

ПО ТУ СТОРОНУ БРАНДМАУЭРА

ДЭВИД ВЕСТ
(DAVID WEST)

david.west@iconlabs.com

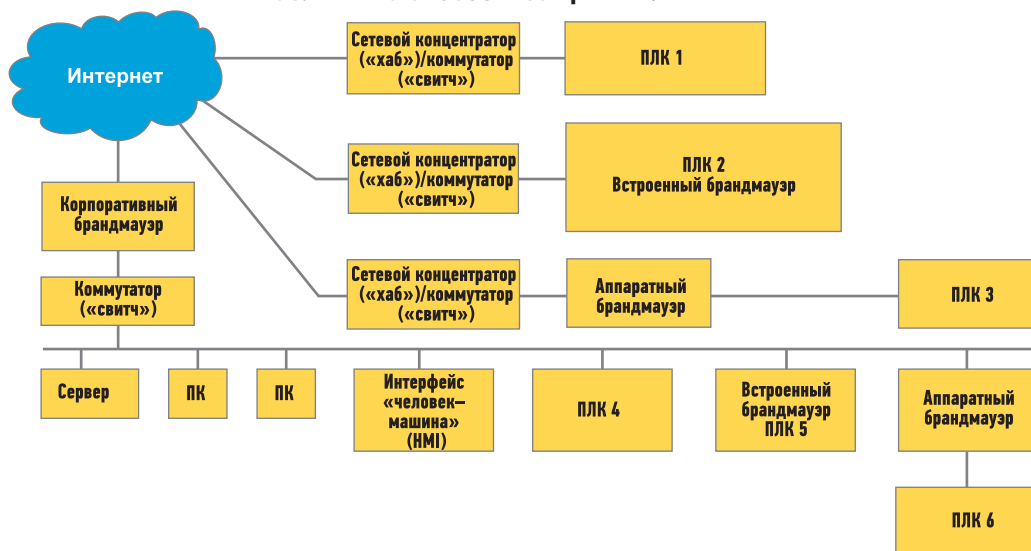
С тех пор как многие промышленные устройства стали уязвимы для хакеров, размещение небольших брандмауэров глубоко в сети (рядом с контроллерами с программируемой логикой или внутри них) — это прямой путь к повышению уровня защищенности.

Хакеры активно атакуют встроенные системы. Пресса часто сообщает о нападениях на автомобильные компьютеры, медицинские устройства и системы SCADA. Вот вопрос, который должен задать себе каждый: «Почему бы мне не установить файрвол?»

Маленькие устройства, соединенные через Интернет, контролируют наши заводы, управляют электросетями, дозируют лекарства с помощью инсулиновых помп и участвуют в нашей жизни другими способами, коих неисчислимое множество. Совсем недавно разработчики встраиваемых устройств даже не думали включать файрволы в свои разработки, дабы обезопасить их от кибератак, считая, что они и так достаточно защищены.

Большинство устройств управления, стандартных или встроенных, разработанных в последние годы, имеют сетевой интерфейс Ethernet, что позволяет подключать их к Интернету. Некоторые имеют защиту паролем и, возможно, протоколы шифрования SSH или SSL, но этого недостаточно. Некоторые устройства не имеют даже такой защиты, в то время как управление осуществляется через ввод имени пользователя и пароля, которые не могут быть изменены.

Различные способы защиты ПЛК



Если бы эти методы были достаточно безопасны, мы бы не узнавали о прорывах защиты из СМИ.

Более старые системы являются и более уязвимыми. В настоящее время устройства зачастую подключены к открытой сети и, как следствие, не имеют защиты. Понимание того, что подразумевается под достаточным уровнем защищенности, устарело и требует модификации. Некоторые, показанные на схеме контроллеры (ПЛК), защищены лучше, чем другие. ПЛК 1 уязвим для атак из Интернета, в то время как ПЛК 2 и 3 имеют локальную защиту против воздействий. ПЛК 4, 5 и 6 находятся под защитой корпоративного файрвола, но атаки могут прийти и со стороны других устройств внутри сети, которые спокойно дойдут до ПЛК 4. Локальные брандмауэры необходимы, и их внедрение упрощает программирование.

РЕАЛЬНЫЕ УГРОЗЫ И «ЛЕКАРСТВА»

Часто разработчики предполагают, что хакеры не будут атаковать устройства, находящиеся глубоко внутри промышленной сети, поскольку преступникам интересны только ПК и сети фирм и компаний. Однако в Интернете без труда можно найти сообщения об атаках на промышленные устройства, что доказывает ошибочность такого подхода. Многие промышленные ПЛК, компьютеры для автоматиче-

ского управления технологическим процессом, а также другие устройства — легкие мишени, и если они будут доступны для вторжения извне, хакеры могут натворить дел.

Разработчики промышленных сетей и встраиваемого оборудования могут взять на вооружение стратегию ИТ-безопасности и применить многослойную методику защиты с использованием брандмауэров и протоколов шифрования. Файрвол обеспечивает предельный уровень безопасности всех устройств, наряду с идентификацией и безопасностью, блокируя атаки, от которых не защитят авторизация и шифрование. Он должен требовать минимум ресурсов, быть эффективным и масштабируемым в широком диапазоне устройств, начиная от маленьких 8-битных систем с простейшей ОС или

даже без нее, заканчивая передовыми многоядерными системами, работающими на ОС реального времени. Персональные файрволы, используемые в офисных приложениях, не удовлетворяют этим требованиям. Брандмауэры для Windows или Linux, если эффективны, то громоздки и не всегда переносимы на встраиваемые или промышленные устройства.

СЕТЕВЫЕ БРАНДМАУЭРЫ ПОМОГАЮТ, НО...

Сетевые или коммерческие файрволы обычно изолируют частные сети от Интернета. Весь трафик между компьютерами внутри Всемирной паутины и частой сети проходит через них. Он настраивается с помощью сетевых правил, чтобы защитить устройства от атак, грозящих из Интернета. Правила, по кото-

Ключевые положения:

- Многие промышленные устройства, установленные глубоко внутри сети предприятия, могут стать мишенью для хакеров.
- Ожидания, что эти устройства в безопасности, так как о них никто не знает, напрасны.
- Небольшие брандмауэры на уровне устройства могут быть настроены таким образом, что обеспечат оптимальную защиту этим устройствам.

рым работает брандмауэр, могут контролировать протоколы, порты и разрешенные IP-адреса. Сетевой экран также может проводить глубокий анализ пакетов, чтобы заблокировать вирусы и вредоносное ПО, атакующее операционную систему. Правильно настроенный, он может обеспечить эффективный уровень защиты против хакеров, DoS-атак, вирусов и зловредных программ.

Однако сетевой экран предназначен для обеспечения защиты внутренней сети с помощью правил для Сети в целом. Требования к связи для отдельно взятого контроллера или какого-либо встроенного устройства глубоко внутри сети очень специфичны, поскольку такие компоненты поддерживают всего несколько протоколов и портов, кроме того, количество IP-адресов, способных связаться с устройством, ограничено. Файрвол, встроенный в такой прибор или смежный с ним, обеспечивает безопасность на уровне устройства с помощью специально подобранных правил, что дает более жесткий контроль.

Файрвол, встроенный в прибор или смежный с ним, обеспечивает безопасность на уровне устройства с помощью специально подобранных правил, что обеспечивает более жесткий контроль.

Атака может также начаться внутри сетевой инфраструктуры. Такие атаки не блокируются сетевым экраном, и устройства без встроенного брандмауэра уязвимы для этих воздействий, поскольку они могут быть инициированы лицами, имеющими доступ к внутренней информации (инсайдерами), или соединениями, которые не проверяются файрволом или же смогли пройти через его защиту. Stuxnet, например, атакует машины в частной сети после проникновения через съемное USB-устройство.

Таким образом, предположение, что контроллер или другое устройство всегда находятся в безопасности под защитой сетевого экрана, должно быть тщательным образом пересмотрено. Сети разрастаются со временем, хакеры учатся обходить файрволы, а способы исполь-

Можно ли с уверенностью утверждать, что встраиваемые устройства всегда будут в безопасности за брандмауэром? И если устройство защищено файрволом, то доверяете ли вы ему настолько, чтобы оставить единственной линией обороны?

зования и включения устройств в сеть меняются. Так возможно ли на самом деле точно утверждать, что встраиваемые устройства всегда будут в безопасности, находясь под защитой брандмауэра? И если устройство защищено файрволом, то доверяете ли вы ему настолько, чтобы оставить единственной линией обороны?

ЗАЩИТА НА УРОВНЕ УСТРОЙСТВА

Файрвол, встроенный в контроллер или отдельный брандмауэр, подключенный к контроллеру, исполняют ряд правил, разработанных для создания безопасной зоны, в которой устройство может спокойно работать. Встроенные брандмауэры становятся все более привычными, поскольку число компаний, понимающих всю важность такого способа защиты производства, неуклонно растет. Правила брандмауэра регулируют допустимые протоколы и порты, которые могут обращаться к устройству. Такие экраны встроены прямо в набор TCP/IP-протоколов устройства и фильтруют пакеты на уровне IP-протокола. Они блокируют нежелательные пакеты данных, попытки несанкционированного доступа и DoS-атаки еще до того, как пройдет аутентификация.

Для создания сетевых правил могут использоваться различные

стратегии. Рассмотрим основные методы фильтрации, их несколько:

1. Фильтрация на основе правил. Каждый пакет сравнивается с набором статических правил, определяющих, отклонить его или пропустить. Все решения принимаются на основе информации, содержащейся в наборе данных пакета.
2. Фильтрация пакетов на основе данных о состоянии соединения (SPI). Информация о состоянии каждого соединения собирается и затем используется для принятия решения.
3. Пороговая фильтрация. Имеется статистика по полученным пакетам и производится слежение за превышением порога, чтобы отсеять лишние пакеты и DoS-атаки.

Первый тип фильтрации создает правила блокирования неиспользуемых протоколов, закрывает ненужные порты и распределяет IP-адреса по «черному» и «белому» спискам. Для некоторых устройств этого достаточно, если хакер пытается завладеть пультом управления извне (с помощью Интернета). В нормальном состоянии контроллер будет связываться только с узким кругом известных ему IP-адресов, поэтому такой способ защиты с помощью списка разрешенных адресов отклонит подобные атаки.

Второй способ защищает против пакетов, полученных с неправильной информацией TCP-состояния, то есть от стандартных интернет-атак. Метод SPI также может быть использован для создания изолированного режима, в котором все соединения иницированы самим контроллером.

Третий вариант является более общим и требует значительных затрат системных ресурсов и времени, но является мощным инструментом для детектирования DoS-атак. ●

Может быть, вы не верите в то, что промышленные устройства — легкая добыча для хакеров. Посмотрите дискуссии студентов, обучающихся по специальности кибер-безопасность в Университете ДеПол (DePaul University), в которых они критически разбирают ПЛК и другие устройства на www.controleng.com/videos. Более подробную информацию по встраиваемым брандмауэрам можно найти на www.iconlabs.com.