



СИСТЕМА КОНТРОЛЯ ДОСТУПА К СЕТИ
NAC DALLAS LOCK

СИСТЕМА КОНТРОЛЯ
ДОСТУПА К СЕТИ

ОБЗОР





СИСТЕМА КОНТРОЛЯ ДОСТУПА К СЕТИ
NAC DALLAS LOCK

СОДЕРЖАНИЕ

Введение	1
1. NAC Dallas Lock.....	2
2. Состав продукта	3
3. Основные сценарии использования	4
4. Поддерживаемые платформы	5
Заключение	6



Размещаемая в данном документе информация предназначена для свободного ознакомления. Центр защиты информации ООО «Конфидент» оставляет за собой право вносить без уведомления любые изменения в данный документ, а также в ПО, которое описано в документе.



СИСТЕМА КОНТРОЛЯ ДОСТУПА К СЕТИ

NAC DALLAS LOCK

ВВЕДЕНИЕ

Концепция «защищённого периметра» в современных корпоративных сетях, при которой всё внутреннее считается доверенным, а внешнее — враждебным, больше не работает: угрозы приходят изнутри так же часто, как снаружи.

- **Внутренние угрозы.** Неконтролируемые устройства и скомпрометированные учётные записи делают традиционные подходы к сетевой безопасности недостаточными.
- **Гибридная работа.** Сотрудники подключаются к ресурсам компании с различных устройств из офиса, дома или любой точки мира.
- **Сторонний доступ.** Подрядчикам и партнёрам требуется доступ к ресурсам сети с ограниченными правами, при этом их устройства могут не соответствовать корпоративным политикам безопасности.

Ответом на эти вызовы стала концепция Zero Trust («нулевое доверие»): каждое устройство и каждый пользователь должны проходить верификацию перед получением доступа к ресурсам сети вне зависимости от их физического расположения. Реализацию этой концепции обеспечивает NAC Dallas Lock — система контроля и управления доступом к сети.



Рисунок 1. Предоставление доступа в концепции Zero Trust



1. NAC DALLAS LOCK

NAC Dallas Lock — программный комплекс, реализующий централизованный контроль и управление доступом к доверенным сетевым зонам корпоративной инфраструктуры. Предназначен для обеспечения защищённого подключения конечных устройств (как стационарных, так и мобильных) к доверенным сегментам корпоративной сети.

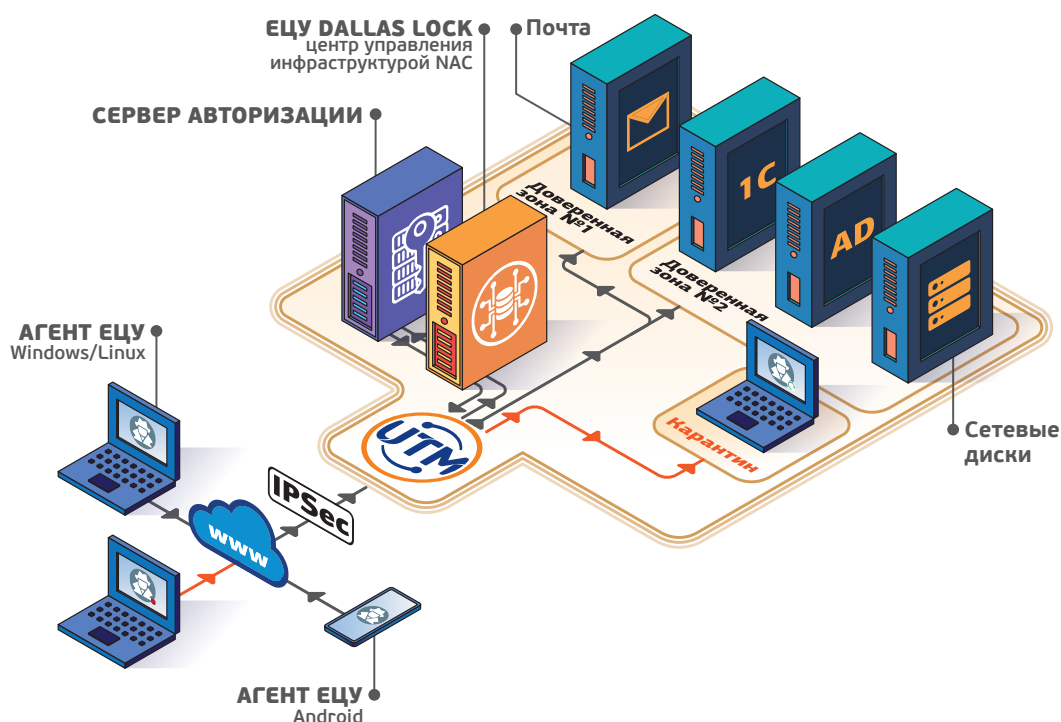


Рисунок 2. Общая схема взаимодействия NAC Dallas Lock

- **Аутентификация и авторизация.** Каждое устройство проходит проверку подлинности перед подключением через Сервер авторизации.
- **Проверка состояния устройства.** Агент ЕЦУ отправляет в ЕЦУ Dallas Lock отчёт о соответствии устройства корпоративной политике безопасности (установленное ПО, конфигурация, целостность системы)¹.
- **Управление доступом.** ЕЦУ Dallas Lock назначает устройству уровень доступа в пределах одной из доверенных зон, выдаёт IP-адрес из соответствующего пула.
- **Карантин и исправление.** Устройства, не прошедшие проверку политик, могут быть изолированы до устранения нарушений¹.

¹. Функциональная возможность будет доступна в следующем релизе.



2. СОСТАВ ПРОДУКТА

КОМПОНЕНТ	РОЛЬ	ОСНОВНЫЕ ФУНКЦИИ
ЕЦУ Dallas Lock 	Централизованное управление	• управление доверенными зонами²; • создание профилей сетевого доступа³; • аудит подключений; • контроль подключения и инвентаризация активов; • проверка соответствия устройств политикам безопасности; • ведение журналов событий безопасности.
WAF Dallas Lock 	Шлюз	• приём IPsec-подключений от агентов; • маршрутизация трафика по доверенным зонам; • ограничение доступа к разрешённым маршрутам; • разрыв соединения по команде ЕЦУ Dallas Lock при отзыве доступа.
Сервер авторизации 	Управление доступом	• обработка запросов аутентификации; • проверка профиля сетевого доступа; • назначение IP-адреса клиенту из пула адресов доверенной зоны.
Агент ЕЦУ Windows/Linux 	Клиент	• установка IPsec-соединения; • сбор информации об устройстве и ПО; • отправка отчётов о соответствии корпоративной политике безопасности⁴; • контроль RDP/SSH-доступа (ПК); • работа в фоновом режиме с низким энергопотреблением (Android); • определение геолокации⁴.
Агент ЕЦУ Android 		

2. Логическая единица, которая определяет, к каким именно сетевым ресурсам (серверам, приложениям, базам данных) устройство имеет право подключаться.

3. Специальный файл, формируемый ЕЦУ Dallas Lock для первичной настройки защищённого подключения.

4. Функциональная возможность будет доступна в следующем релизе.



3. ОСНОВНЫЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

- **Удалённый доступ сотрудников.** Сотрудники подключаются к корпоративным ресурсам через зашифрованное IPsec-соединение с любого поддерживаемого устройства: ПК, ноутбука или смартфона.
- **Защита периметра от неавторизованных устройств.** Только устройства с корректным профилем сетевого доступа и аутентификацией через Сервер авторизации получают доступ в защищённый контур.
- **Сегментация доступа.** Разные категории пользователей (сотрудники, подрядчики, администраторы) получают доступ только к строго определенному набору ресурсов, с автоматическим назначением IP из выделенного пула.
- **Контроль мобильных устройств.** Администратор безопасности в реальном времени видит статус всех подключенных Android-устройств (Подключен/Отключен/Ожидает подключения), их IP-адреса и назначенные доверенные зоны. В случае утери устройства или увольнения сотрудника администратор может в один клик выполнить действие «Запретить доступ». Система принудительно разорвет IPsec-соединение, а авторизационные данные на Сервере авторизации будут удалены. Даже если на устройстве сохранился профиль доступа, подключиться с него больше невозможно.

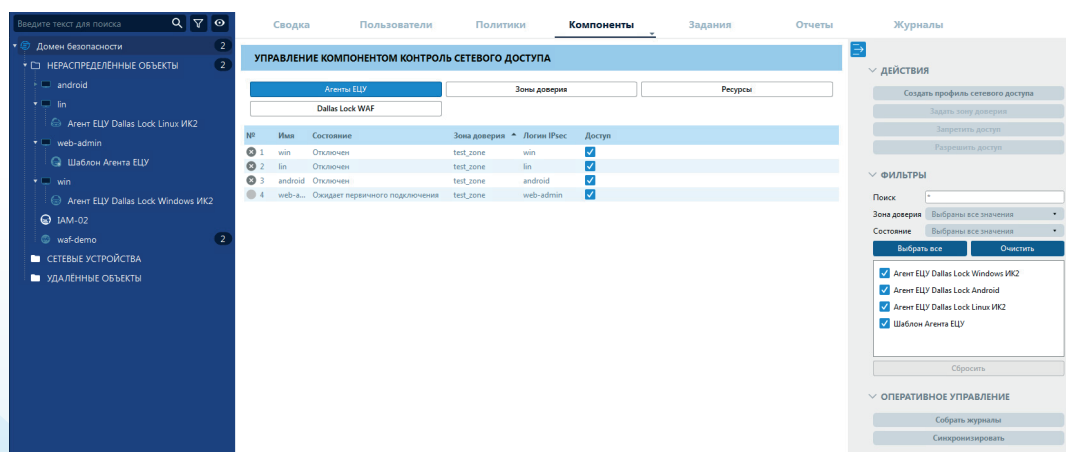


Рисунок 3. Управление компонентом контроль сетевого доступа



4. ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ

КОМПОНЕНТ	ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ
Агент ЕЦУ Windows	Windows 10, 11; Windows Server 2016, 2019, 2022, 2025
Агент ЕЦУ Android	Android 8 и выше Архитектуры: armeabi-v7a, arm64-v8a, x86, x86_64
Агент ЕЦУ Linux	Debian 10.x, 11.x, 12.x; Ubuntu 18.04, 20.04, 22.04, 24.04; Astra Linux Common Edition (Опел) 2.12; Astra Linux Special Edition (Смоленск) 1.6, 1.7, 1.8; Альт Рабочая Станция 9.x, 10.x, К 10.x; Альт Сервер 9, 10.x; Альт 8 СП релиз 10 (Рабочая Станция, Сервер); РЕД ОС 7.3 Муром; РЕД ОС 8; ROSA FRESH DESKTOP 12; МСВСфера АРМ 9
Сервер авторизации	Debian 10.x, 11.x, 12.x; Ubuntu 18.04, 20.04, 22.04, 24.04; Astra Linux Special Edition (Смоленск) 1.7, 1.8; Альт Рабочая Станция 10.x, К 10.x, 11.1; Альт Сервер 10.x; Альт 8 СП релиз 10 (Рабочая Станция, Сервер); РЕД ОС 7.3 Муром; РЕД ОС 8; МСВСфера АРМ 9; МСВСфера Сервер 9



ЗАКЛЮЧЕНИЕ

NAC Dallas Lock является современным инструментом контроля и управления сетевым доступом. Предоставляет администратору безопасности механизмы для централизованной настройки доверенных зон, мониторинга и управления статусами подключений посредством интерфейса ЕЦУ Dallas Lock.

Пользователю системы предоставляется доступ к разрешённым ресурсам через простой интерфейс Агента ЕЦУ.



192029, г. Санкт-Петербург
пр. Обуховской Обороны, д. 51, лит. К
телефон/факс: (812) **325-1037**

<http://www.confident.ru/>
<http://www.dallaslock.ru/>
e-mail:

isc@confident.ru – коммерческие вопросы
helpdesk@confident.ru – техническая поддержка

Схема проезда:



www.confident.ru



www.dallaslock.ru



Telegram-канал



ВКонтакте



Max

