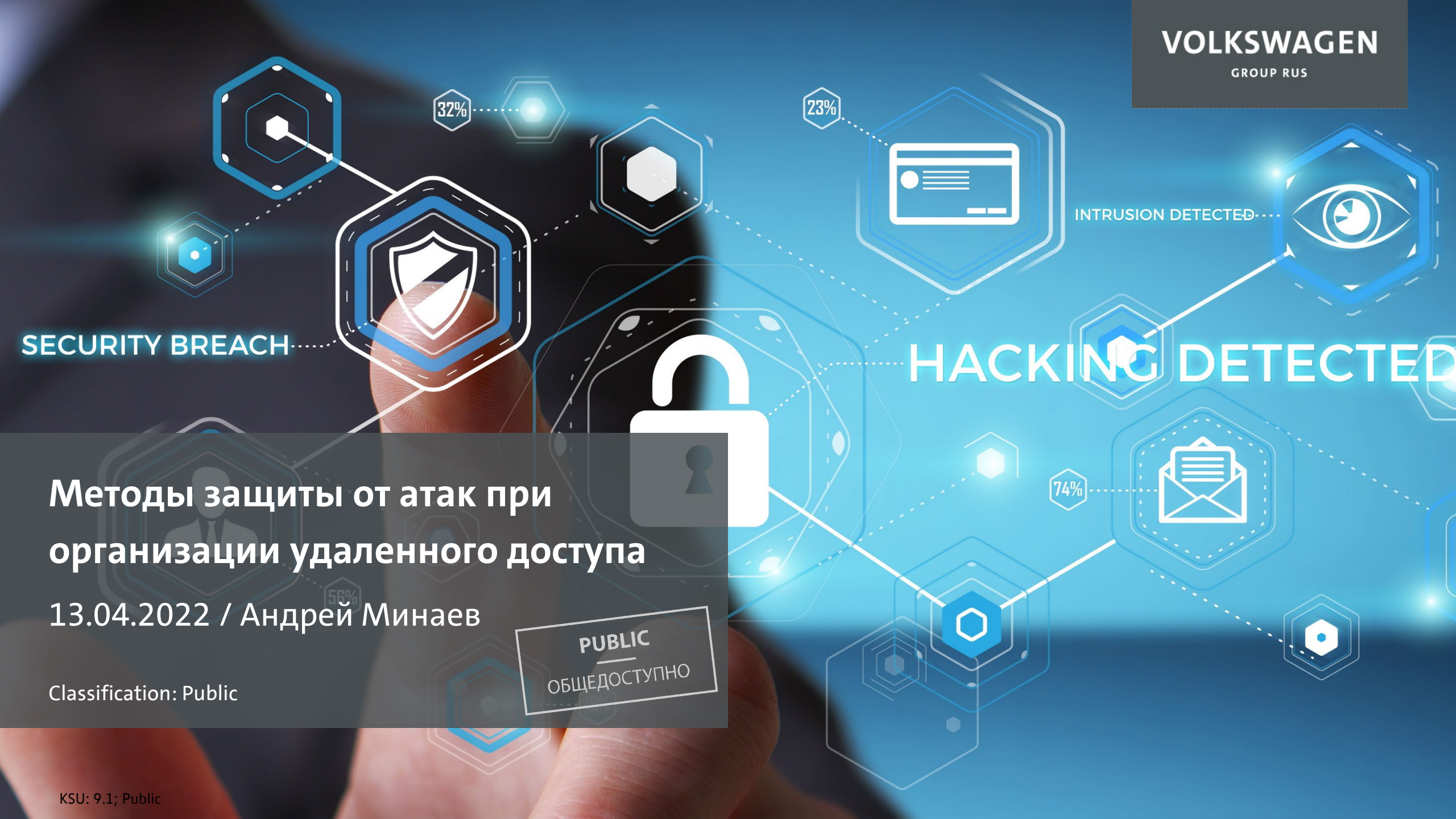


Методы защиты от атак при организации удаленного доступа

13.04.2022 / Андрей Минаев

PUBLIC
ОБЩЕДОСТУПНО

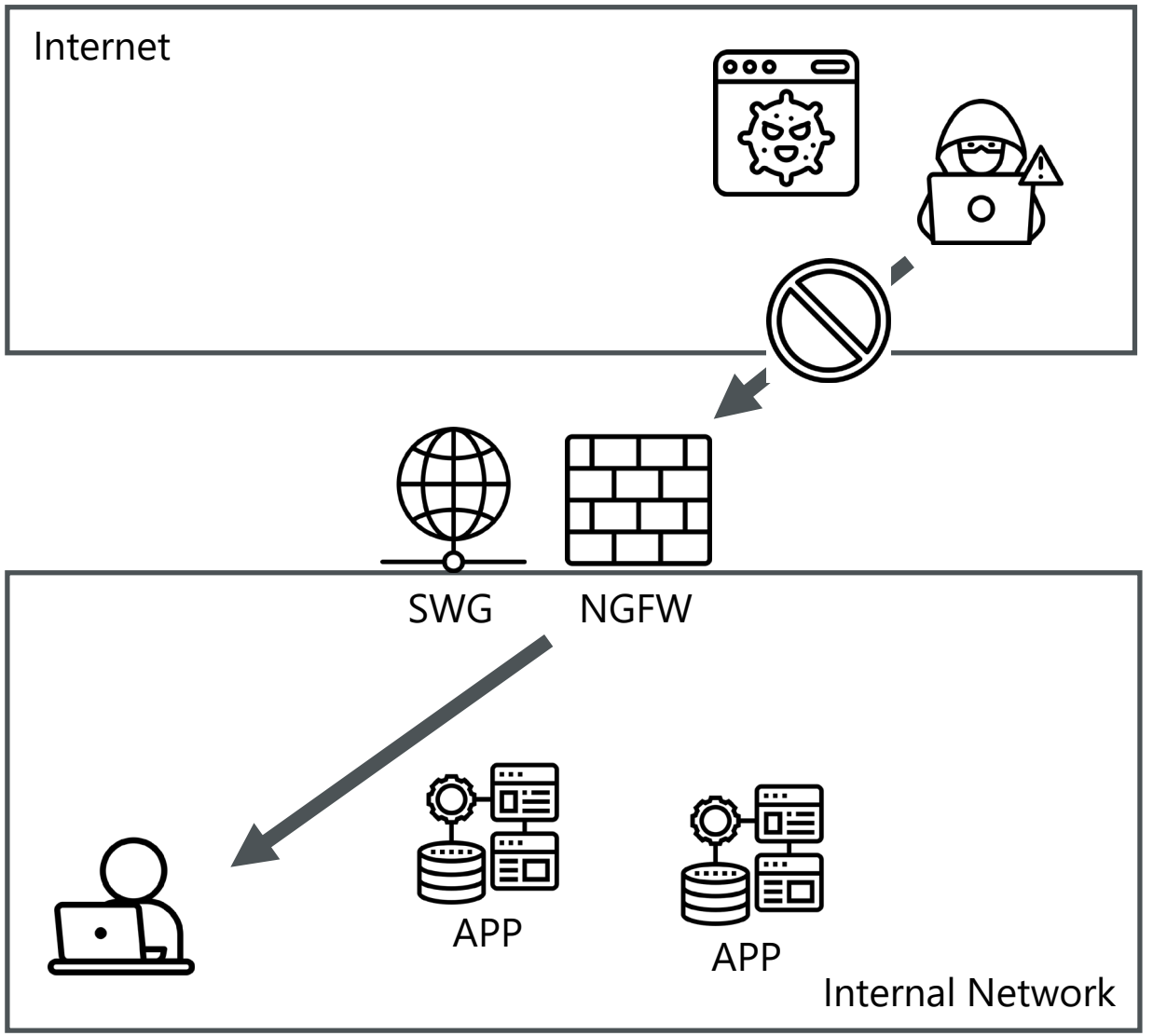
Classification: Public

KSU: 9.1; Public

Пользователи во внутренней сети компании хорошо защищены

Все внешние коммуникации – контролируются

Входящий трафик – NGFW

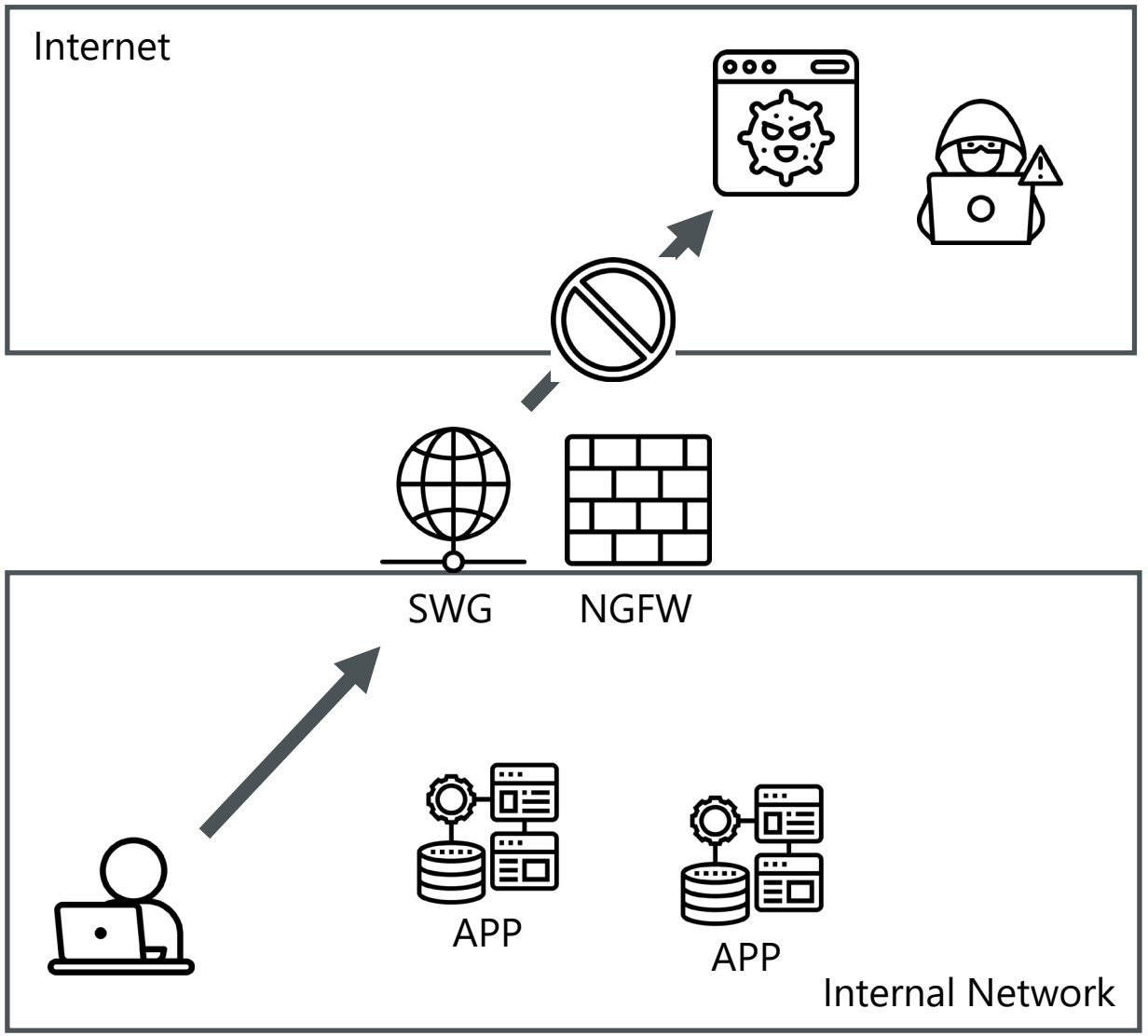


Пользователи во внутренней сети компании хорошо защищены

Все внешние коммуникации – контролируются

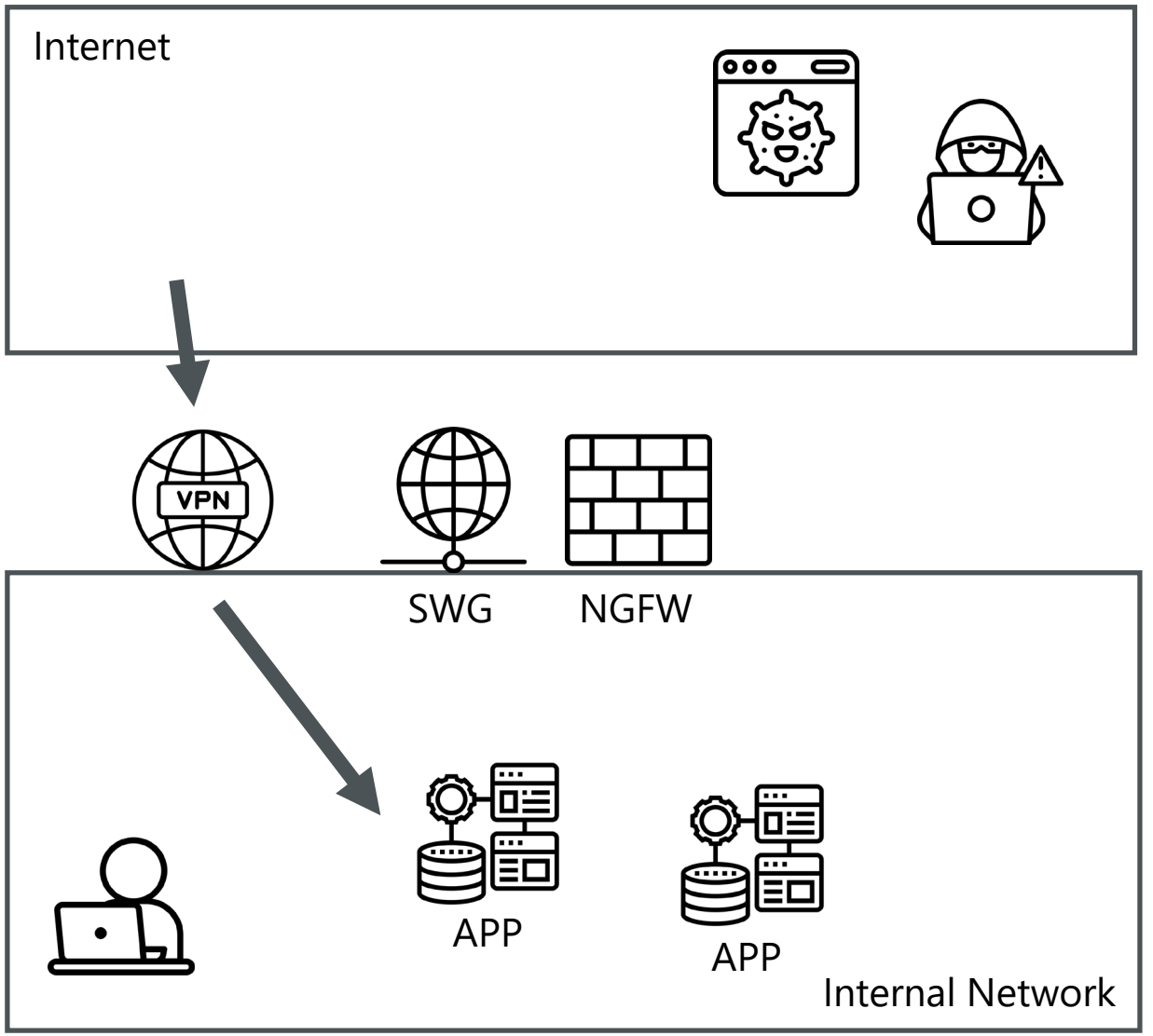
Входящий трафик – NGFW

Исходящий трафик – Secure Web Gateway (SWG)



При перемещении пользователя в интернет список угроз существенно расширяется

Доступ к внутренним приложениям осуществляется через VPN

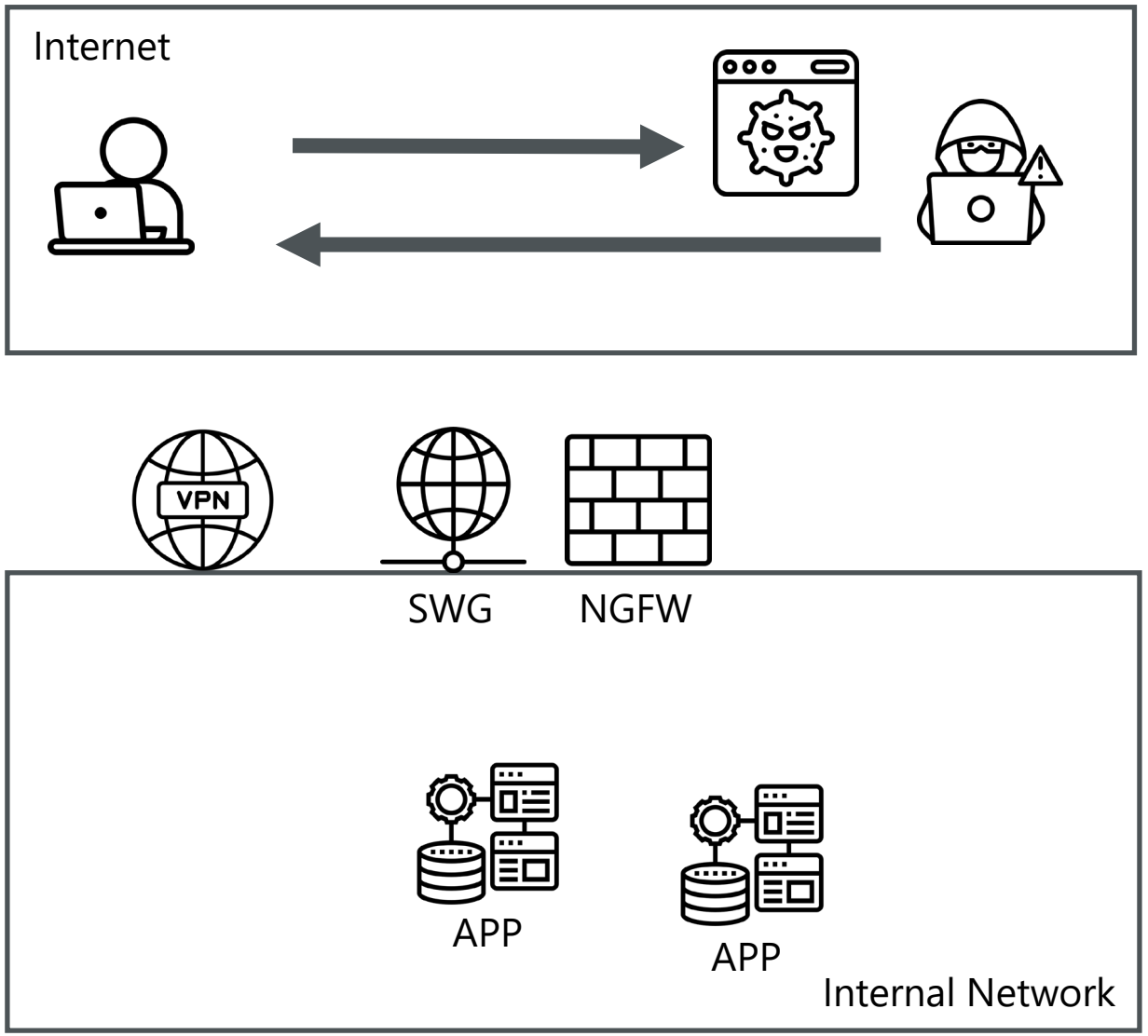


При перемещении пользователя в интернет список угроз существенно расширяется

Все внешние коммуникации – не контролируются:

Входящий трафик – не защищён центральным NGFW. Угроза взлома компьютера пользователя

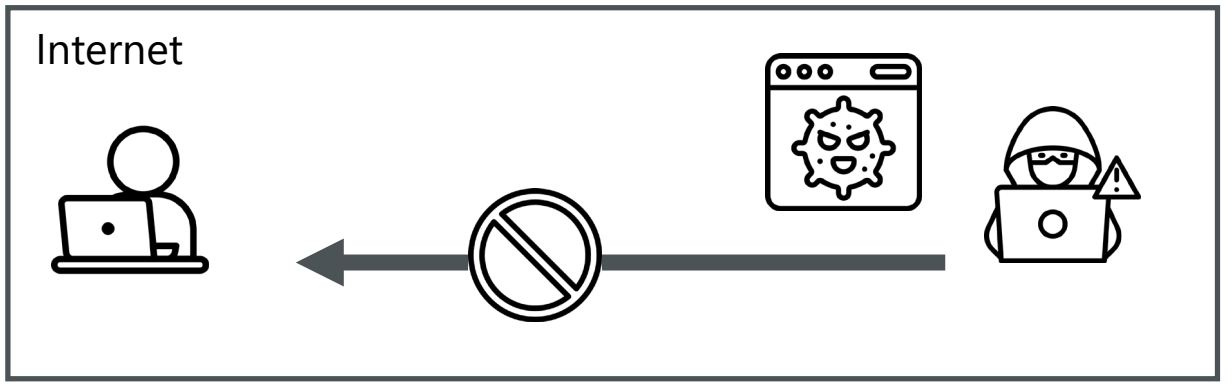
Исходящий трафик – не защищён Secure Web Gateway (SWG). Угроза доступа к вредоносным ресурсам, фишинговым сайтам и т.д.



При перемещении пользователя в интернет список угроз существенно расширяется

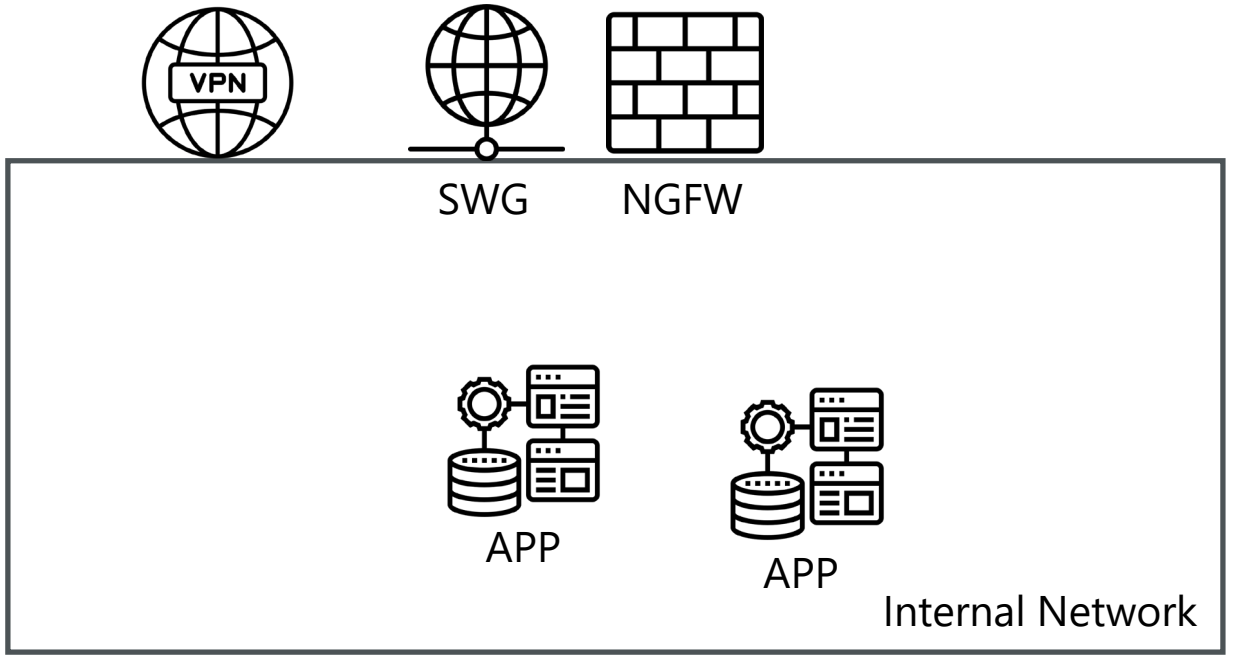
Все внешние коммуникации – не контролируются:

Входящий трафик – не защищён центральным NGFW. Угроза взлома компьютера пользователя



Решение:

- Централизованная установка приложений
- Забрать права локального администратора у пользователей (в т.ч. у руководителей и сотрудников ИТ)
- Принудительное обновление установленных приложений
- Включение Windows Firewall, запрет входящих подключений, особенно доступа по RDP, VNC, ..
- Спец. средства для VPN доступа с не доверенных компьютеров



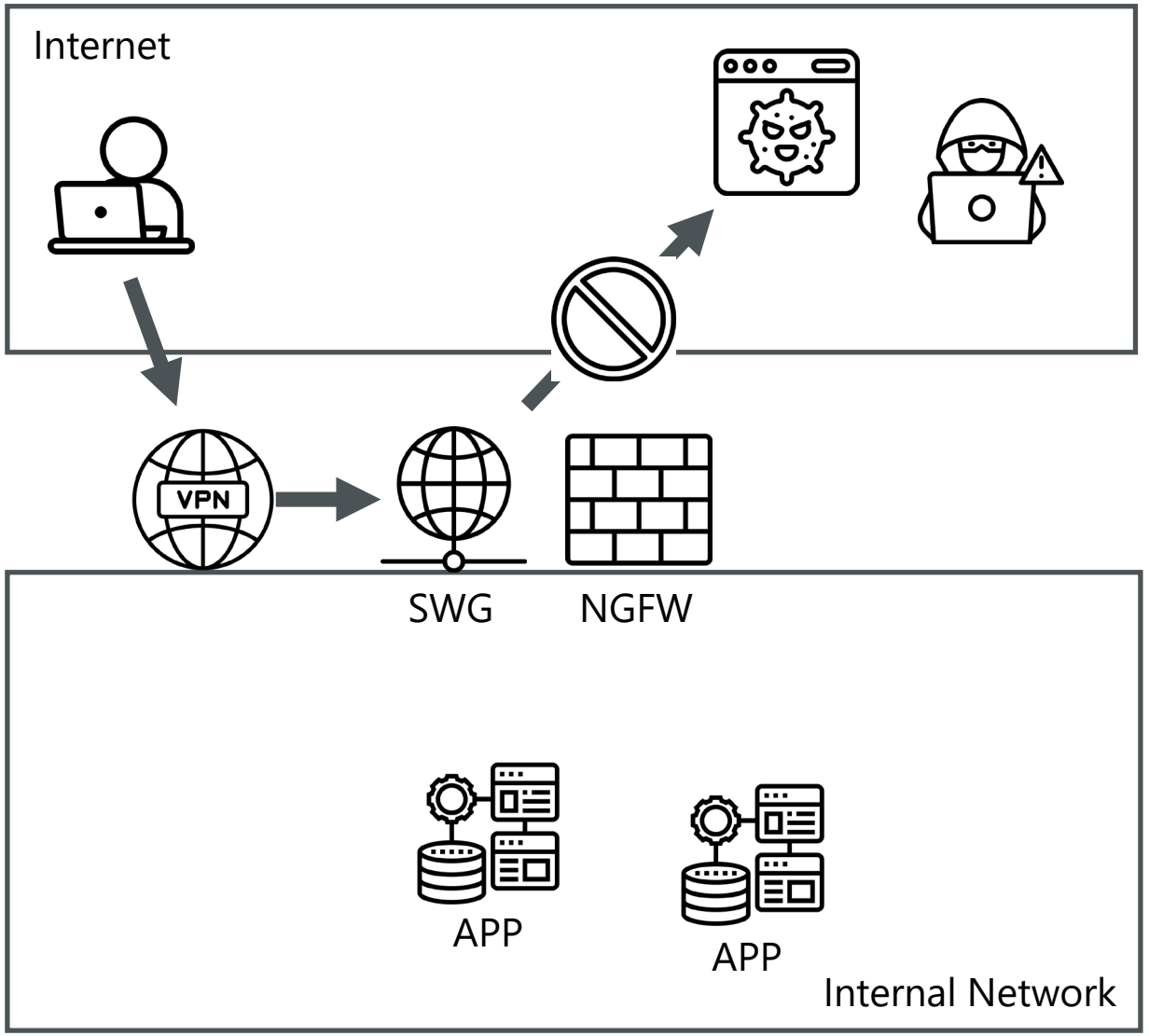
При перемещении пользователя в интернет список угроз существенно расширяется

Все внешние коммуникации – не контролируются:

Исходящий трафик – не защищён Secure Web Gateway (SWG). Угроза доступа к вредоносным ресурсам, фишинговым сайтам и т.д.

Решение:

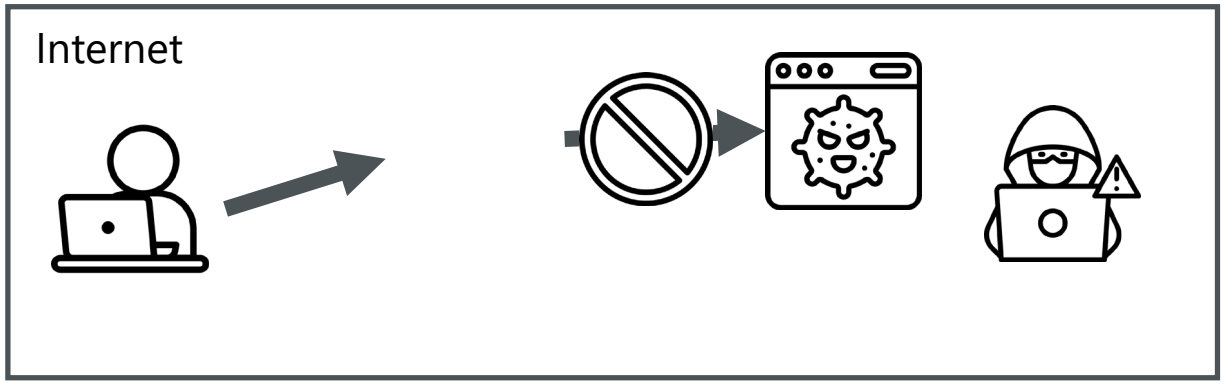
- On premise SWG + Always On VPN
- Cloud SWG для контроля интернет-трафика



При перемещении пользователя в интернет список угроз существенно расширяется

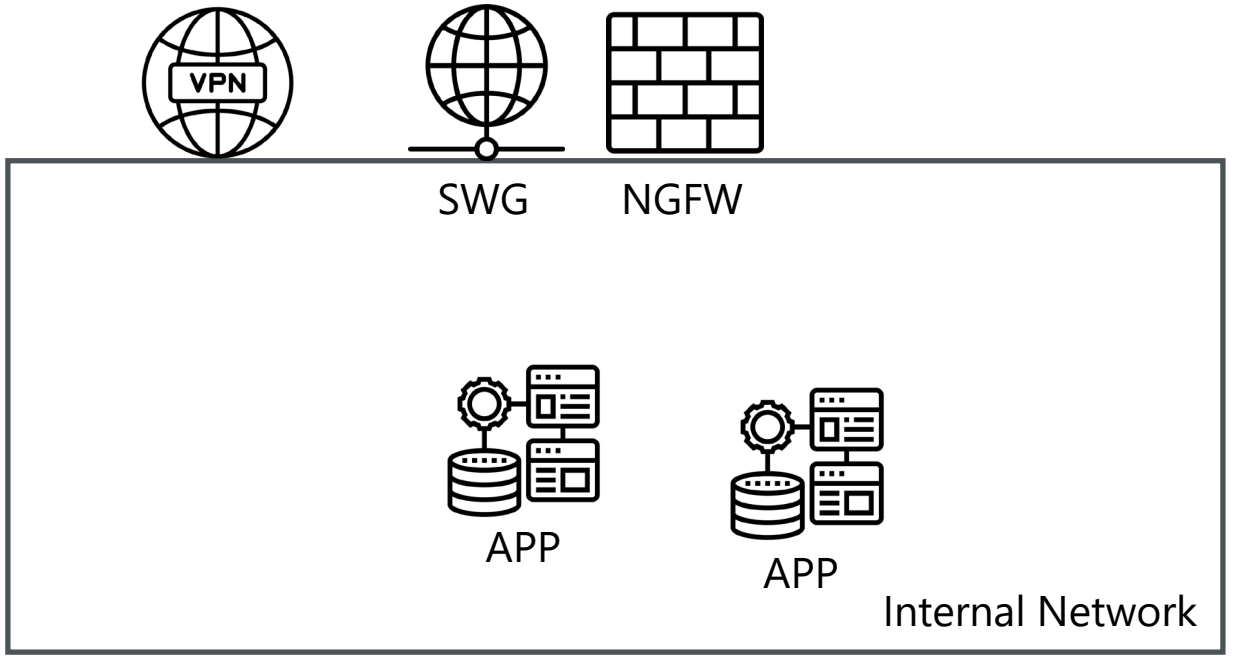
Все внешние коммуникации – не контролируются:

Исходящий трафик – не защищён Secure Web Gateway (SWG). Угроза доступа к вредоносным ресурсам, фишинговым сайтам и т.д.



Решение:

- On premise SWG + Always On VPN
- Cloud SWG для контроля интернет-трафика

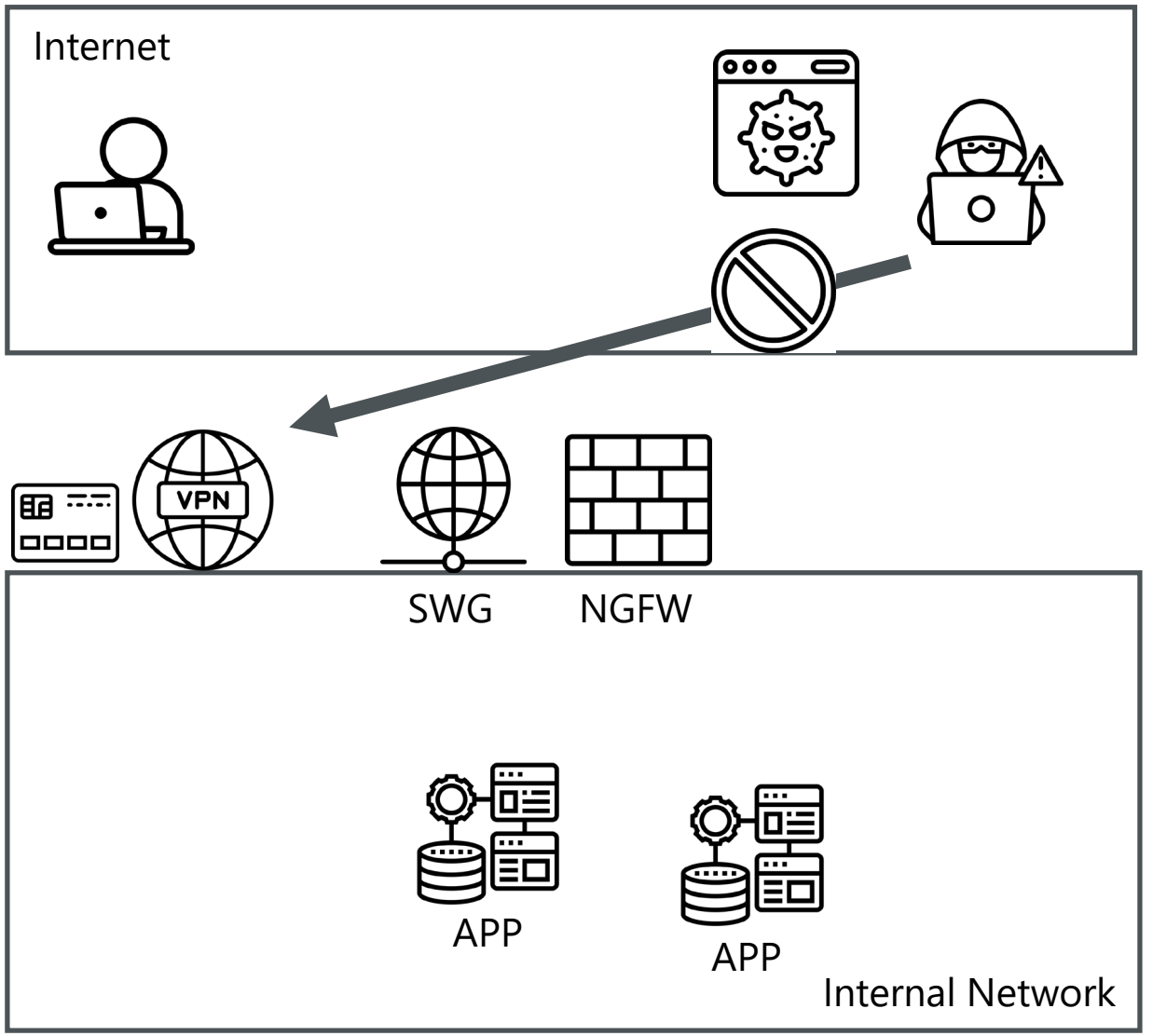


Атаки на систему удаленного доступа

Эксплуатация уязвимостей, Brute Force

Решение:

- Обновление и поддержка VPN решения
- Применение 2FA

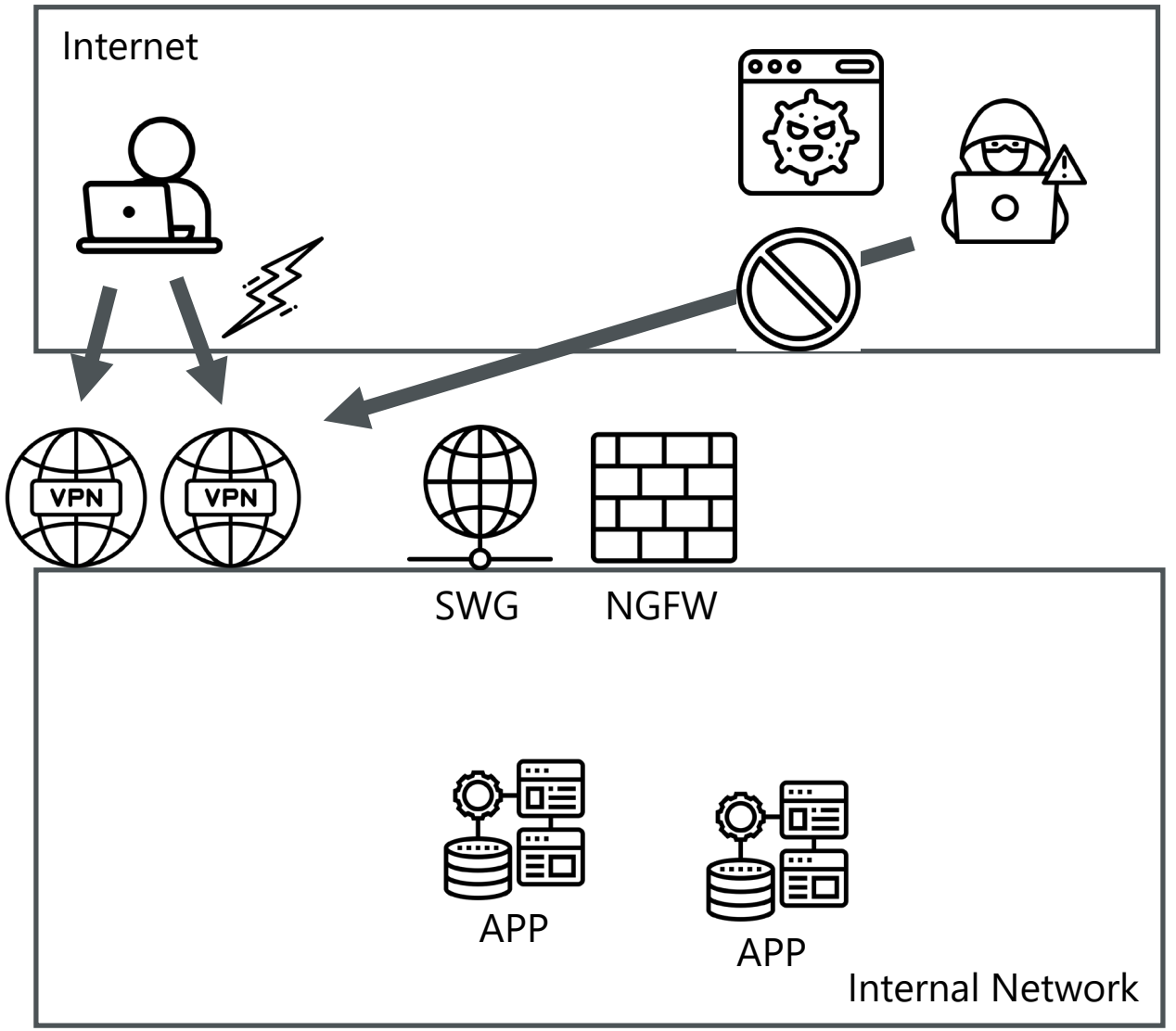


DDOS атаки на сеть компании или VPN шлюз

DDOS атаки на сайты и системы компании. Если у вас нет публичного ресурса, это не значит, что вы в безопасности. Небольшие и дешёвые атаки на сеть компании, которые способны её положить (100 Mbit/s – 1 Gbps) стоят от 50$/сутки. Угроза работы VPN и других решений.

Решение:

- Дублирование сервисов в разных публичных подсетях
- Включение защиты от DDOS
- Запрет на доступ к сети из других стран

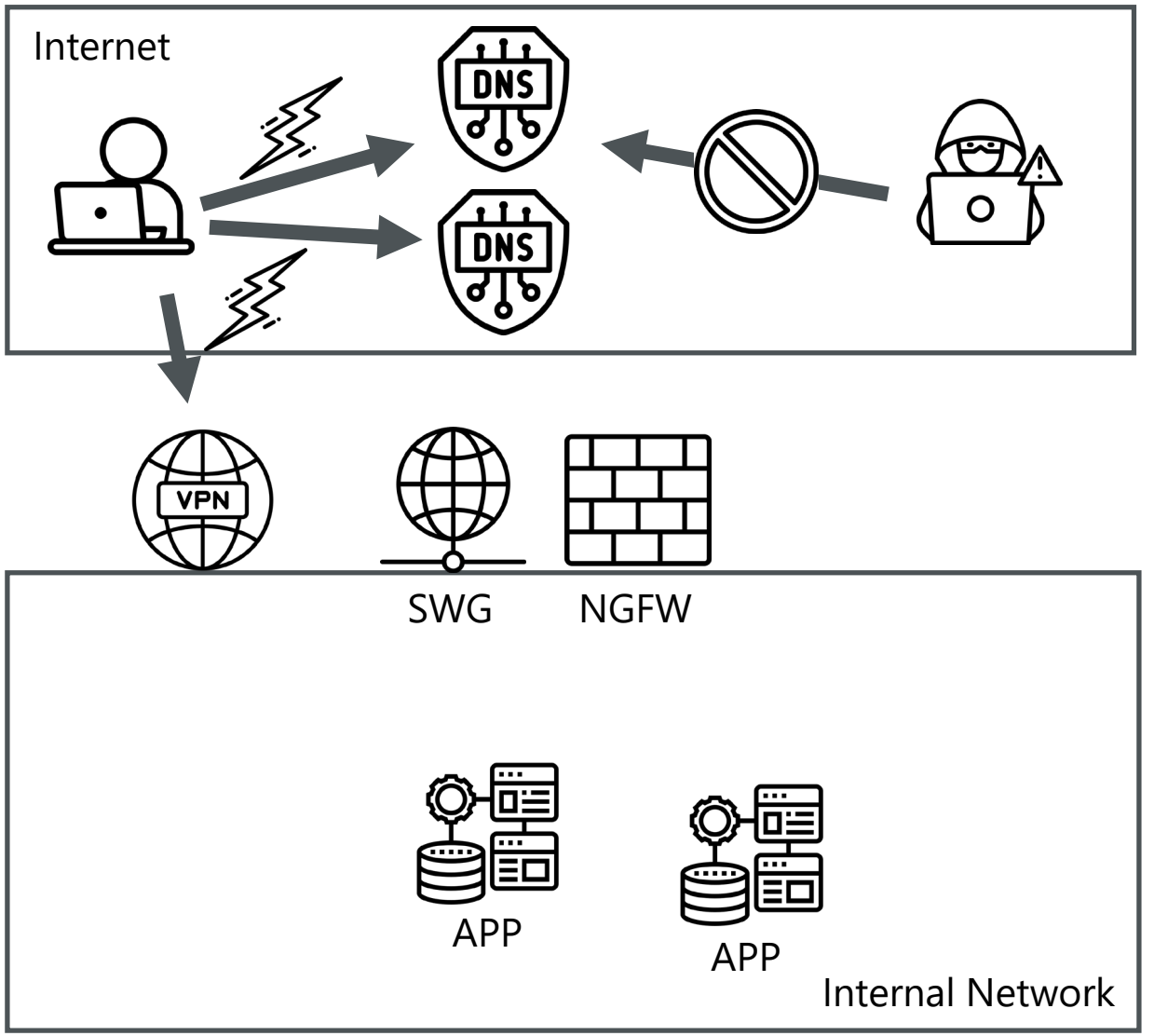


DDOS атаки на DNS

VPN и другие системы могут стать недоступны из-за DDOS атак на DNS сервера

Решение:

- Поднимайте secondary DNS зоны на сторонних DNS серверах
- Мигрируйте на другого DNS провайдера с защитой от DDOS



Выводы

- ✓ Повысьте защищённость рабочих станций
- ✓ Защитите доступ пользователей в интернет
- ✓ Убедитесь, что VPN поддерживается, обновляется и настроена 2FA
- ✓ Защитите каналы связи от DDOS
- ✓ Защитите DNS от DDOS

Андрей Минаев

Andrey.Minaev@vwgroup.ru

www.vwgroup.ru

VOLKSWAGEN
GROUP RUS