Д. И. Бабицина, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.056.53

РАЗРАБОТКА МОДЕЛИ ЦЕНТРАЛИЗОВАННОЙ СЛУЖБЫ КОНТРОЛЯ ДОСТУПА К КОРПОРАТИВНОЙ СЕТИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ И УСТРОЙСТВ

Аннотация. Статья посвящена разработке модели централизованной службы контроля доступа в корпоративной сети с использованием открытых решений. Предложенная архитектура включает аутентификацию пользователей и устройств и интеграцию с Captive Portal, обеспечивая повышение безопасности инфраструктуры.

Ключевые слова: безопасность сети, централизованная аутентификация, контроль доступа, FreeRADIUS, профилирование устройств.

Введение. Длительное время защита корпоративной сети подразумевала наличие «периметра», отделяющего внешнюю сеть от локальной, в которой могли находиться только доверенные устройства и пользователи. Однако на данный момент кратно выросло число людей, работающих с удаленных и с личных устройств, что увеличивает количество недоверенных устройств в сети. Помимо этого, мошенники за последние годы стали чаще предпочитать быстрое внедрение в сеть с помощью внутренних нарушителей вместо длительного изучения уязвимостей безопасности [1]. Для решения данных проблем предлагается введение в корпоративную сеть компании централизованной службы контроля доступа, которая будет аутентифицировать каждое устройство в сети и пользователей, которые используют их. После успешной аутентификации запускается процедура авторизации с получением соответствующих прав.

Анализ существующих публикаций показал, что большинство исследований сосредоточено на вопросах аутентификации пользователей беспроводных сетей, — при этом другие сегменты инфраструктуры, такие как кабельные и удаленные подключения, остаются недостаточно изученными [2, 3].

Кроме того, значительное внимание уделяется интеграции центров аутентификации с Microsoft Active Directory, в то время как использование открытых решений на базе Linux исследуется ограниченно [4, 5].

Отдельные работы акцентируют внимание на методах аутентификации, связанных с применением небезопасного метода при помощи паролей [6].

Проблема исследования. Из-за обширности темы аутентификации пользователей и устройств на практике компании сталкиваются с недостатком системного подхода и затрудняются в выборе оптимальных программных решений, что приводит к фрагментированной и уязвимой инфраструктуре безопасности.

Цель данного исследования — разработать модель централизованной аутентификации, обеспечивающую систематизированный подход к моделированию центра аутентификации пользователей и устройств.

В ходе работы решался ряд задач:

1. Проанализировать современные технологии, применяемые для контроля доступа в корпоративных сетях;

2. Сформировать перечень применяемых технологий и подходов, которые войдут в итоговую модель;

3. Разработать формировать итоговую модель централизованной аутентификации;

4. Выбрать программное обеспечение с открытым исходным кодом для демонстрации предложенной модели;

5. Настроить виртуальный лабораторный стенд и апробировать работу модели.

Материалы и методы. Для реализации лабораторного стенда в рамках данного исследования была использована среда виртуализации GNS3. В качестве операционной системы на виртуальных серверах и рабочих станциях применялась отечественная операционная система RedOS. В рамках разработанной модели контроля доступа были настроены следующие сетевые сервисы: FreeRADIUS-сервер, OpenVPN-сервер, контроллер домена FreeIPA, а также сервис Captive Portal для обратной связи с пользователями. Для профилирования устройств использовались службы анализа DHCP- и DNS-трафика, что позволяло системе идентифицировать тип подключаемых устройств на основе поведенческих признаков.

Результаты. Для обеспечения аутентификации пользователей и устройств в корпоративных сетях распространенной практикой является использование следующих стандартных служб:

1. RADIUS-сервер, выполняющий функции централизованной аутентификации и принятия решения о предоставлении доступа в соответствии с заданными политиками безопасности;

2. Доменный контроллер, реализующий централизованное хранение учетных данных пользователей;

3. VPN-сервер, предоставляющий возможность защищенного удаленного подключения пользователей.

В современных системах NAC (Network Access Control) широко используется интеграция вышеперечисленных служб. Авторами исследования предлагается расширить данную архитектуру за счет использования следующих компонентов:

1. Внедрение центра сертификации для формирования доверенной инфраструктуры между сервисами, входящими в систему NAC, что обеспечивает проверку подлинности компонентов, безопасный обмен данными и повышение общего уровня защищенности корпоративной сети;

2. Использование Captive Portal в качестве механизма интерактивной обратной связи с пользователем. Решение обеспечивает отображение информации о причинах отказа в доступе, например, при некорректном прохождении аутентификации;

3. Профилирование устройств на основе анализа DHCP- и DNS- проб. Сбор такой информации позволяет формировать профиль конечного устройства на основе сетевого трафика, наблюдаемого при подключении к сети. Накопление и анализ таких профилей обеспечивают возможность отслеживания изменений в поведении устройств и своевременного реагирования при обнаружении значительных отклонений.

Объединив все перечисленные службы, авторами исследования была сформирована модель централизованной аутентификации пользователей и устройств, показанная на рис. 1.

Рис. 1. Модель централизованной аутентификации

При выборе компонентов для построения лабораторного стенда предъявлялись определенные авторами исследования требования. Использованное программное обеспечение должно иметь открытый исходный код для обеспечения возможности его внедрения в инфраструктуру малых организаций без значительных финансовых затрат. Предпочтение отдавалось решениям, совместимым с отечественными операционными системами. Исходя из этого, были выбраны следующие проекты:

1. Для реализации службы каталогов рассматривались отечественные проекты, такие как Ред АДМ и Альт Домен. Проект Ред АДМ находится в стадии активной разработки и на момент исследования не обладал всеми необходимыми компонентами, в частности, встроенным центром сертификации. Альт Домен, построенный на базе Samba 4, в большей степени ориентирован на интеграцию рабочих станций на Windows в Linux-домены. Поскольку целью исследования является создание инфраструктуры, оптимизированной под Linux, был выбран проект FreeIPA, являющийся основой некоторых отечественных решений, как наиболее зрелое, открытое и совместимое с отечественными операционными системами решение;

2. В качестве RADIUS-сервера для реализации модели был выбран проект FreeRADIUS. Среди отечественных решений рассматривался проект Eltex NAICE, однако на момент исследования он находился в стадии активной разработки и не имел стабильной финальной версии. При анализе открытых проектов дополнительно рассматривался OpenRADIUS, однако из-за отсутствия активного развития он был признан недостаточно надежным. В результате был выбран FreeRADIUS благодаря своей высокой гибкости, широкой поддержке стандартов аутентификации, масштабируемости и активному сообществу разработчиков;

3. В роли VPN-сервера авторы решили использовать проект OpenVPN, поскольку он имеет высокую совместимость с отечественными операционными системами, обширную документацию и возможности гибкой интеграции с FreeRADIUS, благодаря дополнительным модулям.

4. Captive Portal был реализован в виде набора собственных скриптов, обеспечивающих обработку запросов пользователей и предоставление им информации о причинах отказа в доступе, которые формируются на основе результатов аутентификации и авторизации, а затем динамически отображаются при сетевом запросе пользователя в браузере. В качестве веб-сервера авторы исследования выбрали angie.

5. DHCP- и DNS-пробы были получены из стандартных обращений клиентских устройств к серверам isc-dhcp и bind9 соотвественно. Из сообщений, полученных по протоколу DHCP, можно узнать следующие характеристики клиента: имя устройства; список запрашиваемых опций, который может отличаться в зависимости от вендора; производителя устройства; уникальный идентификатор клиента, который часто совпадает с его MAC-адресом. Из DNS-запросов фиксируются имена сайтов, к которым обращается устройство при включении для проверки доступности подключения к глобальной сети. Полученную информацию по протоколу DNS необходимо сравнивать с данными DHCP-сервера и сохранять в отдельную базу данных для дальнейшего формирования профиля устройства.

Разработанный на основе указанных выше решений виртуальный лабораторный стенд, показан на Рисунке 2.

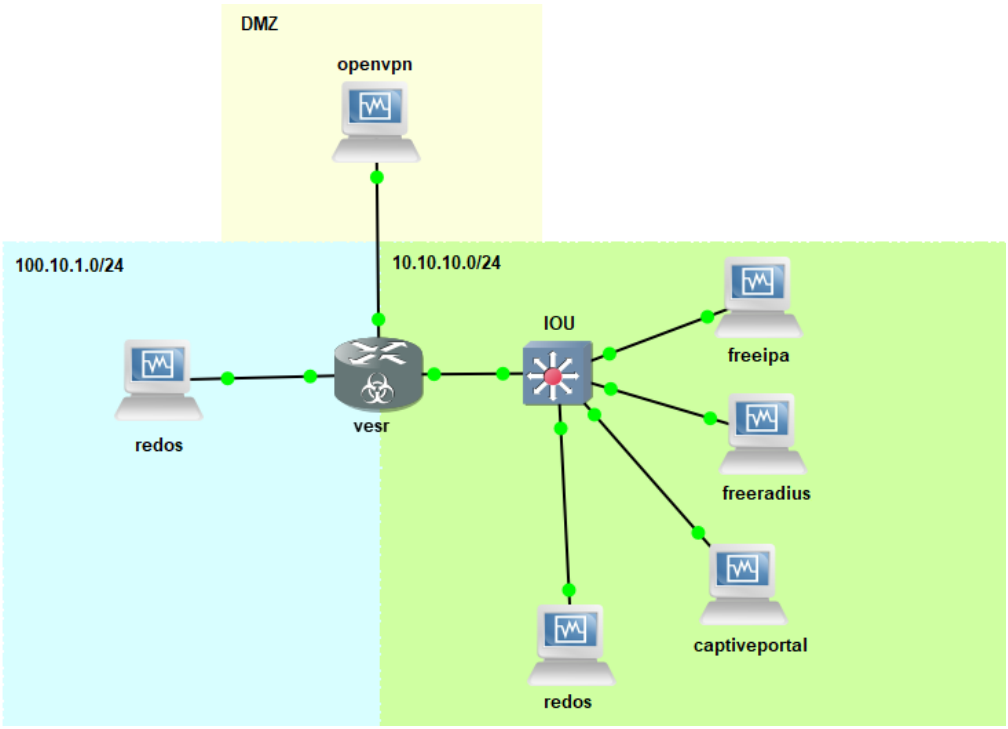

Рис. 2. Лабораторный стенд сети предприятия

Заключение. Таким образом, предложенная авторами модель централизованной службы контроля доступа в корпоративной сети была апробирована на разработанном виртуальном стенде и, благодаря использованию открытых решений, может быть рекомендована к внедрению и тестированию в инфраструктуре реального предприятия. Предложенные решения позволяют повысить уровень безопасности сети и расширить возможности управления доступом.

СПИСОК ЛИТЕРАТУРЫ

1. Аналитический отчет InfoWatch: Россия: утечки информации ограниченного доступа. — Текст: электронный // InfoWatch: официальный сайт. — 2024. — URL: https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-utechki-informatsii-ogranichennogo-dostupa-2023-2024.pdf (дата обращения: 17.04.2025).
2. Тетерин А. Ю. Современные методы обеспечения безопасности в беспроводных компьютерных сетях / А. Ю. Тетерин, И. Г. Бабанин // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения, 21-22 марта 2024 года — Курск, 2024. — С. 163-167.
3. Даньшина А.В. Разработка сервера аутентификации на базе операционной системы Astra Linux / А. В. Даньшина, А. Д. Докшин, М. М. Ковцур // Региональная информатика; информационная безопасность регионов России, 28-30 ноября 2020 года — Санкт-Петербург, 2020. — С. 262-265.
4. Докшин А. Д. Исследование подходов авторизации пользователей беспроводной сети на основе LDAP / А. Д. Докшин, А. В. Даньшина, М. М. Ковцур // Научно-практический электронный журнал Аллея науки. — 2020. — № 3(42) — С. 758-761.
5. Владимиров С. Н. Настройка и использование FreeRADIUS с использованием службы каталогов корпорации Microsoft / С. Н. Владимиров, К. А. Карельская, Н. Г. Михальцов // IX Международная научно-практическая конференция: Информационные ресурсы и системы в экономике, науке и образовании, 29-30 апреля 2019 года. — Тверь, 2019. — С.47-50.
6. Федорченко А. Г. Существующие подходы при идентификации и аутентификации пользователей / А. Г. Федорченко, Я. Д. Драгунов // Научно-технические аспекты развития автотранспортного комплекса, 31 мая 2024 года. — Горловка, 2024. — С. 455-458.