Разработка и внедрение SberNAC

SberNAC

Что это такое и зачем нужен

SberNAC или SNAC - интеллектуальная система контроля доступа, предназначенная для защиты сети на основе профилирования и анализа соответствия политикам безопасности. При каждом подключении конечного устройства или пользователя к сети, SNAC проверяет исходные параметры на наличие необходимых атрибутов и анализирует, какие права доступа необходимо предоставить. Это позволяет автоматически распределять уровень доступа
и предотвращать несанкционированное подключение к ресурсам сети.

SNAC использует передовые механизмы аутентификации, включая собственный RADIUS-сервер, анализирует параметры устройства, позволяет легко интегрироваться с другими система безопасности, создавая многослойную защиту корпоративной сети.

SNAC - это централизованное управление доступом пользователей и устройств, прозрачность администрирования
и уверенность в безопасности информационной среды.

Предпосылки

В рамках эксплуатации разных вендорских продуктов,
во всех из них были выявлены некоторые общие недостатки и ограничения, которые негативно влияли на качество предоставляемых услуг.

— Проблема с производительностью – не справляется с нашими объемами

— Отсутствие возможности кастомизации вендорских продуктов – нам надо больше, чем вендор мог сделать

— Отсутствие возможности интеграции с системами банка

— Закрытость решения – без вендора невозможно качественно поддерживать систему

Финальным триггером отказа стал отказ вендора в поддержке

Требования

Система должна:

- Реализовывать аутентификацию и авторизацию для всех типов подключения
- Поддерживать протоколы Radius и TACACS+
- Иметь возможность легко масштабироваться
- Обеспечивать отказоустойчивость
- Легко и дешево дорабатываться
- Функционал богаче чем был
- Запускаться на всем
- Не требуются платные продукты для работы

Рассматриваемые варианты для создания продукта

Делаем сами
и лучше, чем было

Учитываем опыт решений, с которыми работали и берем от них лучшее

Знаем проблемы и узкие места - исправляем

Делаем тот функционал, которого нам не хватало

Переделать OpenSource FreeRadius
и прочее

Тот же «black box» только бесплатно и без поддержки

То что изначально сделано плохо, хорошо не переделаешь

Купить готовое отечественные решение
Нет готовых решений

Что сделали

как делали

1. Консолидируем сильные стороны решений Cisco и Aruba. Составили описание основного функционала и какие проблемы необходимо устранить

2. Выбрали стэк.
   Golang&React - для сервисов
   GraphQL&gRPC - для взаимодействия
   Postgres&ClickHouse - для хранения

3. Микро сервисная архитектура – возможность делать разные сборки для разных сценариев

4. Разработали свой Radius и TACACS сервер на Golang

5. Реализовали 802.1x и DHCP профилирование, а так же другой полезный функционал

На чем можем работать

технологическая независимость

Платформа

На чем можем работать

Без привязки к вендору и оборудованию. Есть возможность сборки дистрибутива для x86 и RISK

Возможность запуска на разных версиях Linux

Возможность запуска на физических и виртуальных серверах

Работа в режиме standalone или cluster

Сервисы

А здесь вот такой

Отсутствие необходимости в платных решениях для работы системы

Open Source с большим и активным community

Распространенные решения, для упрощения поддержки

Возможности системы

мы уже используем

Поддерживаемые протоколы

Radius – для контроля доступа конечных устройств в корпоративную сеть
TACACS+ - для контроля доступа администраторов к сетевому оборудованию

Портал регистрации

Для гостевых пользователей

Регистрация устройств с подтверждением по смс или звонку.
Возможности настройки длительности гостевой сессии.
Возможность настройки частоты регистрации
Возможность настройки количества регистрируемых устройств

Поддерживаемые методы для протокола Radius

- Authorize Only
- Call-Check
- Login-User с поддержкой LDAP
- EAP-MD5
- EAP-TLS

Поддерживаемые методы для протокола TACACS+

- ASCII
- PAP
- CHAP

Еще полезные функции

- Настройка профилей конечных устройств на базе DHCP атрибутов
- Возможность формирования и скачивания отчетов
- Snapshot для политик
- Поддержка разных вендоров сетевого оборудования
- Возможность добавления новых словарей Radius
- Возможность настройки системы и сервисов из web интерфейса
- API для автоматизации
- Настройка отправки syslog во внешние системы
- Мониторинг системы

Результаты к 2025 году

что уже успели

x2,78 Повышена производительность системы

x3 Снижено потребление ресурсов

100% Устройств в банке работает через новую систему авторизации

500 000+ Устройств online

6 000 000+ Устройств ежемесячно используют систему

Что еще планируем сделать
в 2025-2026 году

На данный момент система работает в промышленной среде ПАО Сбербанк и уже соответствует его высоким стандартам по надежности и безопасности, но мы так же активно ее дорабатываем и реализуем новый функционал.

А вот что мы еще планируем сделать:

— Сделать установщик, чтобы упростить развертывание и первоначальное конфигурирование системы

— Добавить новые dashboards в web интерфейс, чтобы было наглядно

— Сделать compliance клиента для основных ОС таких как MacOS, Windows и Linux, чтобы повысить качество проверки состояния конечного устройства

— Добавить систему в РРПО, для уверенности клиентов