



Трубная Металлургическая Компания

Москва 2021 г.



Решения по организации удалённого доступа в корпоративную сеть. Always On VPN от Microsoft

Шаталов Александр
Технический эксперт Управления
средств защиты ИТ Инфраструктуры

Состояние до ...



Различные способы организации удалённого доступа

Не равномерное использование технологий

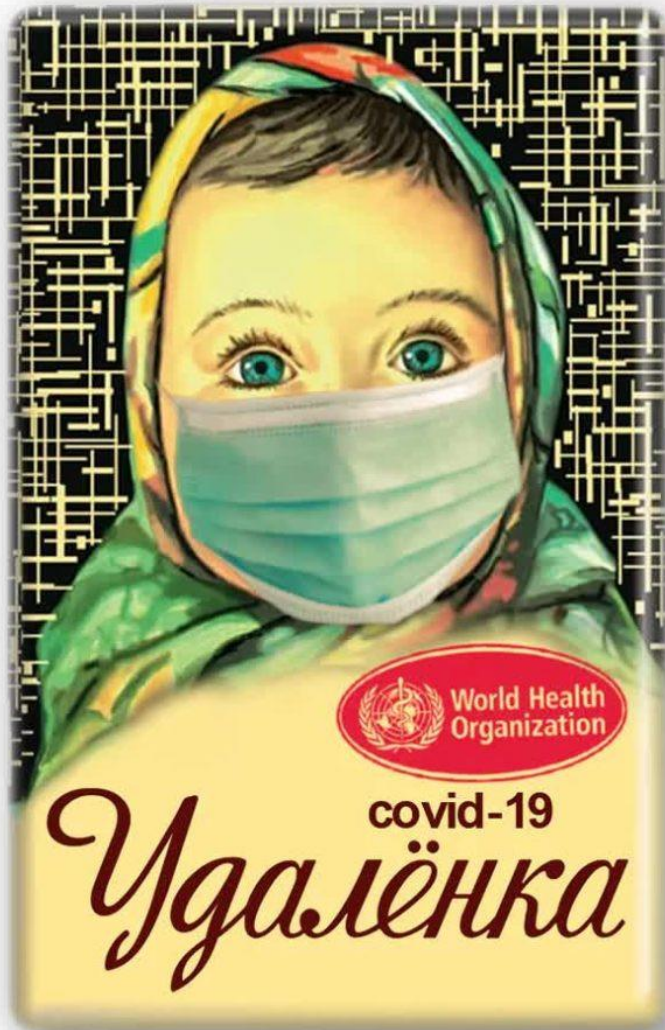
“Индивидуальный” подход в каждом случае

Нет различия для разных групп пользователей (ИТ/Подрядчики/Сотрудники)

Большинство сервисов не доступны из сети Интернет



«Удалёнка»

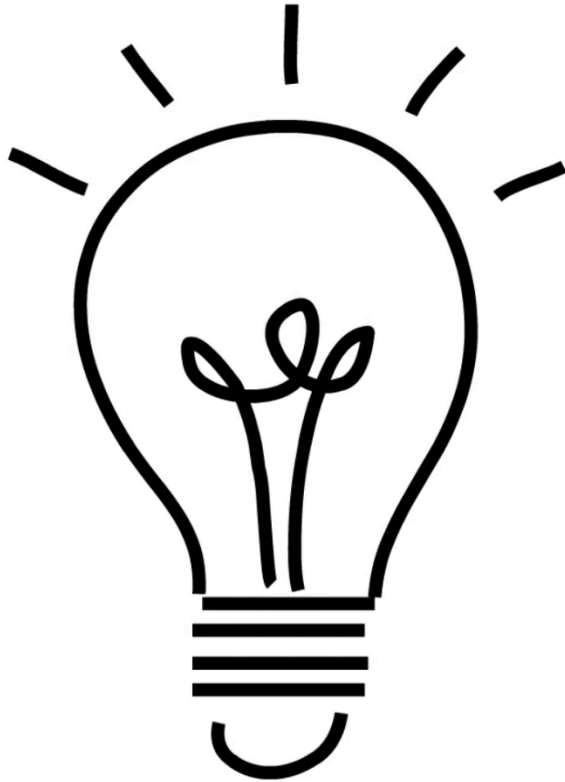


Март						
пн	вт	ср	чт	пт	сб	вс
25	26	27	28	1	2	3
4	5	6	7*	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Необходимо

- Предоставить доступ сотрудникам ко всем ресурсам компании
- СРОЧНО
- И ...

Что делать???



Создадим терминальную ферму

- Аппаратные ресурсы ограничены
- СРОЧНО

Раздадим ноутбуки

- Нет
- А их нигде вообще нет

Поставим VPN на домашние компьютеры

- Лицензии найдем
- Но ...

Требования ИБ для категорий сотрудников



№	Категория пользователя	Наименование программного обеспечения, применяемой технологии
1	Работник Предприятия, являющийся администратором информационной системы	
1.1.	Служебная рабочая станция, сервер управления БД, папка файлового сервера, web- сервер	VDI с выделенной виртуальной машиной
2.	Работник компании (пользователь рабочей станции)	
2.1.	Служебная рабочая станция, сервер управления БД, папка файлового сервера, web- сервер	VDI без выделенной виртуальной машины. Использовать конкурентные лицензии для виртуальных АРМ, без сохранения состояния: виртуальная машина создается при подключении из «золотого образа» и удаляется при выходе.
3	Представитель подрядной организации в рамках проектной деятельности по интеграции	
3.1.	Служебная рабочая станция, сервер управления БД, папка файлового сервера, web- сервер	Доступ через подсистему управления доступом для привилегированных пользователей (Privileged Account Security)
4	Представитель подрядной организации в рамках оказания услуг по технической поддержке/сопровождению программного обеспечения	
4.1.	Служебная рабочая станция, сервер управления БД, папка файлового сервера, web- сервер	Доступ через подсистему управления доступом для привилегированных пользователей (Privileged Account Security)

Требования ИБ для точек входа в систему

Необходимо применять решения по двухфакторной аутентификация;

На виртуальном рабочем месте VDI должны быть установлена поддерживаемая ОС и установлены последние обновления ОС и ПО;

На виртуальном рабочем месте VDI должны быть установлено Антивирусное ПО (АВПО) с последними обновлениями антивирусных баз;

Все подключения должны журналироваться, а данные о факте авторизации, отправляться в корпоративные SIEM- системы;

Контролирующем удаленные подключения самостоятельным подразделением, является СП по ИБ;

Подсистема управления доступом для привилегированных пользователей должна обеспечивать изоляцию сеансов пользователя;

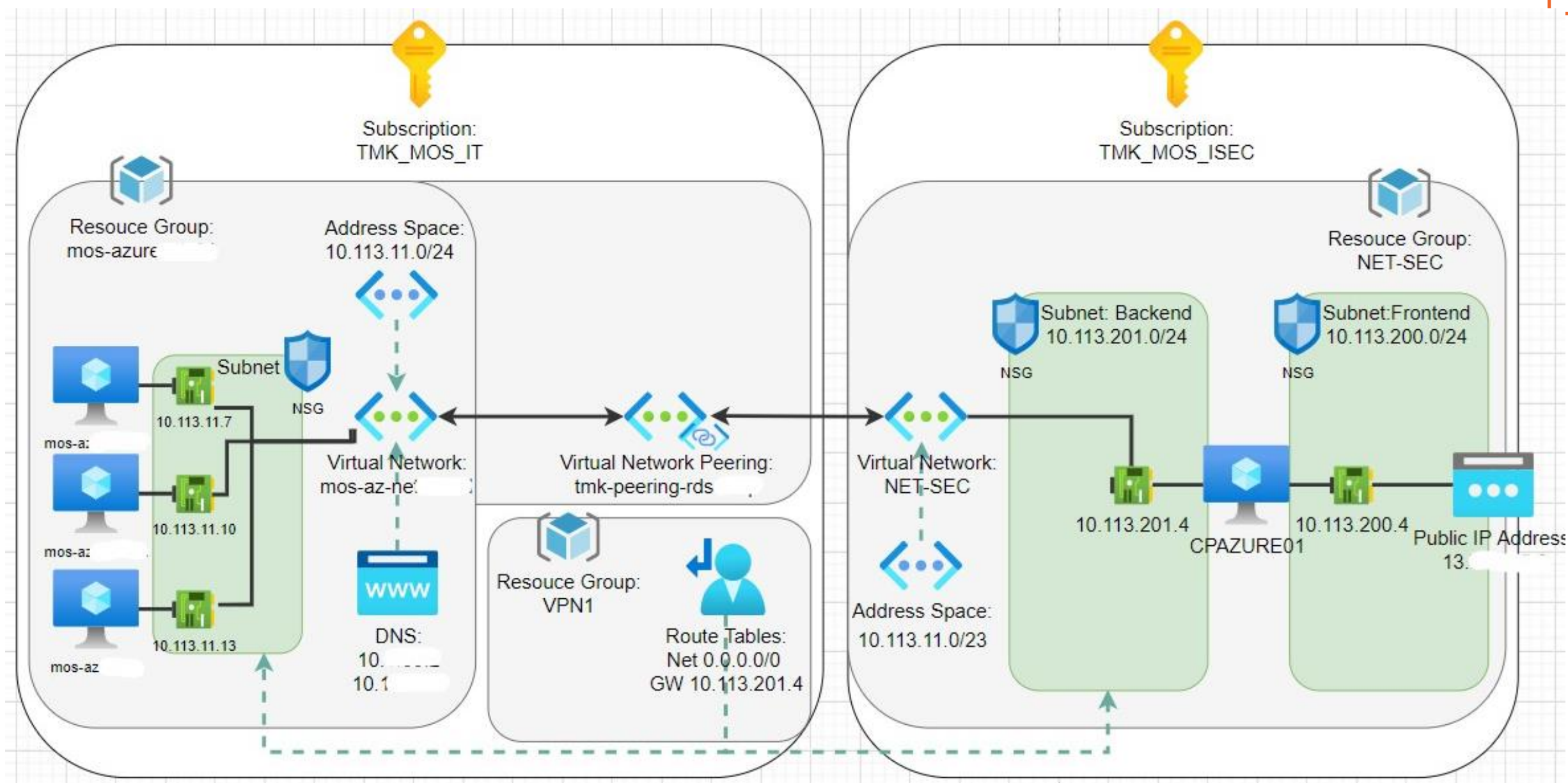
Подсистема управления доступом для привилегированных пользователей должна обеспечивать запись сеансов пользователей и вводимых команд;

Подсистема управления доступом для привилегированных пользователей должна обеспечивать хранение и смену паролей и ключей;

В случае нестандартных задач или длительных совместных проектов с подрядными организациями – разрабатывать решение по доступу в индивидуальном порядке при участии СП по ИБ и СП по ЗИ.

При наличии минимальных признаков компрометации удаленного подключения, соединение должно быть немедленно разорвано и сообщено в СП по ИБ.

Решение в ПАО ТМК | Azure RDS



Решение в ПАО ТМК | WAF



Многоуровневый подход FortiWeb к обнаружению угроз обеспечивает защиту от известных и неизвестных атак

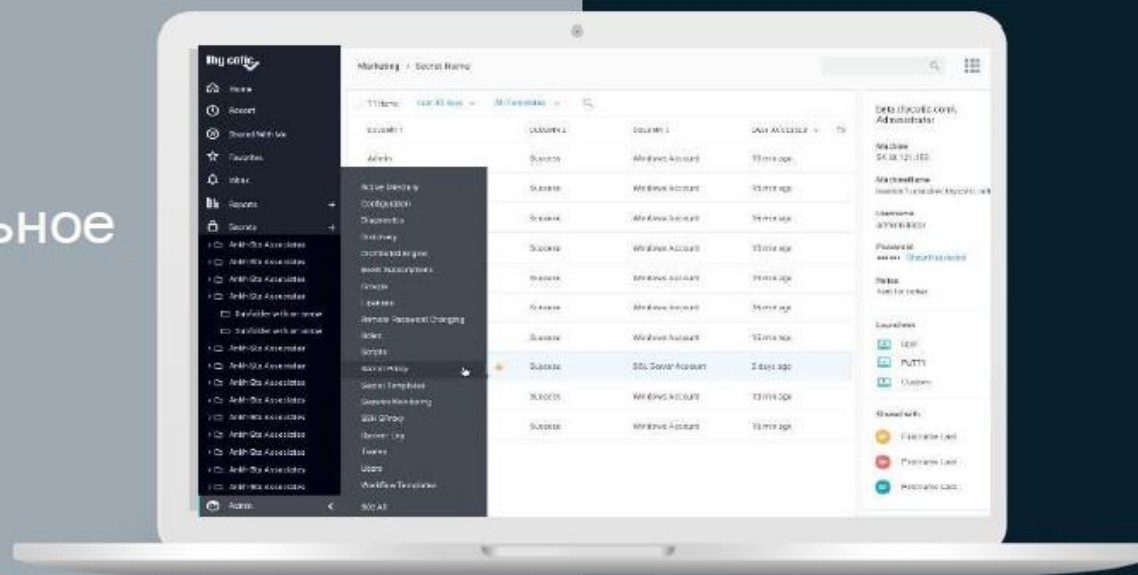


Решение в ПАО ТМК | РАМ



Secret Server

Полнофункциональное
РАМ решение,
доступное как
локально так и в
облаке



Установка
хранилища



Обнаружение
учетных записей



Предоставление
доступа для
внутреннего и
внешнего персонала



Смена
паролей

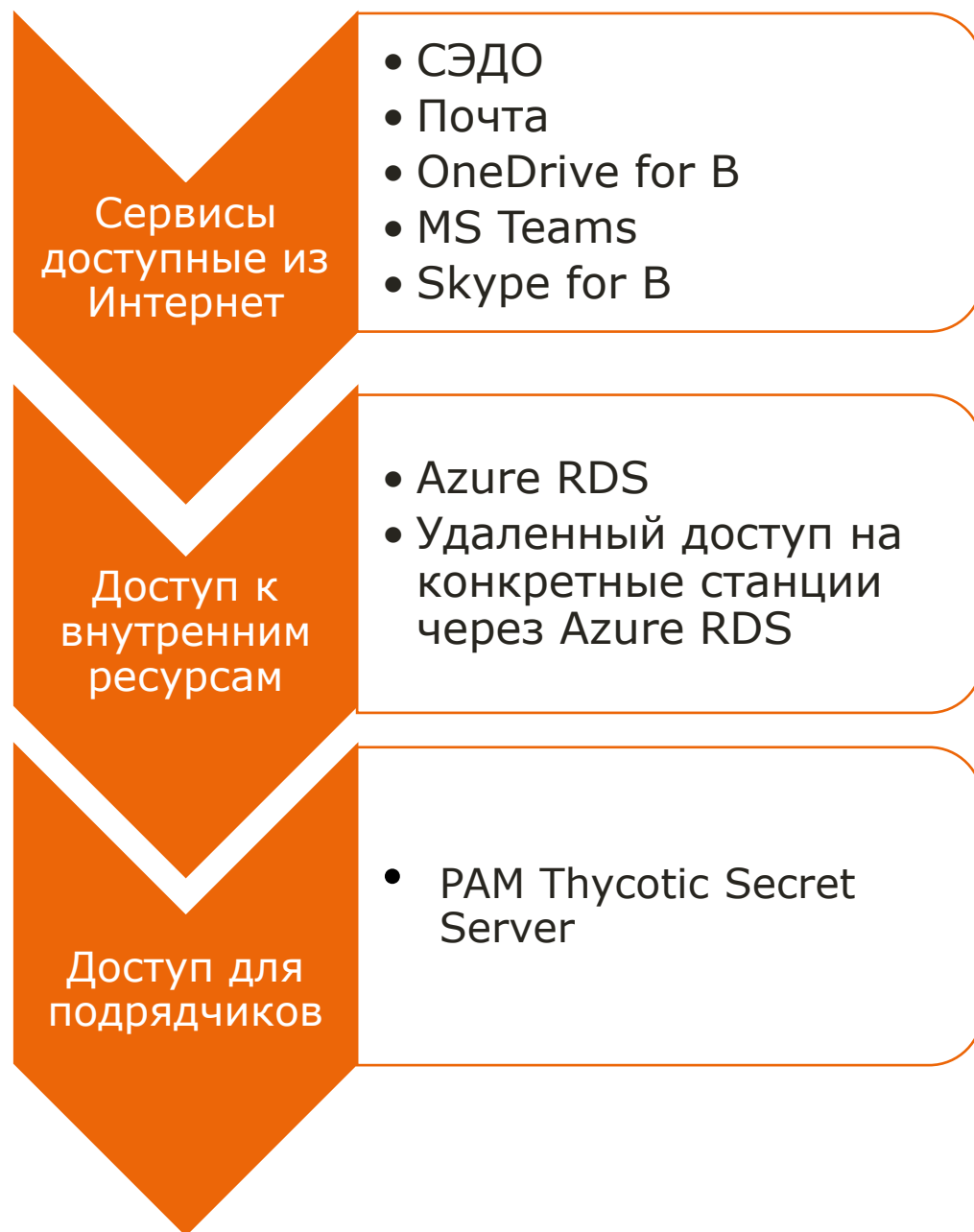


Обеспечение
соблюдения
аутентификации
Zero-Trust



Полный
контроль и аудит

Решение в ПАО ТМК (Не корпоративные устройства)



Скорость развертывания

Удобство пользователя

Подключение с любого устройства

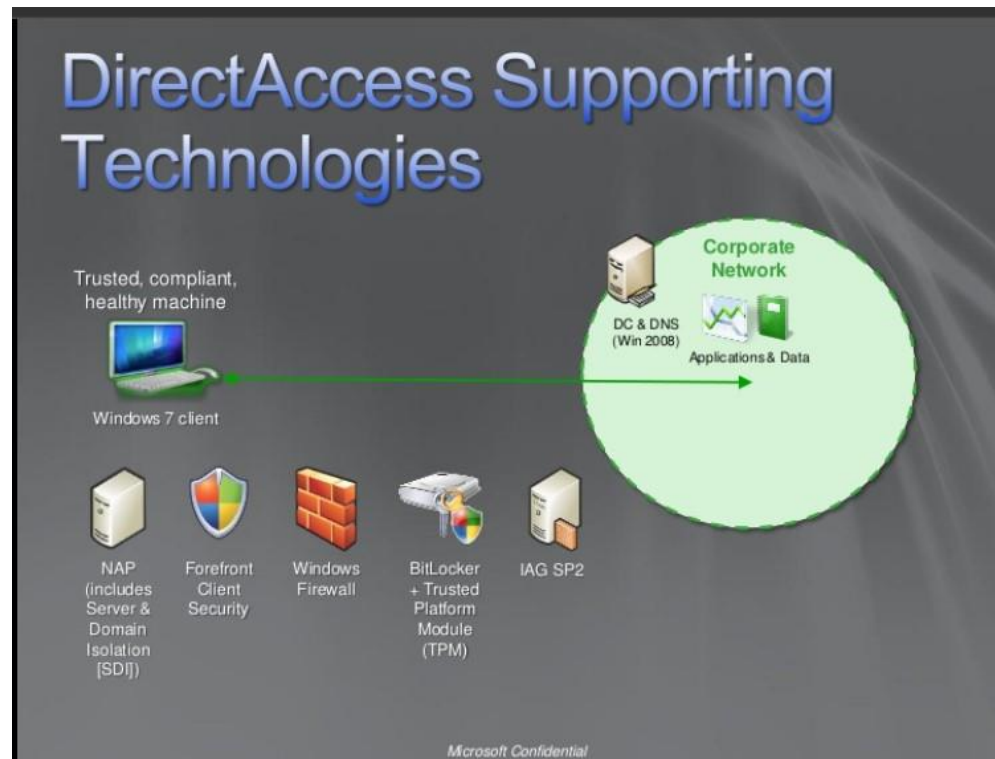
Удобство сопровождения

Требования ИБ Учтены

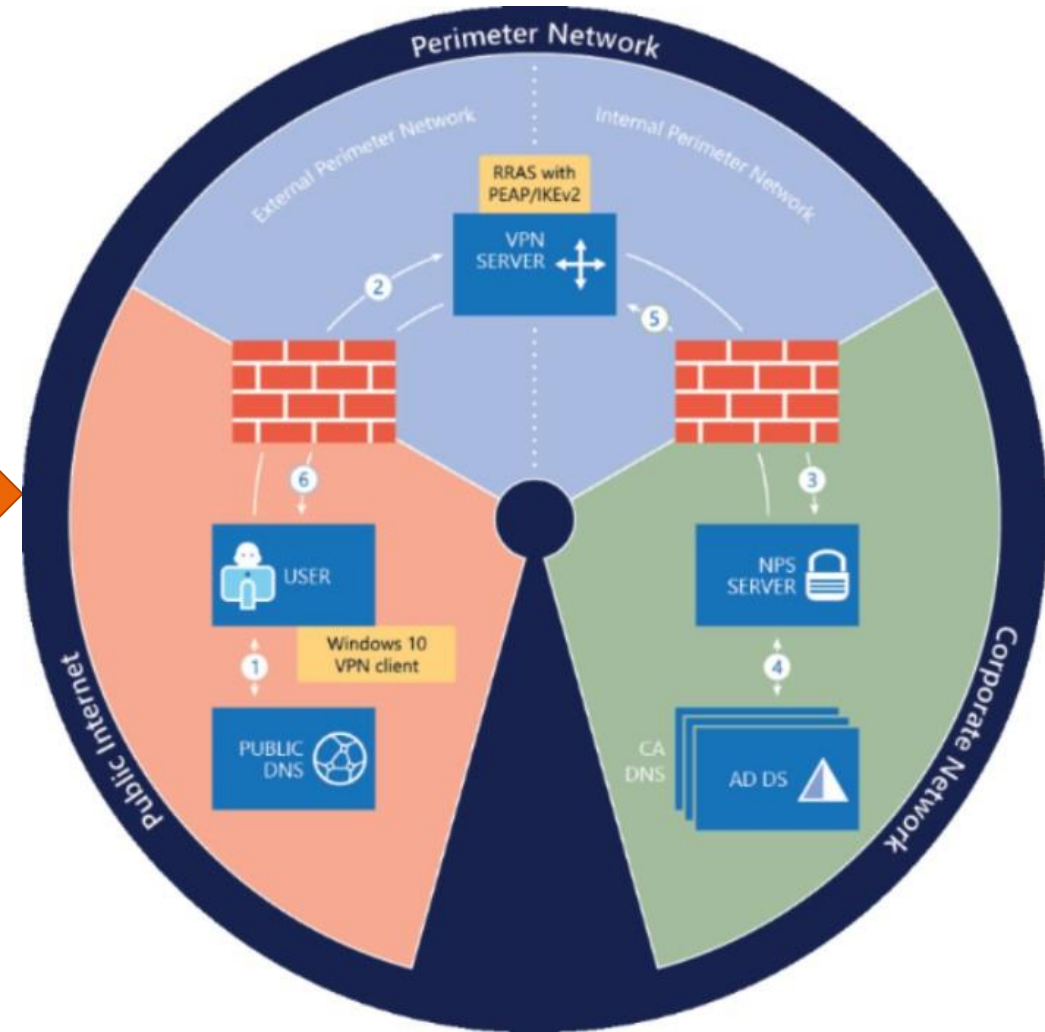
- MFA
- Установка средств защиты
- Установка обновлений
- Обновления ПО
- Подрядчикам предоставляется доступ напрямую к необходимым сервисам

Always ON VPN это следующий этап развития Direct Access

Direct Access



Always ON VPN



Решение в ПАО ТМК (Always ON VPN)



Требование для клиентских устройств

- Клиент должен быть подключённым к домену.
- клиент должен иметь выпущенный сертификат машины.
- клиент должен работать под Windows 10 1709 или более новой версией, причём эту возможность имеют исключительно SKU Enterprise или Education.
- Туннель устройства может быть только IKEv2.

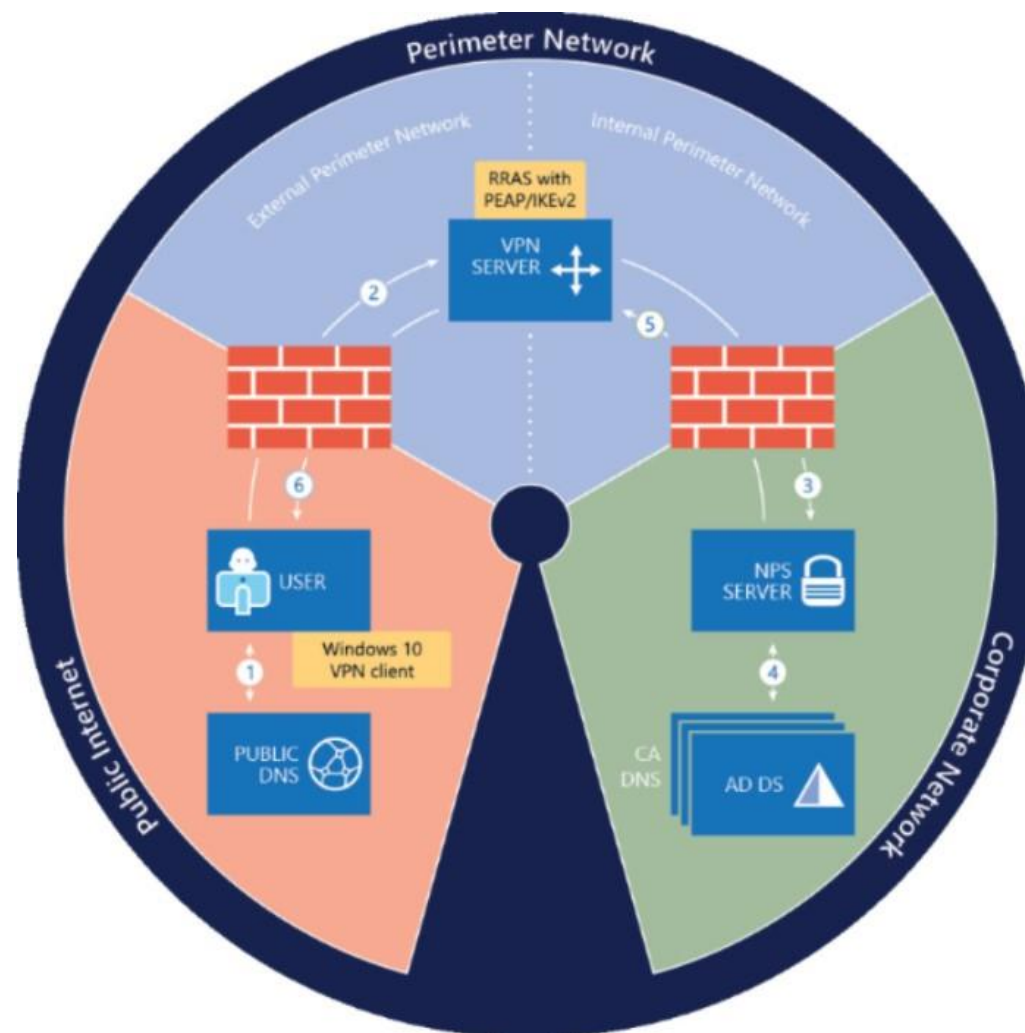


Решение в ПАО ТМК (Always ON VPN)



Что иметь в своей инфраструктуре

- Сервер удалённого доступа
- NPS (Network Policy Server)
- Сервер доменных служб Active Directory
- Microsoft Intune (не обязателен)



Решение в ПАО ТМК (Always ON VPN)



Управление клиентскими устройствами через Microsoft Intune

- Позволяет создать разные профили конфигурации, для отправки на различные группы устройств
- Профиль содержит тонкие настройки по фильтрации сетевого трафика так же позволяет определять сети, которые будут входит в VPN домен данного профиля
- Возможность отслеживать состояния подключенных клиентских устройств
- Гибкость управления

admin center

Home > Devices > AOVPN Device Users >

VPN ...

Windows 10 and later

1 Configuration settings 2 Review + save

Base VPN *

Apps and Traffic Rules

Associate WIP or apps with this VPN ⓘ Not configured

Network traffic rules for this VPN connection ⓘ Add Import

Name ↑↓	App type ↑↓
No data	

Conditional Access

DNS Settings

Proxy

Split Tunneling

Trusted Network Detection

Review + save Cancel

Add Row

Network traffic rules for this VPN connection

Careful: By adding network rules, the VPN connection will be limited to only the rules specified. When adding traffic rules, make sure to add a catch-all rule that is least restrictive, to avoid VPN issues.

Name * Not configured

Rule type ⓘ None

Protocol ⓘ Not configured

Local port ranges ⓘ Import Export

Lower port Upper port

e.g. 8080 e.g. 9080

Remote port ranges ⓘ Import Export

Lower port Upper port

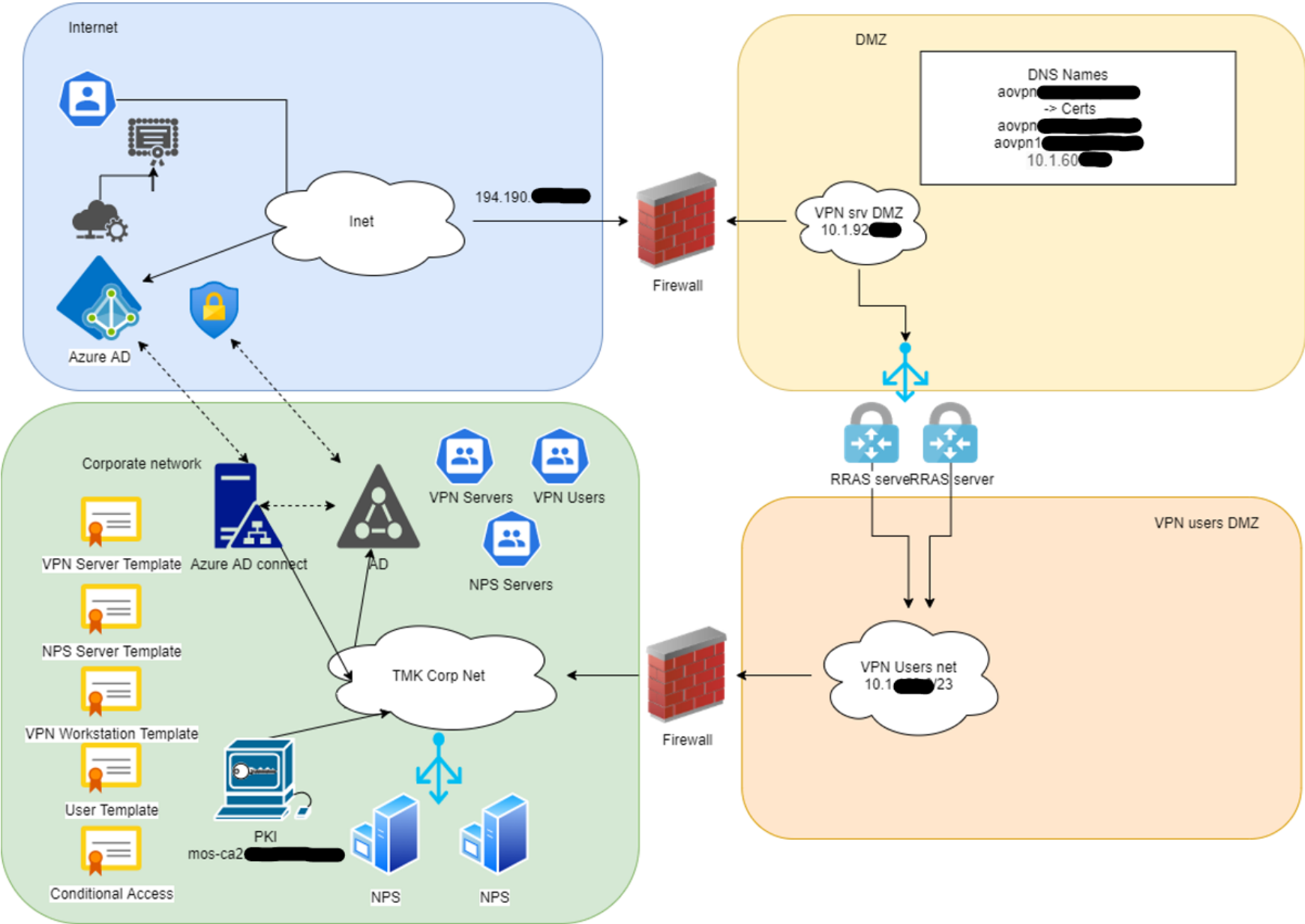
e.g. 8080 e.g. 9080

Local address ranges ⓘ Import Export

Lower IPv4 address Upper IPv4 address

Save Cancel

Решение в ПАО ТМК (Корпоративные устройства)



Спасибо за внимание!

Вопросы?



Узнай больше
о компании ТМК



ТМК eTrade
Интернет-магазин труб



Премиальные резьбовые
соединения ТМК UP