DOI: 10.17117/na.2015.09.731

Поступила (Received): 17.09.2015

<http://ucom.ru/doc/na.2015.09.731.pdf>

**Карамышева М.С., Колмаков В.С., Бадалов Б.М.
Анализ разработанной подсистемы защиты
телекоммуникационной инфраструктуры
Интернет-провайдера**

**Karamysheva M.C., Kolmakov V.C., Badalov B.M.
Analysis, a security subsystem telecom
infrastructure Internet providers**

В работе представлен, анализ разработки подсистемы защиты телекоммуникационной инфраструктуры Интернет-провайдера. Принцип составления анализа состоит в том, чтобы предотвратить проникновение злоумышленника к информации с любыми целями, а также защитить носителей информации от уничтожения или повреждения и предотвратить утечку информации

The paper presents the analysis of the development of telecommunication infrastructure security subsystem ISP. Manner of the analysis is to prevent intruders to the information for any purpose, as well as to protect the media from destruction or damage and to prevent information leakage

Карамышева Мария Сергеевна

Студент

Северо-Кавказский Федеральный университет
г. Ставрополь, пр. Кулакова, 2

Karamysheva Mariya Sergeevna

Student

North Caucasian Federal University
Stavropol, Kulakov ave., 2

Колмаков Вадим Сергеевич

Студент

Северо-Кавказский Федеральный университет
г. Ставрополь, пр. Кулакова, 2

Kolmakov Vadim Sergeevich

Student

North Caucasian Federal University
Stavropol, Kulakov ave., 2

Бадалов Бадал Мухтар-оглы

Студент

Северо-Кавказский Федеральный университет
г. Ставрополь, пр. Кулакова, 2

Badalov Badal

Student

North Caucasian Federal University
Stavropol, Kulakov ave., 2

В работе представлен, анализ разработки подсистемы защиты телекоммуникационной инфраструктуры Интернет-провайдера. Принцип составления анализа состоит в том, чтобы предотвратить проникновение злоумышленника к информации с любыми целями, а также защитить носителей информации от уничтожения или повреждения и предотвратить утечку информации.

Деятельность Интернет-провайдера заключается в предоставлении доступа к глобальной сети интернет. Существует множество технологий для ор-

ганизации доступа абонентов в интернет: Ethernet, волоконно-оптические линии, беспроводные среды (Wi-Fi, Wi-MAX). Основа разрабатываемой подсистемы защиты телекоммуникационной инфраструктуры Интернет-провайдера состоит в настройке различных списков контроля доступа (Access Control List), которые ограничивают доступ к ресурсам сети интернет. Используют списки доступа для ограничения доступа: кому-то что-то запретить. Списки контроля доступом (ACL) дают большую гибкость, чем стандартный набор полномочий «пользователь/группа/остальные».

Перед проектированием подсистемы был проведен анализ, с целью создания подсистемы защиты телекоммуникационной инфраструктуры Интернет-провайдера требуемые информационные услуги, количества серверов, параметров безопасности, выбор Интернет-провайдера, характеристики серверной. Для реализации подсистемы защиты Интернет-провайдера были выбраны типичные требования к организации телекоммуникационной инфраструктуры: корпоративные сервера, домен Windows, электронная почта, выход в Интернет, ЛВС, IP-телефония, повышенная отказоустойчивость, связь (VPN) с удаленным офисом, дополнительные меры безопасности при работе с конфиденциальными данными.

Рис. 1. Структурная схема организации подсистемы защиты

Принцип работы схемы заключается в следующем, например, одна клиентская машина обращается на маршрутизатор, перенаправляет его на основной маршрутизатор отправляет запрос на роутер, а роутер в свою очередь отправляет пакеты на межсетевой экран, межсетевой экран стоит для защиты серверного сегмента. Серверная часть отправляет на роутер сигнал, и открывает доступ к глобальной сети интернет.

Рис. 2. Схема подключения клиентов к сети интернет-провайдера

На рисунке 2 показано типовое подключение клиентов к сети провайдера услуг. Пользователи локальной сети находятся в выделенном сегменте VLAN (VLAN 10, VLAN 20, VLAN 30). Их подключение в интернет осуществляется через L3 интерфейс. Для управления доступом используется трафик управления и мониторинга, а защита подключения клиентов к сети проходит на канальном уровне с используемой технологией VLAN (802.1Q).

Рис. 3. Схема реализации подсистемы защиты интернет-провайдера

На рисунке 3 представлен исходящий трафик, отправляющийся с интерфейса вовне. Список доступа применяем на входящий трафик, тогда неугодные пакеты не будут даже попадать на маршрутизатор и соответственно, дальше в сеть, либо на исходящий, тогда пакеты приходят на маршрутизатор, обрабаты-

ваются им, доходят до целевого интерфейса и только на нём делятся. Стандартный список доступа проверяет только адрес отправителя. Стандартные ACL рекомендуется ставить как можно ближе к получателю (чтобы не фильтровать больше, чем нужно).

Рис. 4. Схема подсистемы защита телекоммуникационной инфраструктуры интернет-провайдера

Списки контроля доступа являются универсальным и мощным механизмом фильтрации. С их помощью можно определить, кому предоставлять определённые политики, а на кого нет, кто будет участвовать в неких процессах, а кто нет, кого ограничиваем в скорость до 56k, а кого до 56M. На рисунке 4 показана подсистема защиты телекоммуникационной инфраструктуры интернет-провайдера. Клиент попадает в коммутатор проходит первые списки доступа, например, ему предоставляется не ограниченный доступ к сети интернет, затем клиент попадает в межсетевой экран. В межсетевом экране настраиваем списки доступа, кому-то запрещаем доступ к определённому контенту, кому-то разрешаем доступ. Общий сегмент демитаризованной зоны создан для клиента, в том числе есть сервера доступ, к которым можно предоставлять пользователям, фактически клиент может напрямую использовать интернет, либо проникнуть на общий сервер, но сегмент управления пользователь не может использовать так как используется VIP net.

Таким образом проведён анализ разработанной подсистемы защиты телекоммуникационной инфраструктуры интернет-провайдера. Были рассмотрены возможные на сегодняшний день технологии построения сетей интернет-провайдера. Для подсистемы защиты использованы ACL списки контроля доступа, при помощи них можно отфильтровать трафик в сети. Подсистема за-

щиты состоит в настройке различных списков контроля доступа (Access Control List).

Список используемых источников:

1. Сюваткин В.С., Есипенко В.И. WiMAX-технология беспроводной связи: теоретические основы, стандарты, применение. Санкт-Петербург: БХВ-Петербург, 2010.
2. Вишневский В., Портной С., Шахнович И. Энциклопедия WiMAX. Путь к 4G. Изд-во: Техносфера, 2011.
3. Весоловский А., Кшиштоф Н. Системы подвижной радиосвязи. М.: Горячая линия-Телеком, 2012.
4. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. Красноярск: Эко-Трендз, 2010.
5. Маковеева, Шинаков. Системы связи с подвижными объектами. М.: Радио и связь, 2010.

© 2015, Карамышева М.С., Колмаков В.С.,
Бадалов Б.М.

*Анализ разработанной подсистемы защиты
телекоммуникационной инфраструктуры
Интернет-провайдера*

© 2015, Karamysheva M.C., Kolmakov V.C.,
Badalov B.M.

*Analysis, a security subsystem telecom
infrastructure Internet providers*