АРХИТЕКТУРА СРЕДСТВА ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

Р. А. Румас[1], **Ю. И. Воротницкий**[2]

[1]Оперативно-аналитический центр при Президенте Республики Беларусь,
[2]Белорусский государственный университет, Минск, Беларусь
E-mail: rra@oac.gov.by

В докладе предложена архитектура аппаратно-программного средства, обеспечивающего однонаправленную передачу данных в компьютерных сетях. Предлагаемая архитектура обеспечивает физическую развязку источника и приемника данных и ориентирована на использование стандартных протоколов.

Ключевые слова: *компьютерная сеть, однонаправленная передача данных, системная архитектура*

Стандартным средством защиты сегментов компьютерных сетей являются межсетевые экраны, работающие на различных уровнях иерархической модели OSI. Они могут анализировать сетевые пакеты вплоть до прикладного уровня, выполнять функции средств предотвращения вторжений, потоковых антивирусных программ, систем DLP и др. Однако даже самые мощные межсетевые экраны не могут гарантировать стопроцентную защищенность сетевых сегментов. Причинами этого могут быть наличие уязвимостей используемого на них программного обеспечения, действия персонала (например, некорректные настройки), перехват учетных данных для доступа к администрированию экрана и т. п. Проблема становится особенно серьезной, если межсетевой экран должен защищать особо критичные сегменты сети [1].

В ряде случаев проблему компрометации межсетевых экранов позволяет решить использование однонаправленных шлюзов, обеспечивающих гарантированную передачу данных только в одном направлении за счет физической развязки между интерфейсами входа и выхода. Тогда, даже если злоумышленнику каким-либо образом удастся захватить полный контроль над однонаправленным шлюзом, работающим на передачу информации из защищаемого сегмента, он не сможет в него проникнуть. Такая однонаправленная передача данных применяется для безопасной передачи информации, например файлов, журналов событий, почтовых сообщений, промышленных протоколов, обновлений программного обеспечения (далее – ПО).

Еще один сценарий применения однонаправленных шлюзов – это одновременная выгрузка и загрузка данных. В этом случае обеспечивается

двунаправленное взаимодействие между сегментами посредством двух однонаправленных шлюзов, один из которых работает на прием, а другой – на передачу данных. Злоумышленнику в случае захвата одного шлюза придется пытаться получить доступ и ко второму однонаправленному шлюзу, что существенно усложняет его задачу. Таким образом, данный сценарий также превосходит по уровню защищенности традиционные схемы с межсетевым экраном на периметре.

Для реализации однонаправленного шлюза на канальном уровне модели OSI источнику и приемнику информации необходимо адресовать пакеты согласно уникальным идентификаторам, называемыми MAC-адресами (Media Access Control). Предварительно по протоколу ARP (Address Resolution Protocol) необходимо обменяться информацией для установления соответствия MAC-адреса и IP-адреса компьютера, с которым необходимо взаимодействовать [2]. Однако при однонаправленном канале передачи данных обмен информацией произведен не будет. Одним из способов решения данной проблемы является установление статического соответствия MAC-адреса и IP-адреса на устройстве-отправителе.

Для работы на сетевом и транспортном уровнях модели взаимодействия OSI при однонаправленной передаче данных необходимо использовать протоколы без установления логической связи, которая подразумевает двунаправленное взаимодействие. Протокол IP на сетевом уровне является протоколом без установления логической связи [3]. При использовании транспортных протоколов следует выбрать UDP, который является дейтаграммным протоколом, реализующим так называемый ненадежный сервис по возможности, который не гарантирует доставку сообщений адресату, но обеспечивает работу без необходимости предварительного сообщения для установки специальных каналов передачи [4]. Для реализации передачи данных можно воспользоваться, например, Unix утилитой NetCat, позволяющая устанавливать соединения TCP и UDP, принимать данные и передавать их [5].

Требуемую функциональность аппаратно-программного средства однонаправленной передачи данных обеспечивает предлагаемое архитектурное решение (рис. 1), включающее 2 медиаконвертера, 2 прокси-сервера, оптический разветвитель (сплиттер).

Медиаконвертеры имеют один Ethernet интерфейс и оптический интерфейс, представленный двумя оптическими модулями: TX – фотопередатчик, RX – фотоприемник. Разделение оптического интерфейса медиаконвертера на два модуля гарантирует физически однонаправленную передачу при использовании со стороны-отправителя TX-модуля, а на стороне-получателя – RX. Наличие активной (по умолчанию) функции LLR

(Link Loss Return) говорит о том, что передатчик оптического порта (TX) конвертера выключается, если приемник (RX) не получает сигнала. Следует отметить, что для работы в данном режиме необходимо наличие оптического разветвителя (сплиттера) для организации передачи сигналов на RX-модуль стороны-отправителя.).

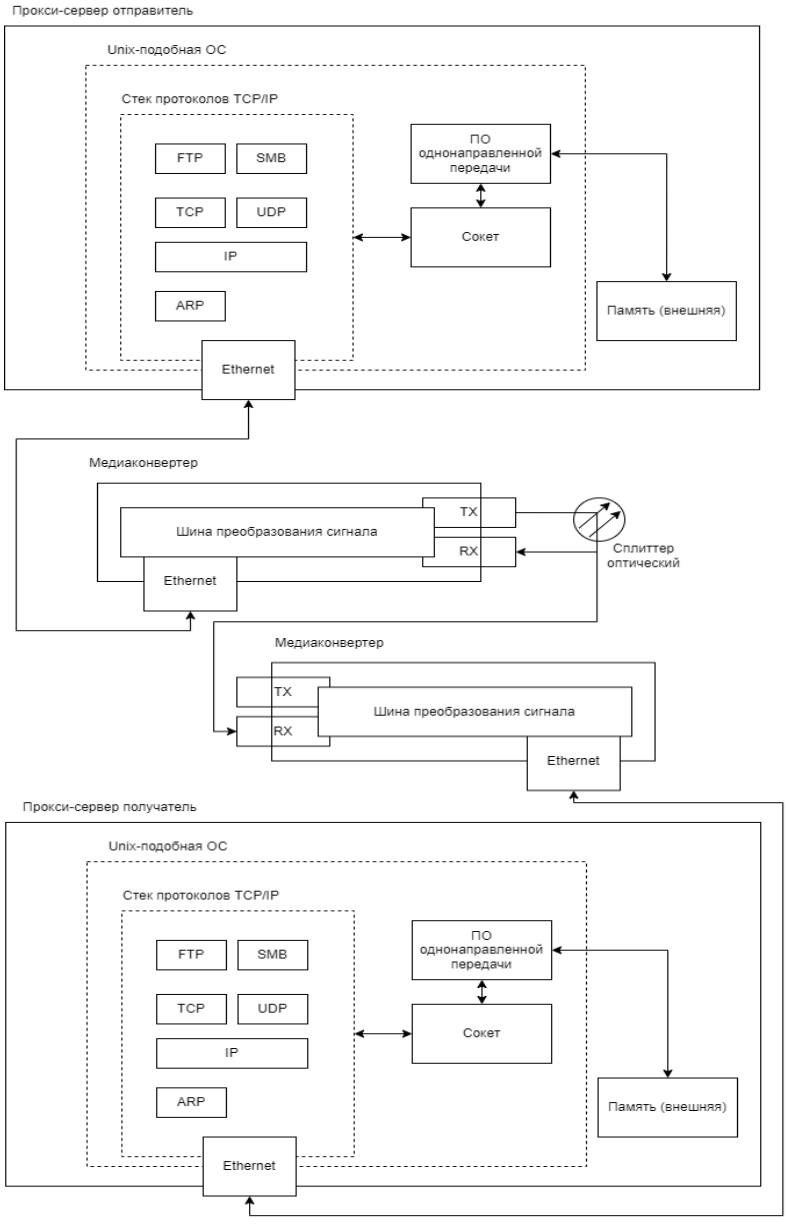

Рис. 1. Архитектура аппаратно-программного средства однонаправленной передачи в компьютерных сетях

Прокси-сервер отправителя и прокси-сервер получателя обеспечивают однонаправленную передачу данных, например файлов, работая на транспортном уровне UDP модели OSI через медиаконвертеры следующим образом:

1. Прокси-сервер отправителя получает файлы данных из открытой сети посредством двунаправленного взаимодействия и протоколов SMB, FTP, SFTP и т. д.

2. Ввиду отсутствия двунаправленного взаимодействия между прокси-сервером отправителя и прокси-сервером получателя, необходимо организовать статическую ARP-запись на стороне-отправителе.

3. ПО на стороне-получателе постоянно прослушивает порт на определенном IP-адресе и ожидает приема UDP-дейтаграмм, преобразуя их в исходное сообщение (файлы данных) и сохраняя их в памяти.

4. ПО на стороне-отправителе постоянно проверяет наличие файлов данных в памяти и при их наличии начинает процесс однонаправленной передачи на заранее настроенный IP-адрес и порт получателя через SOCKET, который, в свою очередь, работает по транспортному протоколу UDP.

5. После передачи на стороне-получателе проверяется контрольная сумма переданных файлов данных по предварительно переданной информации о контрольной сумме от отправителя.

Достоверность передачи обеспечивается путем избыточности (многократной передачи) и проверки каждый раз контрольной суммы.

После передачи и успешной проверки контрольной суммы на стороне-получателе, клиенты из закрытой сети (сети ограниченного взаимодействия) получают переданные файлы данных посредством двунаправленного взаимодействия и протоколов SMB, FTP, SFTP и т. д.

Таким образом описанная архитектура аппаратно-программного средства однонаправленной передачи данных позволит реализовать устройство, которое обеспечит безопасное взаимодействие информационных систем с разной степенью конфиденциальности и гарантирует доставку данных за счет избыточной передачи данных.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2021 [Электронный ресурс]. – Режим доступа: https://ics-cert.kaspersky.ru/publications/reports/2022/03/03/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2021/. – Дата доступа: 01.04.2022.
2. RFC 826: Address Resolution Protocol [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc0826.txt. – Дата доступа: 20.04.2021.
3. RFC 791: Internet Protocol [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc0791.txt. – Дата доступа: 20.04.2021.
4. RFC 768: User Datagram Protocol [Электронный ресурс]. Режим доступа: https://www.ietf.org/rfc/rfc0768.txt. Дата доступа: 20.04.2021.
5. The GNU Netcat Project [Электронный ресурс]. – Режим доступа: http://netcat.sourceforge.net/. – Дата доступа: 20.04.2021.