутизаторах для обеспечения избирательного доступа и контроля над трафиком. Они позволяют фильтровать пакеты протокола IPv4 в соответствии с рядом параметров:

- IP-адрес получателя и отправителя пакета;
- MAC-адрес получателя и отправителя пакета;
- порт получателя и отправителя;
- используемый протокол.

Перечисленные критерии фильтрации используются как межсетевыми экранами (рис. 9), так и управляемыми коммутаторами. Однако между этими устройствами есть существенное отличие: только в межсетевых экранах применяется технология SPI (Stateful Packet Inspection – анализ пакетов с отслеживанием состояния).

Суть данной технологии в том, что для анализа и фильтрации трафика, передаваемого в текущий момент времени, используется информация, полученная в ходе предыдущих циклов обмена данными. Например, будет иметь значение, какое устройство выступило инициатором цикла обмена по определённому протоколу, какое устройство передавало данные последним и какое отклонило пакет из-за ошибки.

В отличие от коммутатора с ACL, анализирующего пакет в режиме реального времени, межсетевой экран владеет более полной картиной информационного обмена, позволяющей более эффективно определять допустимость той или иной транзакции.

Таким образом, списки ACL – это лишь один из элементов мозаики под названием «сетевая безопасность» и ни-

Рис. 9. Межсетевой экран Hirschmann EAGLE One с поддержкой технологии SPI

коим образом не заменяют собой межсетевые экраны.

Заключение

Несмотря на то что коммутатор по своей сути продолжает оставаться довольно «глупым» устройством, основное предназначение которого – распределение пакетов информации по адресатам и сбор и передача данных, всё возрастающие функциональные возможности позволяют находить для данного типа устройств новые варианты применения, в том числе и на ниве обеспечения информационной безопасности. Согласно новейшим концепциям сетевой обороны, коммутаторы становятся передовыми бастионами, встающими на пути злоумышленников, а функции защиты сети – эффективным оружием в их арсенале.

Рассмотренные в статье функции управляемых коммутаторов Hirschmann позволят по-новому взглянуть на проблему защиты сети от несанкционированного доступа, реализовать новые проекты и пересмотреть старые с учётом указанных возможностей.

Кроме того, важно изучить функции коммутаторов, которые планируется использовать в проекте, ещё до того, как будет принято решение о применении той или иной модификации. Коммутаторы Hirschmann имеют различные варианты оснащения программным обеспечением, некоторые функции могут отсутствовать в младших моделях.

Следует отметить, что поставляемые коммутаторы не ограничены в своей функциональности и новые функции становятся доступны по мере обновления производителем встроенного ПО коммутатора, поэтому всегда следует уделять внимание своевременному обновлению прошивок. Обновления встроенного ПО коммутаторов Hirschmann доступны для бесплатного скачивания на официальном сайте производителя, а значит, безопасность сети можно улучшить без лишних материальных затрат. ●

Литература

1. IEEE-SA-IEEE Get 802 Program – 802.1: Bridging & Management [Электронный ресурс] // Сайт IEEE Standards Association. – Режим доступа : http://standards.ieee.org/about/get/802/802.1.html.
2. RADIUS [Электронный ресурс] // Википедия. – Режим доступа : http://en.wikipedia.org/wiki/RADIUS.
3. Belden – The Right Signals Blog [Электронный ресурс] // Официальный блог компании BELDEN. – Режим доступа : http://www.blog.beldensolutions.com/.

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