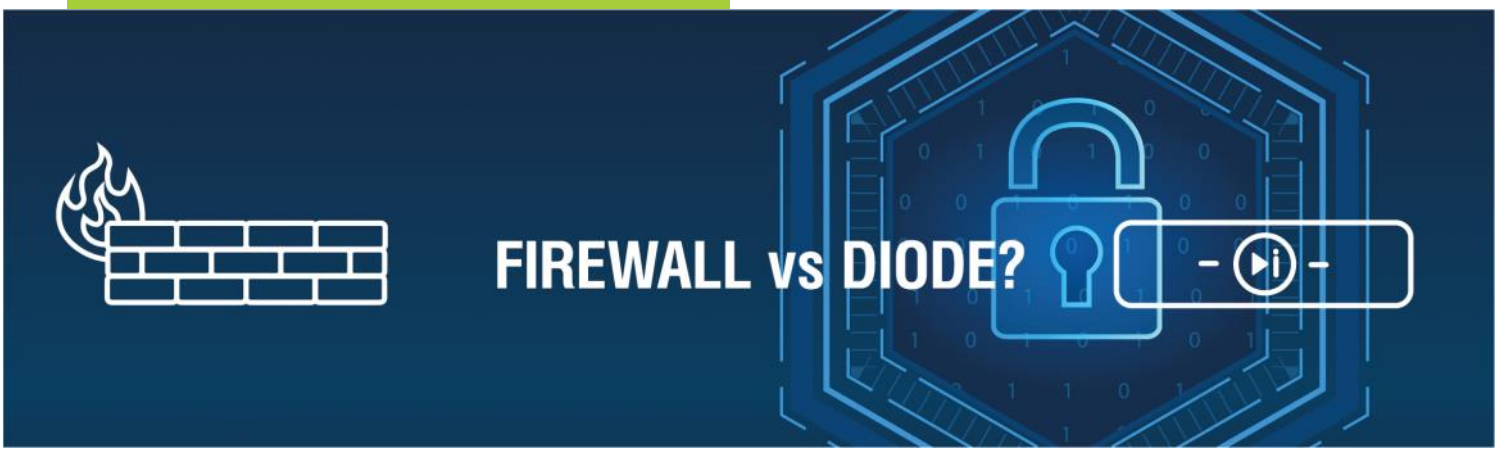


Firewall vs Diode: в чем разница?

При оценке эффективности внедрения устройств однонаправленной передачи данных класса «Diode» их часто сравнивают с широко распространённым классом устройств Firewall. Несмотря на то, что оба этих класса предназначены для защиты сетей, они принципиально отличаются как в технологическом плане, так и в особенностях их применения.

Термин Firewall происходит от названия физического барьера, который устанавливается в зданиях, чтобы препятствовать распространению огня из одной части в другую. Эти барьеры имеют рейтинги огнестойкости по времени и температуре, которые они выдержат, прежде чем неизбежно потерпят неудачу. Ни физический барьер, ни программное обеспечение Firewall не предназначены для долговременной работы/защиты при любых условиях. ПО Firewall для защиты от проникновения в защищаемый сегмент сети также рассчитано на то, чтобы сдерживать определённые типы атак на информационную инфраструктуру.

Устройства однонаправленной передачи данных класса «Diode» изначально разрабатывались для гарантированного предотвращения несанкционированного доступа к системам управления ядерным оружием. Внедрение устройств однонаправленной передачи данных обеспечивает физическое разделение или фактически «воздушный зазор» между сегментами сети, при этом сохраняется возможность передачи данных только в одном направлении. Устройства класса «Diode» изолируют сетевые сегменты, устраняя возможность организации обратного соединения на физическом уровне и обеспечивая гарантированную защиту, основанную на физических принципах.

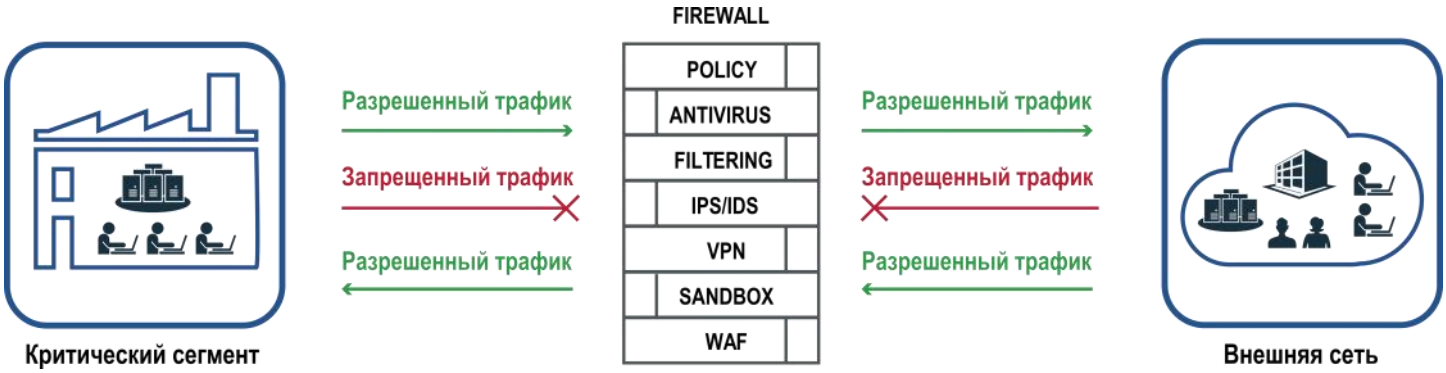
«Diode» обеспечивают гарантированную сегментацию сетей на физическом уровне и за счет применяемых физических принципов гальванической и оптической развязки сетевых сегментов. Такие устройства не подвержены программным ошибкам, эксплойтам нулевого дня или ошибкам настройки. Встроенный физический механизм обеспечения безопасности такого класса устройств не становится менее эффективным со временем. Устройства однонаправленной передачи данных являются основой для построения комплексной системы защиты и обеспечения безопасности объектов критической информационной инфраструктуры (КИИ). Они обеспечивают аппаратную защиту сетей промышленных объектов и объектов ТЭК. Эталонная архитектура представляет собой комплекс решений, в котором интеграция технологической и корпоративной сети реализуется только через однонаправленные шлюзы, а не через межсетевые экраны. Такая архитектура позволяет полностью исключить возможность удаленного доступа к критическому объекту.

AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

Firewall (межсетевой экран)



Современные Firewall предоставляют возможности гибкой настройки, эффективны для замедления проникновения в защищаемый сегмент и для ограниченного предотвращения определенных классов угроз и атак, но не гарантируют стопроцентную защиту от проникновения.

На практике существует большое разнообразие атак, позволяющих преодолеть защитные механизмы Firewall, причем успех определяется принципиальной возможностью двухстороннего взаимодействия сегментов. Например:

- фишинг (отправка специальным образом сформированных электронных писем, манипулирование сотрудниками с целью получения их учетных данных, загрузки вредоносного ПО);
- взлом веб-приложений (эксплуатация уязвимостей с целью получения несанкционированного доступа в периметр защищаемых сетей);
- компрометация домен-контроллера (атака на ключевые узлы ИТ-инфраструктуры, создание фиктивных учетных записей с привилегированным доступом);
- атака через клиентское ПО (компрометация на уровне клиентского промышленного ПО, в том числе установленного у третьих лиц, с целью получения несанкционированного доступа к узлам технологических сетей).

Современные и хорошо спланированные компьютерные атаки указанных выше категорий относительно беспроблемно преодолевают средства защиты в виде программного обеспечения, в том числе Firewall, системы криптографической защиты, системы обнаружения вторжений, антивирусы, и др.

Кроме того, всегда существует возможность ошибок настройки программных решений класса Firewall со стороны обслуживающего персонала и служб технической поддержки, в таком случае банальная халатность может привести к колоссальному ущербу.

Несколько лет назад Firewall были фактически единственной доступной технологией, способной защитить наиболее критические объекты сети и отделить их от открытых сетей. Когда на практике требовалось получить информацию с защищаемого объекта в реальном времени, единственным решением было обеспечить прямую сетевую связность, использовать межсетевые экраны и аналогичные средства защиты и верить в надежность принятых мер. Однако современные компьютерные атаки демонстрируют способность планомерно и эффективно обходить многие средства обеспечения безопасности, в том числе межсетевые экраны.

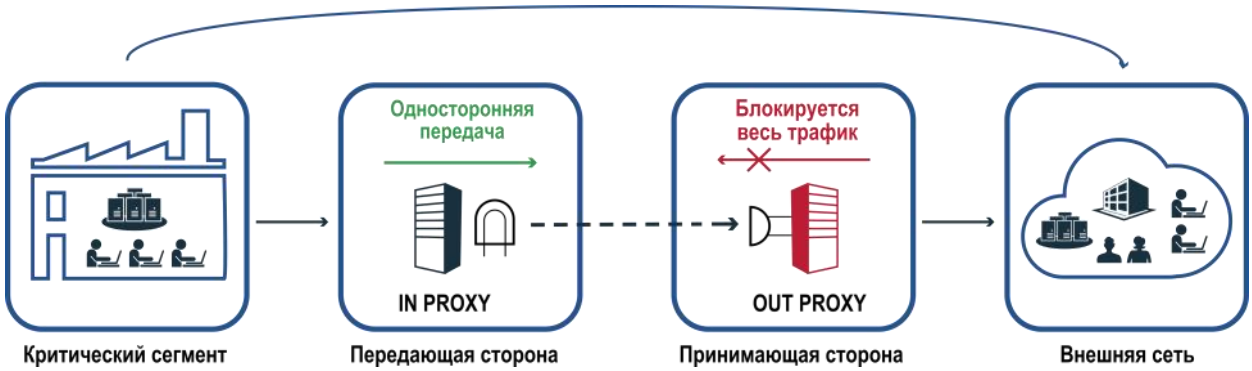
Объекты КИИ могут выполнять сегментацию своих технологических сетей с использованием Firewall, обеспечивая их применение в сетях одного уровня доверия и критичности. При этом точки сопряжения с открытыми и корпоративными сетями защищаются устройствами однонаправленной передачи данных класса Diode. Таким образом, получая эшелонированную защиту технологической сети, объекты КИИ существенно повышают свою безопасность, исключая возможность компьютерных атак и распространения вирусной активности из открытых сетей и сети Интернет.

AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

Устройства однонаправленной передачи данных Diode



Устройства однонаправленной передачи данных класса Diode были разработаны для физического разделения сетей в условиях сохранения канала передачи информации. Как уже отмечалось выше, самые сложные атаки могут использовать согласованную тактику для преодоления современных систем защиты: подбор паролей, взлом многофакторной аутентификации и даже использование методов социальной инженерии. Однако, преодоление «физического разрыва» в диоде с помощью «информационных инструментов» остается невозможным. Устройства класса Diode были предназначены для защиты наиболее важных и критичных сегментов информационной, технологической и военной инфраструктуры, и до сих пор они остаются одним из самых эффективных инструментов обеспечения информационной безопасности.

Устройства однонаправленной передачи данных позволяют обеспечить безопасную интеграцию технологической и корпоративной сетей, а также непрерывный мониторинг функционирования технологической сети из других сегментов, в том числе возможность реагирования на инциденты со стороны служб SOC и NOC. Применение однонаправленных шлюзов для решения задач информационной безопасности обеспечивает конечным потребителям прозрачность требуемых данных, не внося какие -либо существенные сетевые задержки в процесс доступа к информации. При этом исключаются уязвимости, которые, как правило, сопровождают построение архитектуры на основе межсетевых экранов и программных средств защиты.

Решение АМТ-ГРУП

АМТ-ГРУП предлагает устройства однонаправленной передачи данных в рамках линейки продуктов **InfoDiode**. Устройства этой линейки обеспечивают замену межсетевым экранам или дополняют решения, построенные с использованием Firewall, гарантируя надежную и безопасную интеграцию технологической и корпоративной сетей.

Сегодня устройства однонаправленной передачи данных класса Diode являются распространенным средством защиты, которое широко используется во всем мире. Фактически эти решения являются передовой практикой, которую рекомендуют к внедрению ведущие эксперты по информационной безопасности, регуляторы и экспертные организации. В современном мире мы, имея эффективное решение в области безопасности, доступное и на российском рынке, должны задать себе вопрос: «какие из наших критических объектов должны быть настолько доступны для окружающего мира, что мы можем позволить себе защищать их только с помощью межсетевого экрана»?

Продукты InfoDiode выпускаются в различных форм-факторах и конфигурациях: аппаратно-программные решения **АПК InfoDiode PRO в базовой и кластерной конфигурации**, **АПК InfoDiode SMART**, аппаратные решения **АК InfoDiode RACK single, АК InfoDiode RACK double** для монтажа в 19” стойку и **АК InfoDiode MINI** в компактной конфигурации в настольном исполнении или для монтажа на DIN-рейку.

AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

Области применения устройств однонаправленной передачи данных Diode

Интеграция технологической и корпоративной сетей

Наиболее распространенным способом применения устройств однонаправленной передачи данных на объектах КИИ является обеспечение безопасной и эффективной интеграции технологической и корпоративной сетей. В таких случаях Diode, как правило, заменяет межсетевые экраны и приложения на пограничных точках между технологической и корпоративной сетями.

Репликация баз данных и передача исторических данных

Diode часто применяется для репликации различных источников данных из технологической сети в корпоративную сеть. Репликация исторических данных, доставка файлов могут быть использованы в сценариях предоставления отчетности, обмена сырыми данными и файлами, обеспечивающими сопровождение процессов отладки и мониторинга. В том случае, когда в технологическом сегменте сети накапливаются данные, которые необходимо предоставлять для анализа пользователям корпоративной сети, установка устройств однонаправленной передачи данных обеспечивает передачу таких данных в корпоративную сеть, где соответствующие пользователи и приложения могут обращаться к ним без какой-либо угрозы для технологической сети и оборудования критической инфраструктуры.

Получение обновлений

В том случае, когда требуется периодическое обновление антивирусных баз, программного обеспечения и получение иных обновлений и сигнатурных баз, важных для обеспечения безопасности технологической сети, Diode, установленный для передачи данных из открытого сегмента сети в технологический контур (то есть, в обратную сторону), обеспечивает эффективное решение этой задачи. Такое архитектурное решение снижает риски, которые возникают при использовании межсетевых экранов.

Интеграция с программными решениями

Еще одним сценарием передачи данных через устройство однонаправленной передачи данных является передача Syslog трафика на специализированные серверы/системы безопасности. Эти данные используются в целях фиксации событий в SIEM системах, специализированных системах обнаружения вторжений и изменения сетевой топологии, функционирующих в рамках корпоративных SOC, NOC центров.

Мониторинг и контроль функционирования оборудования объекта защиты

Контроль функционирования оборудования

На значительном количестве объектов КИИ и промышленности существует потребность в поддержке функционирующего оборудования со стороны поставщиков и производителей. Для этого, в том числе, могут использоваться специализированные средства мониторинга и диагностики, производимые самим производителем / поставщиком. Применение устройств класса Diode решает эту задачу путем развертывания решения, которое может реплицировать серверы управления и данные из критически важного сегмента сети в сеть DMZ поставщика/производителя. DMZ подключается к центральной системе управления поставщика, чаще всего через VPN. Реплики, передаваемые в DMZ, могут являться точными копиями систем завода и обеспечивать поставщику/производителю полную прозрачность состояния оборудования.

Визуальный мониторинг

Часто возникает потребность осуществлять визуальный мониторинг процессов, происходящих внутри объекта КИИ. Это может быть запись с камер видеонаблюдения или визуальный контроль действий операторов во внешнем ситуационном центре.

AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru