appgate



# APPGATE SDP

## БЕЗОПАСНЫЙ УДАЛЕННЫЙ ДОСТУП К СЕТИ ПО МОДЕЛИ НУЛЕВОГО ДОВЕРИЯ

**Appgate SDP** – платформа сетевой безопасности для предоставления безопасного удаленного доступа к сети по модели нулевого доверия и динамического контроля соблюдения политик доступа ко всем сетевым ресурсам компании (не важно, где они находятся, внутри инфраструктуры или в облаке). На основании профиля пользователя, устройства, информации со сторонних систем и других параметров подключения, формирует зашифрованный канал 1:1 от клиента к целевой системе и динамически контролирует доступ к ней. При подключении возможна дополнительная авторизация пользователя с использованием MFA.

### Задачи и проблемы:

- Опасность использования VPN-решений для удаленного подключения
- Предоставление удаленного доступа только к необходимым ресурсам
- Контроль доступа сторонних пользователей к сети (подрядные организации)
- Необходима проверка контекста устройства, с которого пользователь подключается к сети
- Необходим единый подход для управления политиками доступа для облачных, гибридных и локальных сред
- Обеспечение доступа с наименьшими привилегиями при работе с облачными инфраструктурами (IaaS, PaaS, SaaS)
- Обеспечение безопасного, автоматического и одновременного доступа к облачным и гибридным средам для DevOps команд из единой точки. Поддержка необходимой скорости и гибкости без ограничений
- Интеграция с ИТ-инфраструктурой для добавление дополнительного механизма аутентификации при получении удаленного доступа

appgate

**APPGATE** www.appgate.com

## СХЕМА РАБОТЫ


### Ключевые возможности и преимущества:

- Технология авторизации единичным пакетом (SPA) для маскировки инфраструктуры
- Создание подключения только после аутентификации и авторизации пользователя
- Применение единой структуры ко всем пользователям, устройствам, сетям и ресурсам
- Динамическое создание индивидуальных сетевых подключений для каждого пользователя к необходимым ресурсам
- Микросегментацию и создание “Персонального сегмента” (для каждой пары – пользователь + ресурс)
- Изолирование пользовательских устройств от всех входящих подключений
- Одномоментное построение нескольких защищенных туннелей для доступа к разным ресурсам
- Постоянный мониторинг изменения контекста подключения
- Безопасный гибкий доступ к контейнерам рабочих нагрузок (Kubernetes, Red Hat OpenShift, VMware Tanzu, AWS, Google, MS Azure)
- Использование метаданных для автоматического применения и масштабирования политик
- Контроль IoT устройств
- Гибкое развертывание – внутри локальной инфраструктуры, в любой облачной среде, как услуга.
- Возможность работы со скриптами во всех частях процесса управления доступом
- Двунаправленный API для максимальной интеграции с IT- экосистемой
- Легкость масштабирования и построения отказоустойчивости