УДК 004.056.5 **Технические науки**

Митрошина Екатерина Валерьевна, *студентка,*
5 курс электротехнического факультета
Пермский национальный исследовательский политехнический университет
e-mail: mitroshina.katya@inbox.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕЖСЕТЕВЫХ ЭКРАНОВ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО - УПРАВЛЯЮЩИХ СИСТЕМАХ

Аннотация: В статье рассматриваются основные функции и свойствами межсетевых экранов. А также проводится сравнительный анализ межсетевых экранов с целью выявления наиболее оптимального класса при построении архитектуры безопасности в РИУС.

Ключевые слова: Межсетевой экран, маршрутизатор, трафик.

Abstract: This article describes the main features and properties of firewall. Also here is conducting a comparing analyses to identify the most suitable class during an architecture security formation ICS.

Keywords: Firewall, router, traffic.

При построении распределенных информационно - управляющих систем (РИУС) особое внимание следует уделять защите сети управления технологическими процессами. Сеть управления отслеживает и контролирует все внутренние узлы. Ключевым элементом защиты периметра сети является межсетевой экран. Применение межсетевого экрана позволяет избежать ряда атак при построении высокопроизводительных, безопасных и надежных систем автоматизации предприятий и корпоративной сети в целом.

Межсетевые экраны (МЭ) – это устройства или системы, контролирующие поток сетевого трафика между сетями, которые используют различные силы и средства обеспечения безопасности. МЭ располагаются между защищаемым внутренним сегментом сети и внешней сетью Интернет, а также могут применяться в средах, которые не требуют подключения к Интернету. Так, например, во многих корпоративных сетях применяют МЭ, чтобы ограничить соединения в пределах внутренних сетей, обслуживая более критичные области, тем самым предотвращая несанкционированный доступ к соответствующим системам и ресурсам [1].

Согласно стандарту NIST Special Publication 800-82 (2 издание) существует три общих класса межсетевых экранов, рассмотрим каждый из них.

1. Межсетевые экраны с фильтрацией пакетов.

Самый основной тип межсетевого экрана называется фильтром пакетов [1]. Пакетные фильтры - это межсетевые экраны, которые функционируют на третьем, то есть сетевом уровне модели OSI и принимают решение о разрешении прохождения трафика в сеть на основании информации, которая находится в заголовке пакета. Распространенность этих межсетевых экранов связана с тем, что именно эта технология фильтрации в большинстве случаях используется в маршрутизаторах с функцией экранирования. Создается специальный набор правил с определенными параметрами, с помощью которых можно задавать достаточно гибкую схему разграничения доступа. При поступлении пакета на любой из интерфейсов маршрутизатора, он сначала определяет, может ли он доставить пакет по назначению и только потом маршрутизатор сверяется с набором правил, проверяя, должен ли он пересылать этот пакет [2].

2. Межсетевые экраны с проверкой трафика «потоком».

Межсетевые экраны с проверкой трафика «потоком» – это те же фильтры пакетов, которые включают параметры данных модели OSI на четвертом уровне, то есть на сетевом уровне. Они определяют, являются ли пакеты установления связи разрешенными, а также оценивают содержание пакетов на транспортном

уровне. Таким образом, в качестве параметров, используемых при анализе сетевых пакетов, могут быть:

– тип протокола (например: TCP, ICMP, UDP);
– номера портов получателей и отправителей (для TCP и UDP трафика);
– другие параметры заголовка пакета (например, флаги TCP-заголовка) [2].

3. Межсетевые экраны прикладного уровня с функциями прокси шлюза.

Этот класс межсетевых экранов проверяет пакеты на прикладном уровне, а также фильтрует трафик по правилам определенных приложений [1]. Межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, например, как Telnet и FTP, с целью защиты ряда уязвимых мест. Подобное приложение называется proxy-службой, а хост, на котором работает proxy - служба, - шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все исходящие и входящие пакеты на прикладном уровне [3].

После того как шлюз приложений обнаруживает сетевой сеанс, он останавливает его и вызывает уполномоченное приложение, необходимое для завершения процедуры. Шлюзы прикладного уровня позволяют обеспечить надежную защиту, так как взаимодействие с внешним миром реализуется через некоторые уполномоченные приложения, полностью контролирующие весь исходящий и входящий трафик [4].

Сравнительный анализ

При выборе межсетевых экранов необходимо учитывать некоторые аспекты функционирования автоматизированной системы управления. Межсетевые экраны должны предоставлять механизмы для соблюдения политики безопасности. Например, блокировать все коммуникации, за исключением специально разрешенных коммуникаций между устройствами в незащищенных локальных сетях и в защищенных АСУ; обеспечивать безопасную аутентификацию всех пользователей, стремящихся получить доступ к АСУ;

обеспечивать авторизацию пункта назначения; записывать информационный поток для мониторинга и анализа трафика и обнаружения вторжений.

Рассмотрим основные группы межсетевых экранов, изученные ранее, и сравним их между собой по нескольким критериям, проанализировав достоинства и недостатки каждой группы:

1) Стоимость и реализация.

Пакетные фильтры имеют небольшую цену и простоту реализации, по сравнению с межсетевыми экранами прикладного уровня. Несмотря на это, межсетевые экраны с пакетной фильтрацией имеют ряд существенных недостатков, а данный критерий сравнения не является определяющим при выборе межсетевого экрана в РИУС.

2) Производительность сети.

Производительность сети играет не маловажную роль при эксплуатации РИУС, так как в АСУ необходимо выполнение требования реального времени. Таким образом, наибольшая производительность сети наблюдается в межсетевых экранах с пакетной фильтрацией и проверкой трафика «потоком», т.к анализируется только заголовок пакета, тем самым скорость передачи пакетов значительно выше, чем у межсетевых экранов прикладного уровня.

3) Анализ трафика.

Так как межсетевые экраны с пакетной фильтрацией анализируют только заголовок пакета, за пределами рассмотрения остается поле данных, которое в свою очередь может содержать информацию, противоречащую политике безопасности. Также пакетный фильтр может пропустить в защищаемую сеть TCP-пакет от узла, с которым в настоящий момент не открыто никаких активных сессий, а межсетевые экраны с проверкой трафика «потоком» такую возможность исключают. В целом, недостаток пакетных фильтров заключается в том, что они не умеют анализировать трафик на прикладном уровне, на котором совершается множество атак - проникновение вирусов, отказ в обслуживании и т.д. Что касается МЭ прикладного уровня, то здесь присутствует возможность анализа

содержимого, однако невозможно анализировать трафик от неизвестного приложения.

4) Аутентификация трафика.

МЭ с пакетной фильтрацией присуща слабая аутентификация трафика, которая осуществляется только на основе адреса отправителя. Текущая версия протокола IP(v4) позволяет без особого труда подменять такой адрес, подставляя вместо него любой из адресов, принадлежащий адресному пространству IP-протокола, реализуя тем самым атаку "подмена адреса" (IP Spoofing). Так как сетевой фильтр не запрашивает у пакета идентификатор и пароль пользователя, ведь эта информация принадлежит прикладному уровню. Тем самым МЭ прикладного уровня позволяет контролировать состояние соединения.

Подводя итоги, можно сделать вывод, что использование межсетевых экранов является неотъемлемой частью в построении архитектуры безопасности АСУ. В среде АСУ, межсетевые экраны наиболее часто устанавливаются между сетью АСУ и корпоративной сетью. При правильной настройке, они могут значительно ограничить нежелательный доступ к хост - компьютерам и контроллерам системы управления и от них, тем самым улучшая безопасность.

При выборе межсетевого экрана нельзя ссылаться в пользу только какого-либо из названных экранов, так как некоторые недостатки одних МЭ являются критичными для РИУС, но с другой стороны благодаря присущим им достоинствам могут лучше справляться с поставленными задачами. Тем самым лучше всего использовать несколько межсетевых экранов, таким образом, выстраивая эшелонированную оборону всей сети. Целесообразно использовать комбинацию из МЭ с фильтрацией пакетов, затем МЭ прикладного уровня. Также по совокупности эта комбинация из МЭ не является дорогостоящей, ведь в большинстве случаев пакетный фильтр встроен в маршрутизатор, расположенный на границе сети.

В заключение стоит заметить, что межсетевые экраны являются необходимым, но явно недостаточным средством обеспечения информационной

безопасности, ведь они обеспечивают лишь первую линию обороны и не способны защитить от ряда уязвимостей.

Библиографический список:

1. NIST Special Publication 800-82 Rev. 2 Guide to Industrial Control Systems (ICS).

2. Современные методы и средства сетевой защиты. Межсетевые экраны. [Электронный ресурс] // URL: http://www.lghost.ru/lib/security/kurs1/theme03_chapter02.htm (дата обращения: 5.11.2016).

3. Классификация межсетевых экранов. [Электронный ресурс] // Журнал сетевых решений. URL: http://www.osp.ru/lan/1999/09/134421/ (дата обращения: 10.11.2016).

4. Межсетевые экраны. Способы организации защиты. [Электронный ресурс] // КомпьютерПресс. URL: http://compress.ru/article.aspx?id=10145 (дата обращения: 11.11.2016).

5. Брандмауэр: понятие, сущность и свойства. [Электронный ресурс] // Библиофонд. URL: http://bibliofond.ru/view.aspx?id=446811 (дата обращения: 5.11.2016).