Secure corporate network to access the web-resources
Kobzeva E.
Защищенная сеть предприятия для доступа к web-ресурсам
Кобзева Е. А.

Кобзева Екатерина Александровна / Kobzeva Ekaterina – студент,
кафедра информационной безопасности автоматизированных систем,
Северо-Кавказский федеральный университет, г. Ставрополь

Аннотация: *в статье анализируются методы защиты сети предприятия для доступа к web-ресурсам, рассматривается модель угроз и объясняется значимость защищенной сети. Также здесь описывается наиболее приемлемый способ, чтобы минимизировать утечку информации и несанкционированный доступ.*

Abstract: *The article analyzes the enterprise network security methods to access the web-based resources, is considered a threat model explains the importance of a secure network. There is also described the most appropriate way to minimize information leakage and unauthorized access.*

Ключевые слова: *распределенная защищенная сеть, методы защиты сети предприятия, конфиденциальная информация, утечка информации, несанкционированный доступ.*

Keywords: *distributed secure network, methods of protecting the enterprise network, confidential information, information leakage, unauthorized access.*

В настоящее время множество предприятий имеют распределенную сеть в пределах одного города или области. В связи с этим осуществляется передача документов и другой конфиденциальной информации через web-ресурсы, например, через электронную почту, но многие пользователи не соблюдают правила безопасности, из-за чего впоследствии осуществляется несанкционированный доступ к web-ресурсам или перехват информации (утечка данных).

Для того чтобы произвести защиту информации предприятия, необходимо создать модель угроз предприятия, таблица 1.

Таблица 1. Модель угроз предприятия

Источник угрозы	**Нарушитель**	**Уровень реализации угрозы**	**Тип объекта среды**	**Угроза безопасности**	**Способ реализации угрозы**
Компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных атак	Хакер	Уровень технологических процессов и приложений	ПО, предназначенное для обработки персональных данных	Нарушение доступности	Атаки «DoS»
Сотрудники предприятия, являющиеся легальными участниками процессов в ИС и действующие в рамках предоставленных полномочий	Технический персонал, имеющий доступ к аппаратному обеспечению	Физический уровень	Физические носители информации, в составе системы хранения данных	Нарушение конфиденциальности	Утрата

После анализа модели угроз выбираем методы защиты сети предприятия для доступа к web-ресурсам. Защищенная распределенная сеть предприятия представлена на рисунке 1.

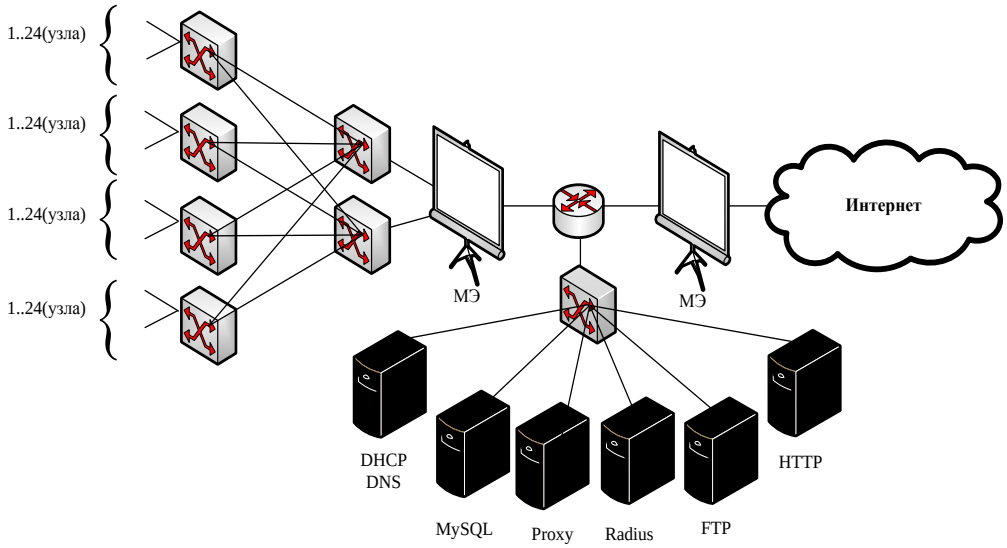

Рис.1. Защищенная распределенная сеть предприятия

К методам защиты сети предприятия для доступа к web-ресурсам относятся:

1. VipNet.

Это программное обеспечение, которое позволяет безопасно передавать данные между другими узлами сети, используя криптозащиту.

Сеть VipNet имеет три основных программных комплекса:

- Vipnet Administrator - осуществляет управление защищенной сети;
- VipNet Coordinator (является сервером) - определяет в реальном времени состояние объектов и доступ к данным в защищенной сети;
- VipNet Client - выполняет функции персонального экранирования, подписи и шифрования.

2. Межсетевое экранирование.

Играет роль фильтра пакетов, проходящих через сеть Интернет [2].

Одним из межсетевых экранов является netfilter, таблица 2.

Таблица 2. Команды работы с межсетевым экраном (брандмауэром) netfilter на примере Linux.

Команда	**Обозначение**
iptables –A OUTPUT –j DROP	запрещает все исходящие соединения по всем интерфейсам
iptables –R OUTPUT 1 –j ACCEPT	разрешает все исходящие соединения по всем интерфейсам
iptables –A INPUT –p icmp –j ACCEPT	разрешает все входящие ICMP пакеты на всех интерфейсах
iptables –I OUTPUT 1 –p icmp –j ACCEPT	разрешает все исходящие ICMP пакеты на всех интерфейсах
iptables –I OUTPUT 1 –p dns –j ACCEPT	разрешает все исходящие DNS пакеты на всех интерфейсах
iptables –A INPUT –i eth0 –o lo –j DROP	запрещает передачу пакетов с интерфейса на интерфейс
iptables –A FORWARD –i eth0 –o lo –j DROP	
iptables –A FORWARD –i lp –o lo –j DROP	
iptables –A INPUT –i lp –j ACCEPT	разрешает все входящие соединения на кольцевом (loopback) интерфейсе
iptables –A INPUT –p tcp --dport 22 –j ACCEPT	запрещает все входящие соединения кроме портов: 22/TCP (ssh), 25/TCP (smtp), 80/TCP (http), 110/TCP (pop3), 143/TCP
iptables –A INPUT –p tcp --dport 25 –j ACCEPT	
iptables –A INPUT –p tcp –j ACCEPT --dport 80	

Команда	Обозначение
iptables –A INPUT –p tcp –j ACCEPT --dport 110	(imap4) и 443/TCP (https) на всех интерфейсах
iptables –A INPUT –p tcp –j ACCEPT --dport 143	
iptables –A INPUT –p tcp –j ACCEPT --dport 443	

IPtables – утилита командной строки, которая является интерфейсом управления работой межсетевого экрана (брандмауэра), а конкретно netfilter для ядер Linux.

В данном случае в качестве фильтрации используются следующие правила:

- INPUT – правила фильтрации входящих пакетов.
- OUTPUT – фильтр исходящего трафика, сгенерированного локально.
- FORWARD – фильтрация маршрутизируемого транзитного трафика.

3. Контентная фильтрация.

Данный тип фильтрации обязательно должен состоять из отдельного сервера, дополнений браузера, утилит.

4. Разграничение доступа.

Клиенты предприятия, которые используют web-ресурсы, должны иметь каждый свою роль. Администратор сети должен распределить доступ к ресурсам, используя ограничение доступа или его разрешение [1]. Для этого наиболее лучшим способом является Radius – сервер, в который администратор заводит учетную запись каждого клиента и определяет ему права. В данном случае это удобно, так как, если сотрудник окажется уволенным, его учетная запись будет просто удалена.

Таким образом, чтобы защитить распределенную сеть предприятия, необходимо изучить возможные угрозы информационной безопасности и определить методы защиты сети. Однако наилучшим способом защитить конфиденциальную информацию – это использовать несколько методов ее защиты. Для этого необходимо распределить права сотрудников, установить фильтры, которые будут определять внутри и вне сети угрозы, а также возможный несанкционированный доступ к важной информации и непосредственно загрузить программное обеспечение, которое будет шифровать переданные данные, что позволит обезопасить сеть от утечки данных.

Литература

1. Кобзева Е. А. Системный анализ методов контроля доступа к web-ресурсам, 2016.
2. Михеев В. А. Доступ к Веб-ресурсам: проблемы контроля, 2013.