СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

УДК 004.056.53

ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Алейникова Д.И., студентка гр.961402

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук

Аннотация. В работе описаны технологии аутентификации пользователей в беспроводных сетях. Изучены основные протоколы аутентификации, авторизации и учёта, их особенности и основные отличия. Проведен анализ использования протокола RADIUS для контроля доступа в беспроводных сетях.

Ключевые слова. Беспроводные сети, контроль доступа, аутентификация, AAA, TACACS+, RADIUS.

В настоящее время технологии беспроводной передачи данных являются очень востребованными, что обусловлено сравнительно невысокой стоимостью и простотой построения беспроводных сетей, связанные с отсутствием кабелей, а также возможностью подключения к сети не только стационарного компьютера, но и других устройств. Беспроводные сети легко масштабируемы и не требуют больших затрат на обслуживание. Следует отметить, что использование беспроводной среды передачи данных приводит к возникновению вопроса о защите передаваемой информации и инфраструктуры сети в целом. Данные передаются по воздушному каналу и для перехвата трафика злоумышленнику достаточно использовать приёмник, установленный в радиусе действия сети, в то время как в кабельных сетях ему необходимо получить физический доступ к кабельной системе или оконечному устройству. При развертывании беспроводной сети следует уделять внимание обеспечению конфиденциальности и целостности передаваемых данных, проверке подлинности беспроводных клиентов и точек доступа.

В предыдущей работе [1] уже были рассмотрены основные принципы построения беспроводной локальной сети и организации VLAN на базе контроллеров Cisco WLC. В данной работе внимание уделяется процессам аутентификации беспроводных клиентов.

Для обеспечения контроля доступа к информационным ресурсам сети через беспроводное подключение можно воспользоваться технологией AAA (Authentication Authorization Accounting), которая основывается на трёх принципах: аутентификация, авторизация и учёт. Аутентификация – проверка подлинности клиента по его идентификатору, таким образом подключиться к сети смогут только разрешенные клиенты. Авторизация – определение и предоставление прав доступа клиента. Учёт – отслеживание действий клиента в сети. Следует отметить, что AAA можно использовать не только для контроля доступа пользователей к сети, но и для дистанционного администрирования сетевых устройств.

Для реализации технологии AAA существуют такие протоколы как RADIUS (Remote Authentication Dial-In User Service) и TACACS+ (Terminal Access Controller Access Control System), которые используются при взаимодействии WLC и AAA-сервера.

Протокол RADIUS был создан независимой группой разработчиков. На транспортном уровне использует протокол UDP, порты 1812 – для аутентификации, 1813 – для учёта. Следует отметить, что процессы аутентификации и авторизации совмещены, существует поддержка учёта действий пользователя в сети. Нет возможности разделить три основных процесса технологии AAA, их обработкой занимается одно устройство. Однако протокол позволяет проектировать гибкую распределенную систему, включающую в себя несколько RADIUS-серверов, которые перенаправляют запросы друг другу в случае отсутствия данных пользователя в локальной базе данных. Протокол поддерживает ограниченное число типов аутентификации (Clear text и CHAP). Характеризуется средней степенью защищенности: в отправляемых пакетах шифруется только поле с паролем. RADIUS позволяет обслуживать только одного клиента в каждый момент времени. Протокол допускает использование брандмауэра между клиентом и сервером, а также технологий трансляции IP-адресов. Это обусловлено тем, что IP-адрес клиента содержится не только в заголовке, но и в теле пакета.

TACACS+ был разработан компанией Cisco Systems, которая периодически выпускает его модификации. На транспортном уровне использует протокол TCP, порт 49. TACACS+ позволяет обслуживать несколько пользователей в каждый момент времени. Протокол предоставляет возможность разделить процессы аутентификации, авторизации и учёта по отдельным серверам.

Поддерживает такие типы аутентификации как: CHAP, ARAP, Clear text. Характеризуется высокой степенью защищенности в силу того, что шифруется всё тело отправляемого пакета. TACACS+ поддерживает аутентификацию внешнего типа: сервер аутентификации отправляет клиенту приложения пароль и клиент самостоятельно сравнивает полученный пароль и введенный пользователем. Такой тип авторизации является уязвимостью протокола. Злоумышленник может скомпрометировать данные пользователя при следующих условиях: на сервере включена функция внешней аутентификации пользователя; сервер аутентификации не производит проверку IP-адресов клиентов или злоумышленник произвел атаку IP-spoofing; злоумышленник узнал некоторое количество логинов пользователей и секретный ключ клиента и сервера, который хранится в открытом виде и на сервере, и у клиента. Решением проблемы может быть отказ от поддержания такого типа авторизации. TACACS+ не допускает наличие брандмауэра между клиентом и сервером, потому что найти соответствующий ключ можно только по IP-адресу клиента, а при работе через брандмауэр IP-адрес клиента будет изменяться по технологии трансляции сетевых адресов. Протокол TACACS+ не поддерживает возможность перенаправления запроса на другие серверы аутентификации.

Таким образом, для аутентификации пользователей в беспроводной сети предпочтительнее применять RADIUS. Используя UDP на транспортном уровне, он работает быстрее TACACS+, которому перед отправкой запроса необходимо каждый раз устанавливать TCP-соединение через процесс трёхстороннего рукопожатия. Так же RADIUS позволяет проектировать гибкую распределенную систему, что предпочтительно в случае, если пользователь захочет авторизоваться в системе, физически перемещаясь по разным регионам. В отличие от TACACS+ протокол RADIUS допускает наличие брандмауэра и применение технологий трансляции сетевых адресов без использования дополнительных настроек.

На рисунке 1 представлен пример построения безопасной инфраструктуры беспроводной сети на базе концепции AAA с использованием программного обеспечения Cisco Packet Tracer.

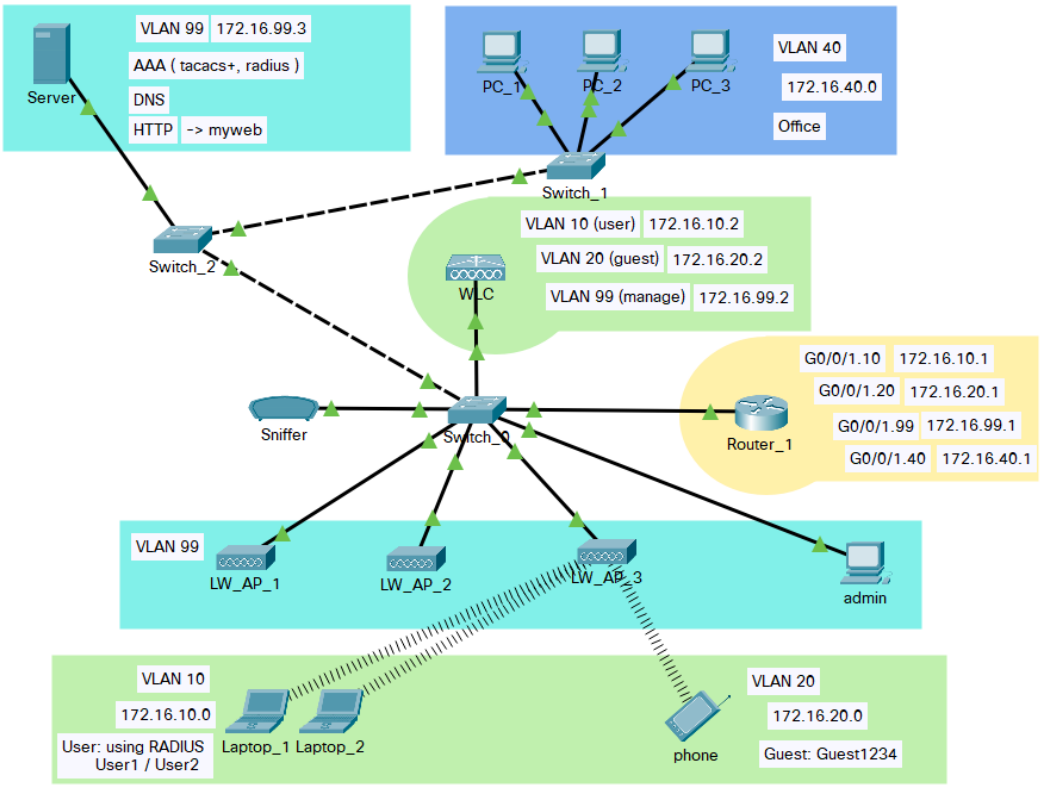

Рисунок 1 – Построение локальной сети в Cisco Pocket Tracer

В моделируемой сети было сконфигурировано два VLAN для беспроводной сети: гостевой и пользовательский, для рабочих организации. Для аутентификации и авторизации клиентов из VLAN для сотрудников организации используется удаленный RADIUS-сервер, а для гостевого – локальная база данных WLC. Рассмотрим процесс взаимодействия WLC и RADIUS-сервера, при попытке пользователя подключиться к сети:

– клиент отправляет запрос на аутентификацию, включающий такие идентификаторы пользователя как логин и пароль;

– точка доступа перенаправляет запрос на адрес WLC;

– WLC получает запрос клиента, формирует запрос аутентификации данного пользователя и отправляет его на RADIUS-сервер. Запрос включает в себя ключ симметричного шифрования, который используется для установления соединения с сервером;
– WLC ожидает ответ в течение определенного времени, по истечению которого, если ответ не был получен, запрос будет отправлен повторно;
– RADIUS-сервер проверяет IP-адрес WLC и ключ симметричного шифрования в своем конфигурационном файле, при соответствии адреса и ключа соединение между устройствами считается установленным;
– RADIUS-сервер проверяет подлинность логина и пароля пользователя, если данные неверны, то отправляет пакет «Доступ запрещен» на WLC, содержащий код ошибки, но если данные верны, то отправляется пакет «Доступ разрешён»;
– на основе полученного ответа WLC предоставляет или запрещает доступ пользователя к сети.
Таким образом, использование в беспроводных сетях протокола RADIUS для аутентификации пользователей на базе технологии AAA является более предпочтительным, в виду гибкости, быстродействия и безопасности процесса аутентификация пользователя посредством RADIUS-сервера.

Список использованных источников:

1. Алейников, Д.И. Принципы построения безопасной инфраструктуры беспроводных сетей на базе контроллеров Cisco WLC / Д.И. Алейникова // Технические средства защиты информации: тез. докл. XIX Белорусско-российской науч.-техн. конф. / редкол.: Т.В. Борботько, [и др.]: Минск: БГУИР, 2021. – С. 15-16.
2. Ettrecap manual [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=tXprJgbEWXg&list=PLQQoSBmrXmrysEaVNia7KVwf85qATIi1V&index=78 – Дата доступа: 01.04.2022
3. Ettrecap manual [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/ru_ru/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html – Дата доступа: 01.04.2022

UDC 004.056.53

AUTHENTICATION PROTOCOLS IN WIRELESS NETWORKS

Aleinikova D.I.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD in technical sciences, associate professor

Annotation. User authentication technologies in wireless networks are described in this research. The basic authentication, authorization and accounting protocols, their features and main differences are studied. The use of the RADIUS protocol for access control in wireless networks is analyzed.

Keywords. Wireless networks, access control, authentication, AAA, TACACS+, RADIUS.