

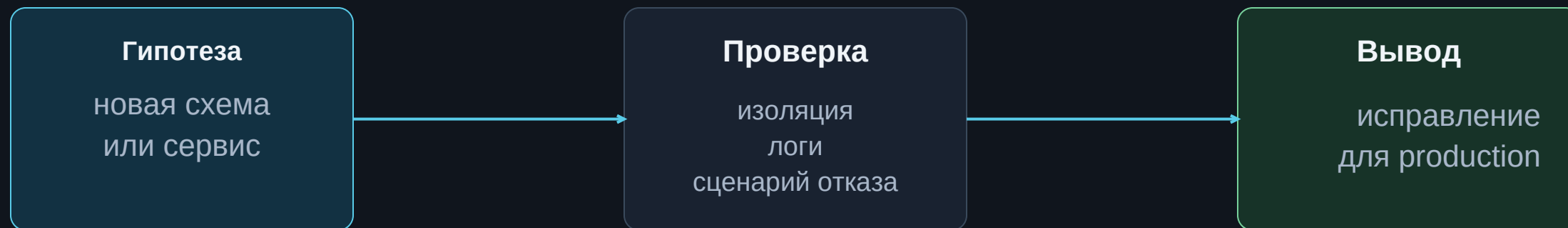
HomeLab как полигон для пентеста и AI

Проверять схемы и сервисы до production

Илья Кобельков · руководитель ИТ-направления · HomeLab

**Лаборатория нужна не ради эксперимента.
Она нужна, чтобы production не стал экспериментом.**

HomeLab как безопасный полигон



Найдённая проблема здесь дешевле, чем инцидент там.

Что именно мы проверяем

Схемы сети

маршруты
VPN
VLAN
firewall rules

Сервисы

reverse proxy
WebSocket
Docker
API

AI и агенты

SSH
MCP tools
секреты
исходящий трафик

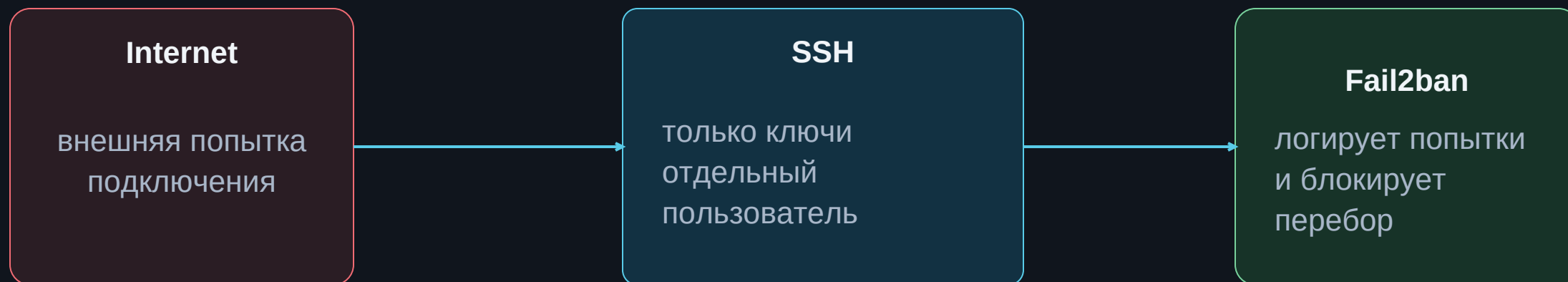
Вопрос один: какой доступ действительно получает компонент, если он ошибся или скомпрометирован?

Кейс: WireGuard не делает WAN кластерной сетью



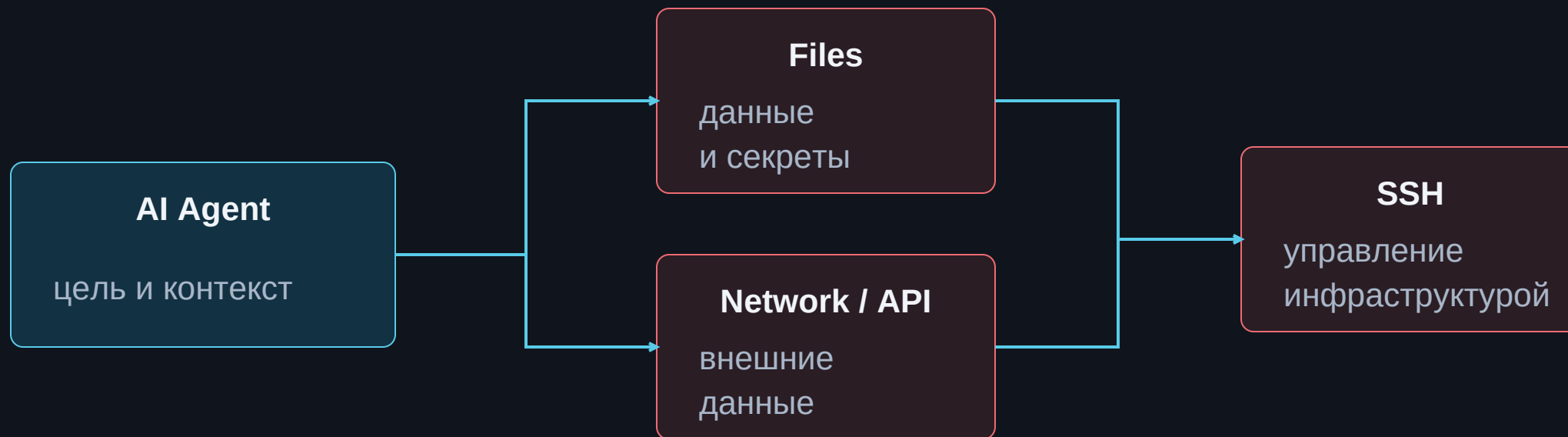
Вывод из пентеста схемы: обычный ring не проверяет пригодность управляющего контура.

Кейс: SSH доступ ограничивают до входа



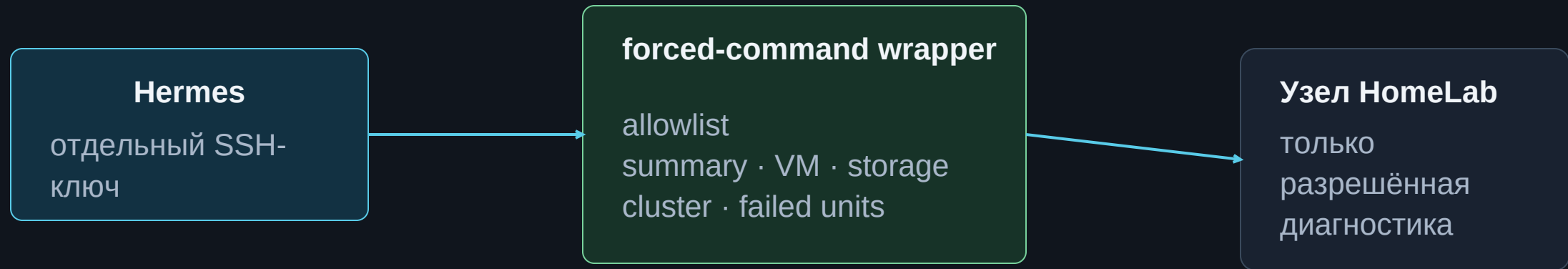
Проверяем не наличие SSH, а то, какой вход он действительно разрешает.

AI расширяет поверхность пентеста



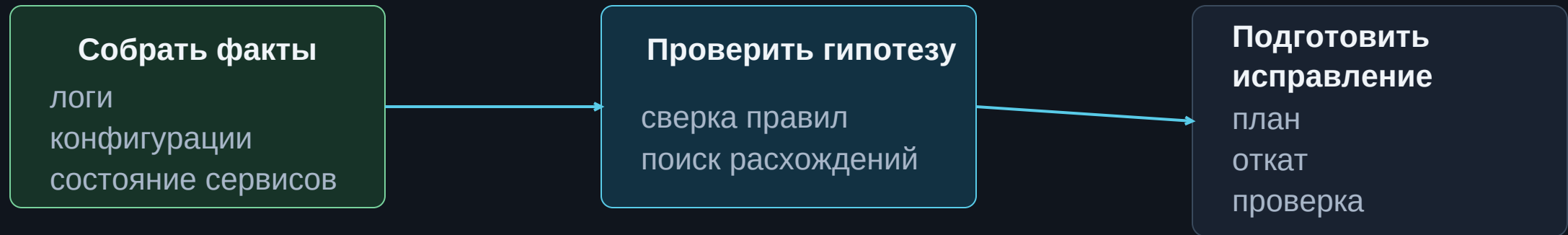
Агент = сервисная учётная запись, которой дали возможность выбирать действия.

Проверяем не prompt, а техническую границу



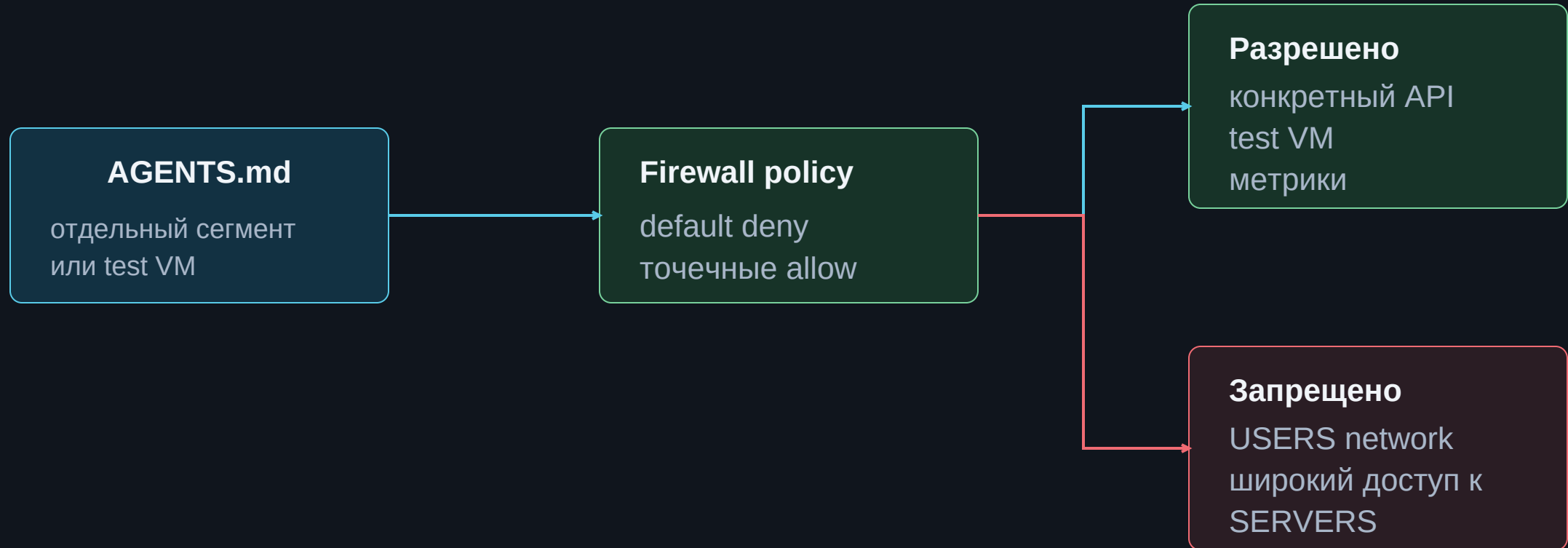
ssh node reboot → Denied. Allowed diagnostics: ...

AI нужен для самого цикла проверки



Владелец подтверждает изменения. Агент не получает права решать это сам.

Следующая проверка: Agent Security Zone



Сначала проверяем, что агент не может сделать лишнее.
Потом подключаем полезный инструмент.

HomeLab → проверка → исправление production

AI помогает быстрее пройти путь от сигнала до проверенного плана.

проверить

ограничить

исправить

подтвердить