WHITEPAPER

Работа из дома

Решения с использованием продуктов и услуг NComputing

Пандемия COVID-19 изменяет привычный нам ритм работы. Вынужденный режим самоизоляции лишает предприятия их талантов. Нормальный рабочий режим становится невозможен, а жесткая реальность заключается в том, что работа на дому (WFH) больше не является роскошью; это необходимость. Независимо от того, были ли вы знакомы с продуктами для виртуализации или же вынуждено пришли к такому подходу, наша задача - показать различные способы виртуализации вашего офиса.

Вступление

Сценарии, описанные в данном документе, вращаются вокруг людей, работающих удаленно. Требования к их домашнему офису просты - клавиатура, мышь, монитор (или два) и устройство доступа. Эти устройства могут быть физическим оборудованием, таким как ПК, ноутбуки или тонкие клиенты. Они также могут быть программными решениями. Приведенные здесь варианты использования помогут вам определить наиболее подходящие решения для ваших нужд.

NComputing предлагает комплексные и гибкие решения для виртуализации и организации домашних офисов. Мы создали линейку продуктов, которые дополняют сценарии, обсуждаемые здесь. Мы начнем с простых решений, таких как наша платформа vSpace Pro, и постепенно будем переходить к более сложным: Microsoft Remote Desktop Services, VERDE VDI и Citrix.

NComputing предоставляет системы виртуализации настольных систем по всему миру уже 17 лет. Это наша специальность, так что давайте начнем.

Зачем это нужно?

Управление настольными компьютерами и ноутбуками сотрудников - это дорогостоящая и трудоемкая реальность для ИТ. Даже с современными инструментами управления настольными системами, обновление операционных систем и приложений, добавление новых пользователей и поддержание соответствующих уровней безопасности может стать серьезной головной болью. Когда объекты управления физически удалены от администраторов, это еще больше усложняет ситуацию.
Виртуализация рабочих столов - это способ решить многие из этих проблем.

NComputing®
Compute Smartly™

Преимущества для пользователей:

- **Повышенная гибкость и мобильность:** Пользователи могут получать доступ к своим приложениям и виртуальным рабочим столам из любого места, используя различные устройства, такие как тонкие клиенты и домашние ПК, без ущерба для производительности.
- **Аппаратная независимость:** Старые компьютеры, на которых все еще работают устаревшие ОС, такие как Windows XP, могут использовать расширенные возможности современных ОС, таких как Windows 10, работающих в виртуальной среде на серверах.
- **Непрерывность бизнеса и аварийное восстановление:** Бизнес может быть непрерывным за счет быстрого устранения сбоев оборудования.

Преимущества для IT:

- **Простота развертывания и управления:** Администраторы могут легко управлять виртуальными рабочими столами из единого центра и быстро предоставлять их по мере необходимости, устраняя необходимость управлять каждым пользовательским устройством независимо.
- **Снижение затрат:** ИТ-специалисты могут сэкономить на стоимости оборудования, используя более дешевые тонкие клиенты вместо традиционных ПК. Тонкие клиенты потребляют меньше энергии и требуют меньшего внимания, обеспечивая дополнительную экономию на эксплуатационных расходах.
- **Усиленная безопасность:** Конфиденциальные данные остаются в центре обработки данных, а не хранятся локально на компьютерах пользователей.
- **Защита данных:** Поскольку данные не хранятся локально, в случае любой аварии они быстро восстанавливаются, обеспечивая безотказную работу и надежность системы.

Типы виртуализации

Существует два основных метода виртуализации: серверные вычисления (SBC) и инфраструктура виртуальных рабочих столов (VDI). SBC - это гомогенные рабочие столы на основе терминальных сеансов для пользователей с одинаковыми требованиями. Например, дети в школьных компьютерных классах должны иметь доступ к одной и той же операционной системе и набору приложений. То же самое можно сказать, например, о сотрудниках колл-центров.
Развертывания VDI, как правило, представляют собой разнородные рабочие столы на основе виртуальных машин (ВМ), предоставляя гибкие вычислительные среды для различных типов пользователей и потребностей. Сотрудникам бухгалтерии, разработчикам программного обеспечения или маркетинговому отделу могут потребоваться разные операционные системы и набор приложений. VDI обеспечивает гибкость для удовлетворения любых потребностей.
Критическое различие между архитектурами виртуальных рабочих столов SBC и VDI заключается в методах предоставления операционной системы в виртуальных рабочих столах. VDI использует полностью независимые экземпляры операционных систем для каждого виртуального рабочего стола и обеспечивает взаимно-однозначное взаимодействие между операционной системой (ОС) и пользователем.
С помощью виртуализации SBC один экземпляр операционной системы поддерживает несколько пользователей. Все они имеют свои персональные учетные записи в этой системе, обеспечивая взаимодействие одной ОС и множества пользователей. Хотя производительность и опыт пользователей очень похожи, опыт администрирования сильно отличается, и стоит понять, как на них влияют различия между двумя архитектурами.

SBC-based platforms

Эта архитектура позволяет пользователям совместно использовать одну среду рабочего стола сервера в виде отдельных сеансов. Эта общая среда может работать на серверах в ЦОД или на ПК в офисе или классе. Для небольших пользовательских сред (менее 100) не требуется гипервизор, что делает его чрезвычайно простым в настройке и развертывании. В случае больших развертываний общая среда может работать внутри виртуальной машины на сервере. Несколько виртуальных машин на нескольких серверах могут масштабировать развертывание до тысяч пользователей.

- Несколько пользователей используют одну ОС.
- Приложения находятся в одной ОС.
- Изоляция терминальных сессий пользователей.

VDI-based platforms

Эта архитектура использует гипервизор для запуска ОС на виртуальной машине (ВМ), отсоединяя ее от аппаратного обеспечения ПК. Обычно несколько виртуальных машин работают на серверах в ЦОД, изолируя среду пользователей от физического устройства, позволяя пользователям получать доступ к своим виртуальным рабочим столам с любого ПК, ноутбука или тонкого клиента из любого места. А поскольку вычислительные ресурсы централизованы, управление и обслуживание упрощаются для ИТ.

- У каждого пользователя есть персональная ОС (ВМ).
- Приложения находятся на отдельной ОС (ВМ).
- Изоляция пользователей на основе ВМ.

Четыре платформы

Следующие четыре платформы будут подробно рассмотрены в наших случаях использования. Вот краткое введение каждого из них и той роли, которую NComputing играет в них.

vSpace PRO

vSpace Pro - это комплексное решение для предоставления пользователям рабочих столов Windows. Хранение данных и выполнение программ осуществляется на серверах, а не на локальных компьютерах. Вы получаете производительность, подобную ПК, благодаря серверным вычислениям (SBC). vSpace Pro - это система виртуализации сеансов. Каждый пользователь получает свою рабочую область, но все пользователи используют одинаковую операционную систему и приложения.

Эта платформа поддерживает 11 популярных операционных систем Windows для использования с тонкими клиентами NComputing, Chromebook и ПК, на которых установлено программное решение LEAF OS. Для работы сеансов платформа vSpace Pro использует собственный протокол UXP.

vSpace Pro предоставляет готовое решение для централизованного управления всеми пользовательскими сеансами и устройствами.

Microsoft

Службы удаленных рабочих столов (RDS) - это платформа для виртуализации приложений и рабочих столов, которая может быть развернута как на локальных серверах, так и на основе облачных сервисов.

Для работы с Microsoft RDP компания NComputing предлагает специально разработанные и оптимизированные тонкие клиенты RX-RDP и RX420 (RDP), поддерживающие Microsoft RemoteFX и обеспечивающие простоту развертывания и высокую производительность при работе с инфраструктурой Microsoft Windows Server или VDI.

Кроме того, компания NComputing реализовала нестандартные мультимедийные возможности стандартного развертывания RDS с помощью серверного программного пакета SuperRDP, позволяющего повысить производительность потоковой передачи HD-видео локально или из Интернета.

verde

VERDE VDI - это разработанное с нуля решение на базе ядра Linux. Оно поддерживает широкий спектр конечных устройств доступа, включая ПК с различными ОС, тонкие и программные клиенты, а также любые браузеры с поддержкой HTML5, предоставляя пользователям рабочие столы Windows или Linux. Поддерживаемые протоколы включают UXP, RDP и SPICE.
VERDE VDI - это безопасное, простое в использовании решение VDI корпоративного уровня. Он предлагает три важных компонента возможностей:

- Клиенты Windows и Linux являются равноправными
- Задержка WAN устраняется путем децентрализации обработки VDI на границе вашей организации.
- Она охватывает вычислительную структуру конечного пользователя от локального до облачного или гибридного с использованием нашей уникальной технологии Cloud Branch.

Безопасная платформа VERDE VDI предотвращает проникновение в систему вредоносных программ, вирусные атаки, утечки данных и несанкционированный доступ к внутренней сети. Кроме того, весь трафик зашифрован.

CITRIX

Citrix разрабатывает серверные, сетевые и облачные технологии, в том числе программные решения для виртуализации рабочих столов и приложений.

NComputing разработал устройства доступа, оптимизированные для Citrix HDX. Они соответствуют производительности, безопасности и управляемости, необходимым для требовательных пользователей Citrix.

NComputing является одним из участников программы Citrix Ready Workspace Hub, направленной на ускорение преобразования рабочих мест и решение инновационных сценариев использования корпоративного IoT.

WFH Solutions by Use Case Scenario

NComputing supports extensive and flexible work-from-home scenarios depending on the solution type. Below is a basic overview of the use case scenarios.

vSpace PRO	Microsoft	verde	CITRIX
EASY TO DEPLOY	EASY TO DEPLOY	EASY TO DEPLOY	EASY TO DEPLOY
FEATURE SET	FEATURE SET	FEATURE SET	FEATURE SET
BUDGET FRIENDLY	BUDGET FRIENDLY	BUDGET FRIENDLY	BUDGET FRIENDLY

Локальное развертывание

- 1. VPN
- 2. Перенаправление портов

Локальное развертывание

- 3. VPN
- 4. RD Шлюз
- 5. Перенаправление портов

Развертывание в Azure Cloud / Windows Virtual Desktop

- 6. Azure RD Шлюз

Только сеансы

- 10. VPN
- 7. Перенаправление портов

Только удаленные ПК

- 11. VPN
- 8. Перенаправление портов

Удаленные ПК и сеансы

- 12. VPN
- 9. Перенаправление портов

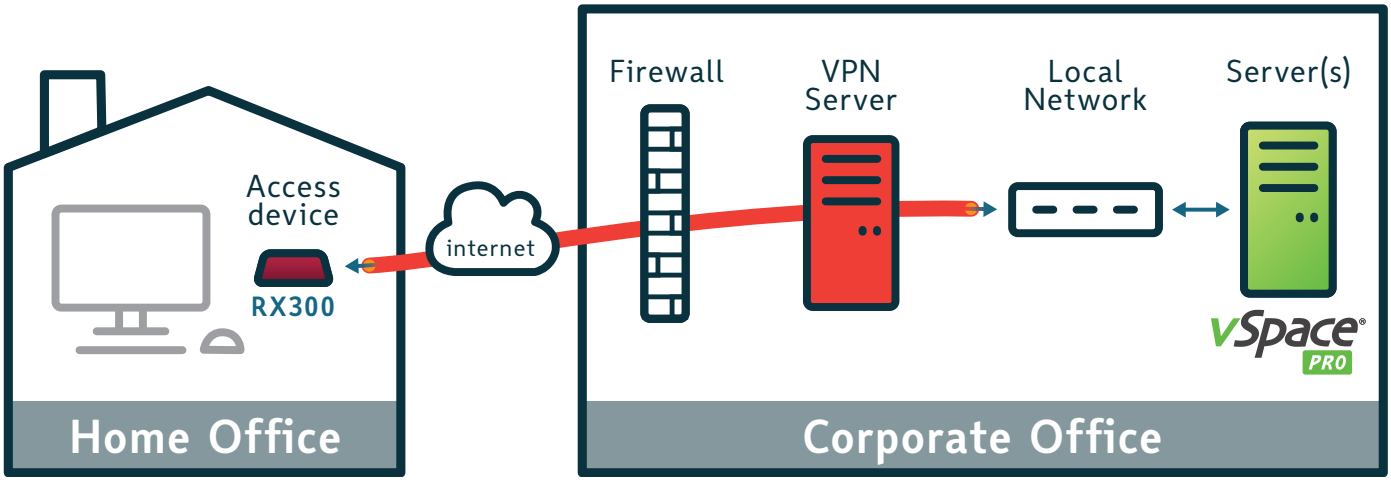
Локальное развертывание

- 13. Netscaler/gateway

Развертывание Citrix Cloud

- 14. Служба Citrix Gateway

Сценарий 1: vSpace Pro - VPN



Профиль:

- Сеть офисов малого и среднего размера
- Инфраструктура VPN
- Нужен доступ к внутренним ресурсам

Общее описание:

VPN позволяет людям устанавливать безопасные соединения с удаленной компьютерной сетью. Они могут получить доступ к защищенным ресурсам в этой сети, как если бы они подключались непосредственно к серверам. Клиенты, которые развертывают программное обеспечение vSpace Pro, могут получать удаленный доступ к своим пользовательским сеансам через тонкие клиенты NComputing, которые поддерживают VPN.

Процесс установки:

1. Настройте и инициализируйте VPN-сервер, включая IP-адрес, пул адресов DHCP и выбрав тип шифрования.
2. Создайте учетные записи пользователей. Введите имя пользователя и пароль, а также установите права доступа: ко всей локальной сети или только к маршрутизатору.
3. Настройте тонкие клиенты для подключения. Как правило, все, что требуется, это адрес VPN-сервера, имя пользователя и пароль.

Поддерживаемые устройства:

- **RX300**
- **LEAF OS**
- **vSpace Pro Client** для Windows и Chromebook

Платформа:

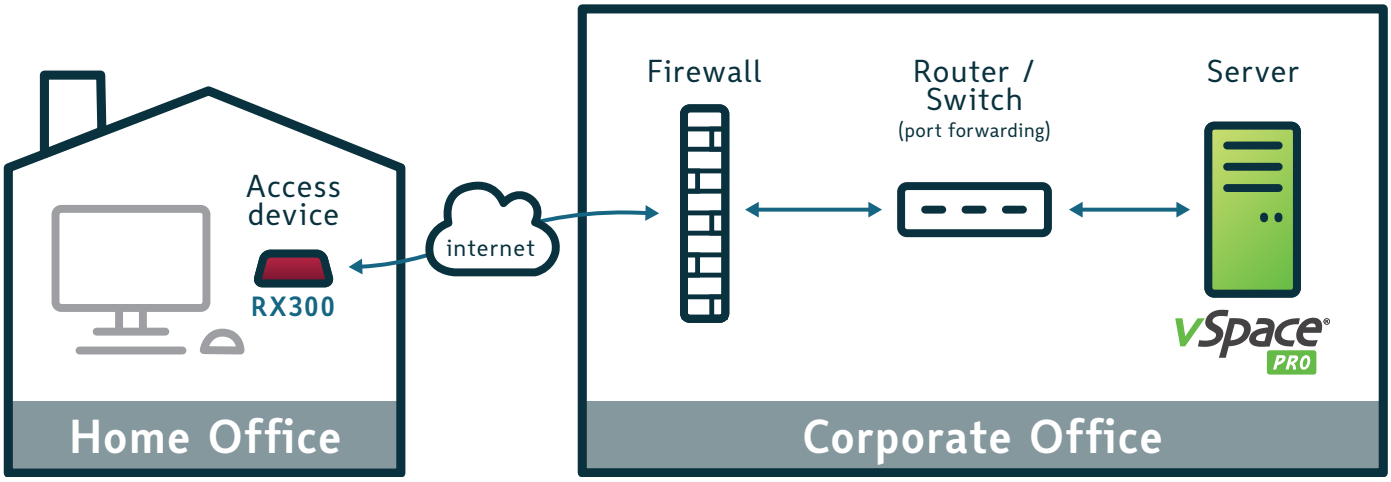
- **vSpace Pro Enterprise**

Особенности реализации:

- **VPN добавляет дополнительные уровни защиты:**
  - Используется только один открытый порт, который защищен именем пользователя и паролем.
  - Весь трафик шифруется.
  - Внутренние ресурсы защищены паролем.
- Предоставляет доступ ко всем развернутым серверам vSpace Pro и внутренним ресурсам.
- Умеренно простая конфигурация. Требуется информация о пользователе, но не требуется информация о внутренних ресурсах.
- Старые семейства устройств NComputing (**серии L, M300, MX**) не поддерживают VPN.
- Необходимо иметь достаточное количество лицензий на места VPN.
- Трафик во внутреннюю сеть и из нее может быть немного медленнее из-за процесса шифрования.

Additional resources: See Appendix A

Сценарий 2: vSpace Pro - Перенаправление портов



Профиль:

- Сеть офисов малого и среднего размера
- Нет инфраструктуры VPN
- Нужен доступ к внутренним ресурсам

Общее описание:

Переадресация портов сопоставляет порт на IP-адресе вашего маршрутизатора (ваш публичный IP-адрес) с портом и IP-адресом сервера vSpace Pro, к которому вы хотите получить доступ. Правило переадресации портов перехватывает трафик данных на публичный IP-адрес маршрутизатора вашей компании и перенаправляет его на IP-адрес внутреннего сервера vSpace Pro. Это позволяет тонким клиентам NComputing подключаться к серверу vSpace Pro в частной сети. Обычно ваш провайдер использует преобразование сетевых адресов (NAT) для обеспечения подключения к Интернету через маршрутизатор. Для включения опции переадресации портов вам потребуется изменить конфигурацию вашего маршрутизатора.

Процесс установки:

1. Найдите внутренний IP-адрес вашего сервера vSpace Pro.
2. Найдите публичный адрес вашего роутера.
3. Создайте правило переадресации портов (порт 27605) на вашем маршрутизаторе.
4. При необходимости настройте динамический DNS (DDNS) для IP-адреса маршрутизатора (т.е. вам не нужно беспокоиться об изменении публичного IP-адреса маршрутизатора вашим провайдером).
5. Настройте тонкие клиенты NComputing для подключения к общедоступному IP-адресу вашего маршрутизатора и/или DDNS маршрутизатора.

Предупреждение: открывая доступ к своему серверу из Интернета - убедитесь, что используете надежный пароль.

Поддерживаемые устройства:

- Тонкие клиенты **RX300**, **L250**, **L300**, **L350**, **M300**, **MX100**
- **LEAF OS**
- **vSpace Pro Client** для Windows и Chromebook

Платформа:

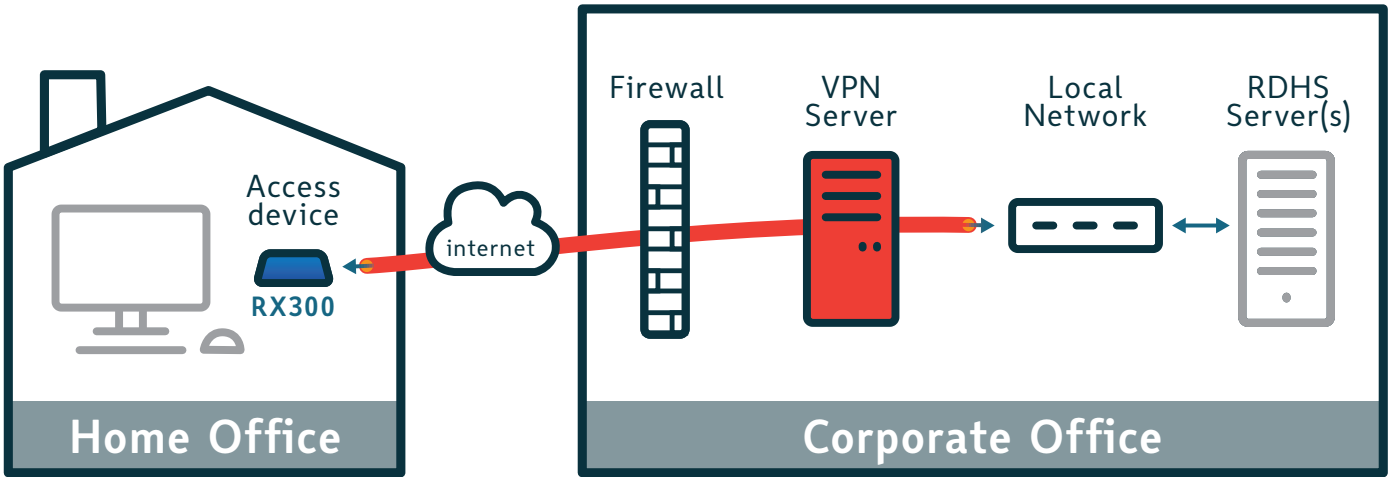
- **vSpace Pro Enterprise**

Особенности реализации:

- Простота в настройке.
- Перенаправляет пользователя в частную сеть без пароля.
- Работает с динамическим DNS.
- Поддерживает все клиенты NComputing, совместимые с vSpace Pro.
- Безопасность зависит от того, насколько хорош брандмауэр маршрутизатора; Требуется установить надежный пароль для учетных записей ваших пользователей.
- Не весь трафик зашифрован.
- На производительность сеанса пользователя может повлиять задержка.
- Для доступа к нескольким серверам vSpace Pro требуются правила переадресации нескольких портов.

Additional resources: See Appendix A

Сценарий 3: Microsoft RDS - VPN



Профиль:

- Сеть офисов малого и среднего размера
- Нет настройки шлюза RD
- Инфраструктура VPN
- Нужен доступ к внутренним ресурсам

Общее описание:

Клиенты, которые развертывают RDSH-серверы, могут получать доступ к своим сеансам удаленно, используя тонкие клиенты NComputing, поддерживающие VPN.

VPN позволяет устанавливать безопасные соединения с удаленной компьютерной сетью. Пользователи могут получить доступ к защищенным ресурсам в этой сети, так как если бы они подключались непосредственно к серверам.

Процесс установки:

1. Настройте и инициализируйте VPN-сервер, включая IP-адрес, пул адресов DHCP и выбрав тип шифрования.
2. Создайте учетные записи пользователей. Введите имя пользователя и пароль, а также установите права доступа: ко всей локальной сети или только к маршрутизатору.
3. Настройте тонкие клиенты для подключения. Как правило, все, что требуется, это адрес VPN-сервера, имя пользователя и пароль.

Поддерживаемые устройства:

- Тонкие клиенты **RX-RDP**, **RX420(RDP)**, **RX300**.
- **LEAF OS***

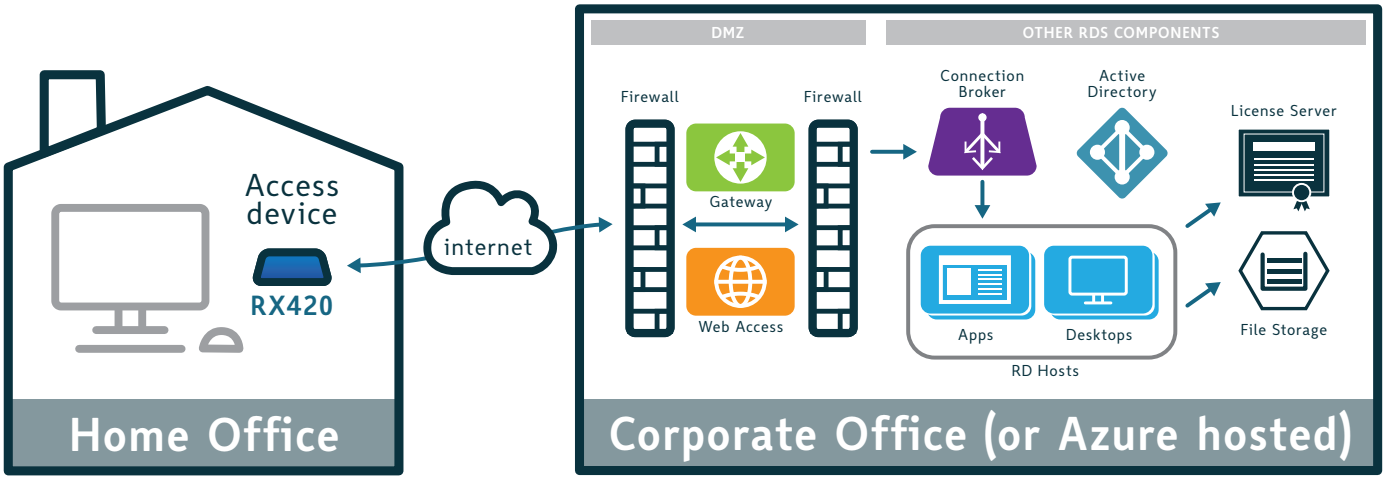
Особенности реализации:

- **VPN добавляет дополнительные уровни защиты:**
  - Используется только один открытый порт, который защищен именем пользователя и паролем.
  - Весь трафик шифруется.
  - Внутренние ресурсы защищены паролем.
- Предоставление доступа ко всем развернутым серверам RDSH и внутренним ресурсам.
- Умеренно простая конфигурация. Требуется информация о пользователе, но не требуется информация о внутренних ресурсах.
- Необходимо иметь достаточное количество лицензий на места VPN.
- Трафик во внутреннюю сеть и из нее может быть немного медленнее из-за процесса шифрования.

* Поддержка будет добавлена до Q3 2020.

Additional resources: See Appendix A

Scenario 4: Microsoft RDS - RD Gateway



Профиль:

- Офисная сеть малого и среднего размера
- Настроен шлюз RD Gateway
- Нет инфраструктуры VPN
- Нужен доступ к внутренним ресурсам

Общее описание:

Шлюзовый сервер удаленного рабочего стола используется для предоставления защищенных соединений, использующих HTTPS-шифрование, с компьютеров за пределами корпоративной сети. Конфигурация была упрощена, начиная с Windows Server 2012.

Процесс установки:

1. Установите роль шлюза RD в Windows Server (требуется существующее развертывание RDS).
2. Настройте сертификат SSL для сервера шлюза удаленных рабочих столов. (SSL-сертификаты используются для шифрования связи между тонкими клиентами RDS и серверами RD Gateway. Самозаверяющее имя SSL-сертификата должно соответствовать полному доменному имени (FQDN) сервера RD Gateway.
3. Запустите диспетчер шлюза удаленных рабочих столов и настройте «Политику авторизации подключений» и «Политику авторизации ресурсов».
4. Включите/перенаправьте TCP-порт 443 на брандмауэре на сервер шлюза удаленных рабочих столов.
5. Экспортируйте самозаверяющие публичные сертификаты и скопируйте их на поддерживаемые тонкие клиенты.
6. Настройте тонкие клиент для связи со шлюзом удаленных рабочих столов, введя имя FQDN.

Поддерживаемые устройства:

- Тонкие клиенты **RX-RDP**, **RX420**(RDP), **RX300**
- **LEAF OS***

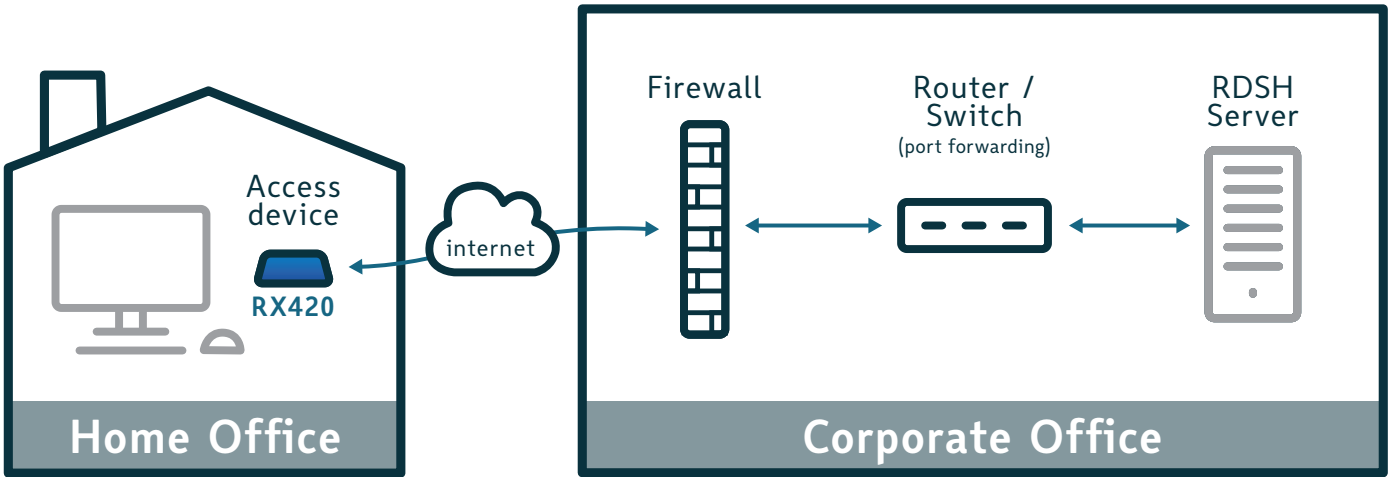
Особенности реализации:

- Не требуется VPN.
- Разрешает удаленные подключения через брандмауэр (без открытия порта 3389).
- Поддерживается всеми клиентами, поддерживающими NComputing RDP.
- Гибкое развертывание (локальное или облачное).
- Дополнительные действия по настройке RD Gateway и управлению сертификатами.

* Поддержка будет добавлена Q3 2020.

Additional resources: See Appendix A

Сценарий 5: Microsoft RDS - Перенаправление портов



Профиль:

- Сеть офисов малого и среднего размера
- Нет настроенного шлюза RD Gateway
- Нет инфраструктуры VPN
- Нужен доступ к внутренним ресурсам

Общее описание:

Клиенты, которые развертывают RDSH-серверы, могут получать удаленный доступ к своим пользовательским сеансам с помощью метода переадресации портов на маршрутизаторе. Однако такой подход может привести к уязвимостям безопасности (переадресация порта 3389) и должен быть последним вариантом, если у клиента нет RD Gateway или инфраструктуры VPN. Администратор должен установить надежные пароли для учетных записей, чтобы снизить уязвимость системы.

Переадресация портов сопоставляет порт на IP-адресе вашего маршрутизатора (ваш общедоступный IP-адрес) с портом и IP-адресом сервера RDSH, к которому вы хотите получить доступ. Правило переадресации портов перехватывает трафик данных на публичный IP-адрес маршрутизатора вашей компании и перенаправляет его на IP-адрес внутреннего сервера RDSH. Это позволяет тонким клиентам NComputing в публичной сети подключаться к серверу RDSH.

Обычно ваш провайдер использует преобразование сетевых адресов (NAT) для обеспечения подключения к Интернету через маршрутизатор. Для включения опции переадресации портов вам потребуется изменить конфигурацию вашего маршрутизатора.

Процесс установки:

1. Найдите внутренний IP-адрес вашего сервера vSpace Pro.
2. Найдите публичный адрес вашего роутера.
3. Создайте правило переадресации портов (порт 27605) на вашем маршрутизаторе.
4. При необходимости настройте динамический DNS (DDNS) для IP-адреса маршрутизатора (т.е. вам не нужно беспокоиться об изменении публичного IP-адреса маршрутизатора вашим провайдером).
5. Настройте тонкие клиенты NComputing для подключения к общедоступному IP-адресу вашего маршрутизатора и/или DDNS маршрутизатора.

Предупреждение: открывая доступ к своему серверу из Интернета - убедитесь, что используете надежный пароль.

Поддерживаемые устройства:

- Тонкие клиенты **RX-RDP**, **RX420**(RDP), **RX300**
- **LEAF OS***

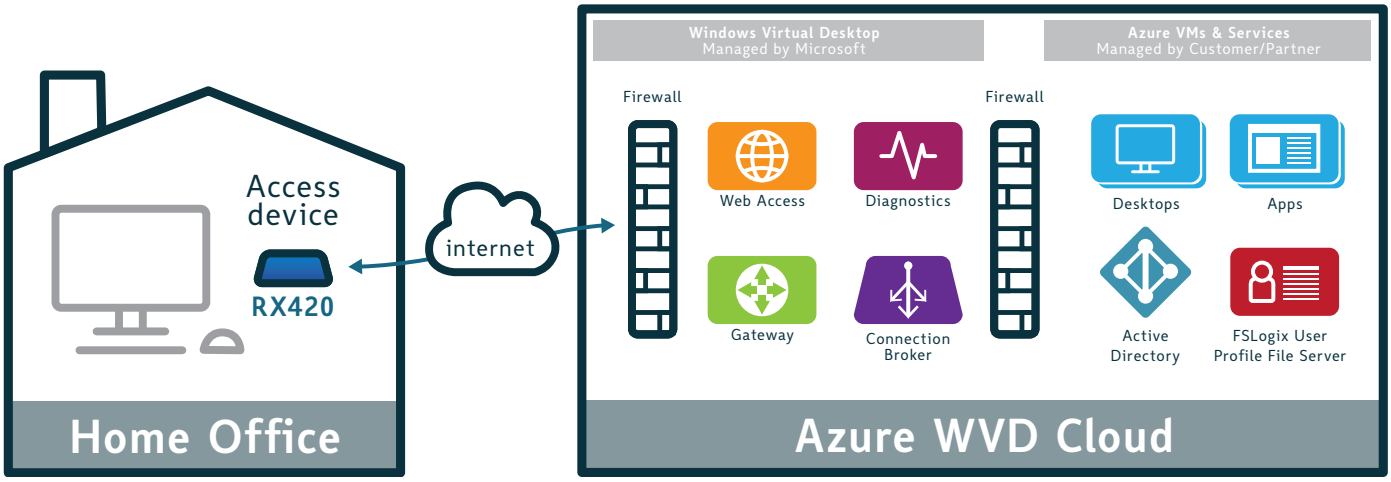
Особенности реализации

- Простота настройки.
- Требуется только адрес и порт RDSH-сервера.
- Работает с динамическим DNS.
- Безопасность зависит от качества брандмауэра;
- Требуются надежные пароли пользователей (могут быть уязвимы для атаки методом перебора).
- На производительность сеансов пользователей может повлиять задержка.

* Поддержка будет добавлена Q3 2020.

Additional resources: See Appendix A

Сценарий 6: Microsoft Virtual Desktop (WVD) – Azure Cloud



Профиль:

- Сеть офисов малого и среднего размера
- Заинтересованность в DaaS (рабочий стол как услуга)
- Нет локального Microsoft RDS
- Нет инфраструктуры VPN
- Нужен доступ к внутренним ресурсам

Общее описание:

Windows Virtual Desktop (WVD) - это служба виртуализации рабочих столов и приложений, запущенная компанией Microsoft в облачном сервисе Azure. Она позволяет настраивать многосессионные рабочие столы Windows 10 вместе с виртуальным офисом 365 ProPlus с соответствующими лицензиями Microsoft.

Процесс установки:

1. Первоначальная настройка WVD с помощью Azure и регистрация.
2. Подготовьте среду WVD с помощью PowerShell и настройте клиент Windows Virtual Desktop.
3. Настройте контроллер домена и виртуальные машины (например, виртуальную машину, диск, конфигурацию сети и т. д.).
4. Настройте VPN (ресурсы, сертификаты и т.д.).
5. Завершите настройку виртуального рабочего стола Windows (например, контроллер домена, Azure AD, виртуальные машины, назначение пользователей, публикация приложений и т.д.).

Поддерживаемые устройства:

- Тонкие клиенты **RX-RDP**, **RX420**(RDP), **RX300***
- **LEAF OS***

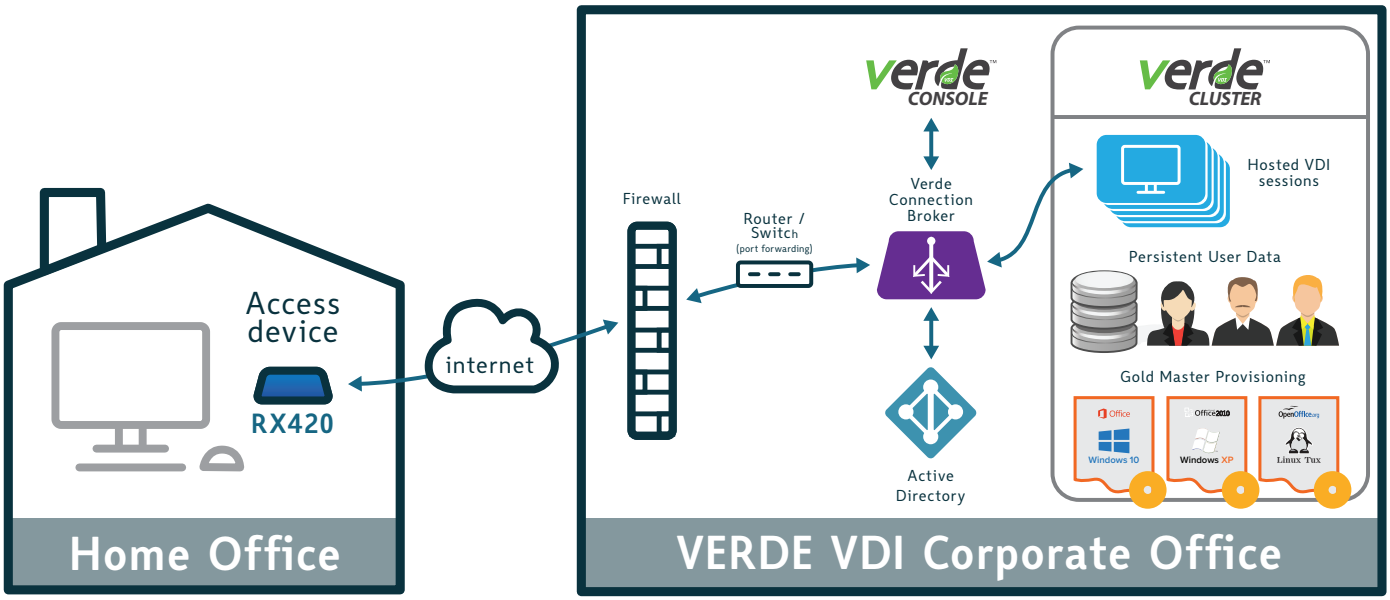
Особенности реализации:

- Легкий доступ пользователя из любой точки мира.
- Встроенная защита/межсетевой экран без VPN или переадресации портов.
- Масштабируемый и высокодоступный дизайн.
- Данные размещены на серверах сторонней организациеи (Microsoft), не нужны локальные резервные копии
- На взаимодействие с конечным пользователем могут повлиять регионы доступности Azure.
- Низкая стоимость запуска, но более высокая стоимость владения с течением времени.

* Поддержка будет добавлена Q3 2020.

Additional resources: See Appendix A

Сценарий 7: VERDE VDI – VM только сеансы: перенаправление портов



Профиль:

- Сеть офисов малого и среднего размера
- Нет инфраструктуры VPN
- Нужен доступный VDI

Общее описание:

Платформа виртуализации VERDE VDI от NComputing представляет собой специально разработанное универсальное решение, обеспечивающее безопасную, простую в использовании инфраструктуру VDI корпоративного уровня по очень доступной цене. VERDE VDI поставляет виртуальные рабочие столы Windows и Linux и идеально подходит для малого и среднего бизнеса.

Клиенты VERDE VDI, могут получить удаленный доступ к своим сеансам VDI с помощью метода переадресации портов на маршрутизаторе.

Customers can optionally enable the VERDE Gateway Feature to provide an additional layer of security and control for remote access. The VERDE Gateway Feature comes with the **VERDE VDI** solution.

Процесс установки:

1. Настройте и разверните VERDE VDI.
2. Найдите IP-адрес вашего брокера соединений VERDE.
3. Найдите публичный адрес вашего роутера.
4. Создайте правила переадресации портов 8443 и 48622 на вашем маршрутизаторе.
5. При необходимости настройте Динамический DNS (DDNS) для IP-адреса вашего маршрутизатора.

   (Вам не нужно беспокоиться об изменении публичного IP-адреса маршрутизатора вашим провайдером).
6. Тонкие клиенты NComputing подключаются к общедоступному IP-адресу вашего маршрутизатора и/или к DDNS.

Поддерживаемые устройства:

- Тонкие клиенты **RX-RDP**, **RX420**(RDP), **RX300**
- **LEAF OS***
- Клиент VERDE Windows

Платформа:

- VERDE VDI

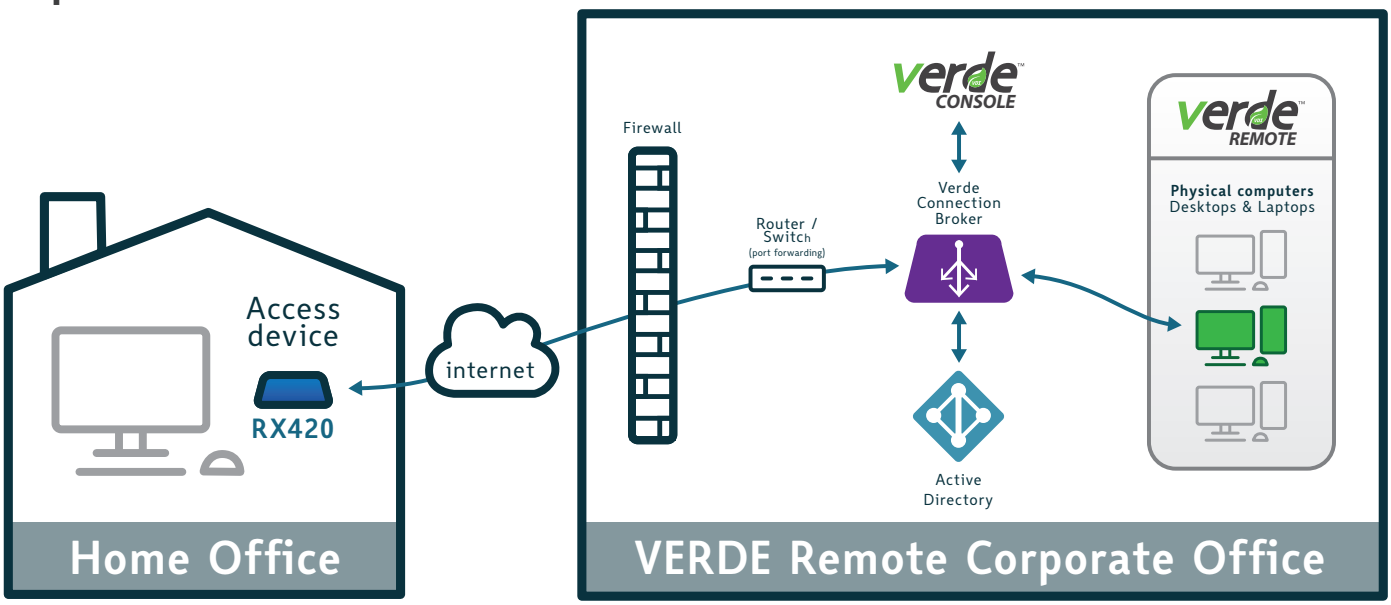
Особенности реализации:

- Сквозной SSL-шифрованный трафик без VPN.
- Истинное решение VDI, более простое в настройке и развертывании.
- Стоит дешевле, чем другие решения VDI
- (Необязательно) Функция шлюза VERDE обеспечивает дополнительный уровень безопасности и контроля для удаленного доступа.
- VERDE Connection Broker может быть не защищен.

* Поддержка будет добавлена Q3 2020.

Additional resources: See Appendix A

Сценарий 8: VERDE VDI – Только удаленные ПК: Перенаправление портов



Профиль:

- Сеть офисов малого и среднего размера
- Нет инфраструктуры VPN
- Необходим доступ к существующим физическим ПК в офисе.

Общее описание:

VERDE Remote Access - это простое в развертывании виртуальное устройство Linux, которое устанавливается в среде клиента. Это позволяет пользователям дома подключаться к своему ПК в корпоративном офисе и использовать его так, как если бы они сидели перед ним.

Функция удаленного доступа VERDE настраивается администратором для определения критериев подключения. Весь трафик данных надежно зашифрован, защищая физические ПК от несанкционированного удаленного доступа.

Администратор может легко отслеживать состояние подключения компьютеров и, при необходимости, принудительно отключать или выключать их.

Клиенты также могут включить функцию шлюза VERDE, чтобы обеспечить дополнительный уровень безопасности и контроля для удаленного доступа. Функция VERDE Gateway является частью VERDE VDI.

Процесс установки:

1. Настройте и разверните VERDE Remote Access.
2. Найдите IP-адрес вашего брокера соединений VERDE.
3. Найдите публичный адрес вашего роутера.
4. Создайте правила переадресации портов 8443 и 48622 на вашем маршрутизаторе.
5. При необходимости настройте динамический DNS (DDNS) для IP-адреса маршрутизатора вашей организации (Вам не нужно беспокоиться об изменении публичного IP-адреса маршрутизатора вашим провайдером).
6. Тонкие клиенты NComputing подключаются к общедоступному IP-адресу вашего маршрутизатора и/или к DDNS.

Поддерживаемые устройства*:

- Тонкие клиенты **RX-RDP**, **RX420**(RDP), **RX300**
- **LEAF OS**
- Клиент VERDE Windows

Платформа:

- VERDE VDI с удаленным доступом*

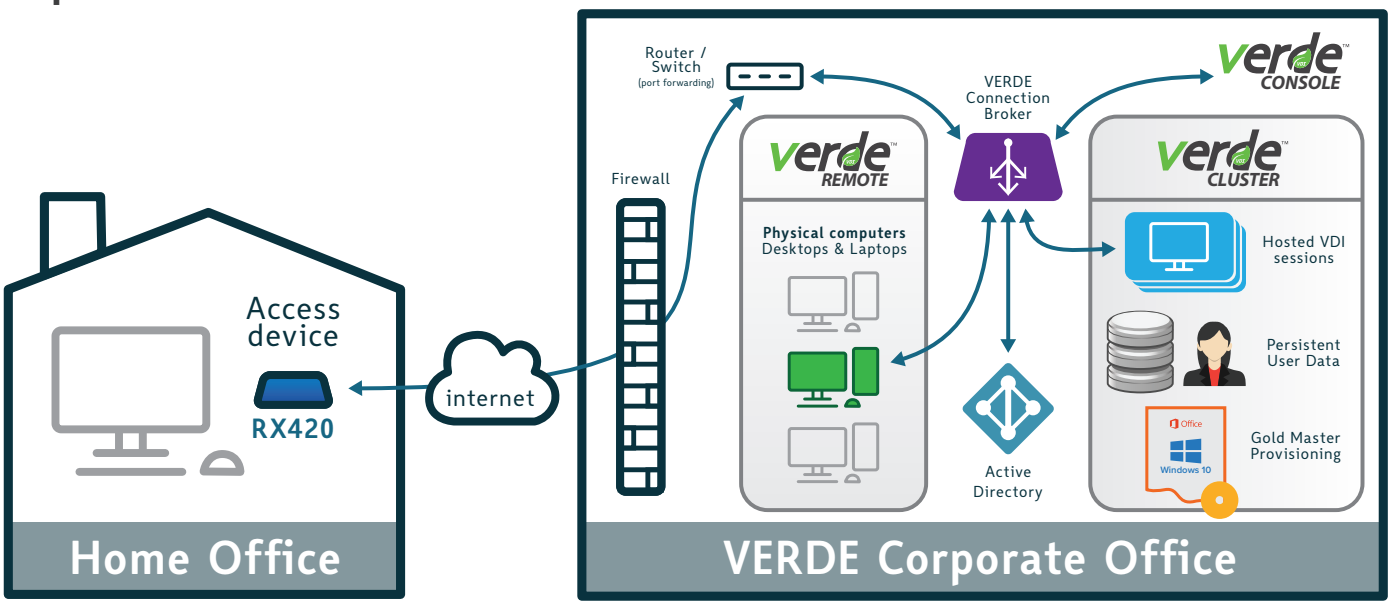
Особенности реализации

- Безопасный удаленный доступ. Сквозной SSL-шифрованный трафик между устройством доступа и физическими ПК без VPN.
- Требуется минимальная инфраструктура.
- (Необязательно) Функция шлюза VERDE для обеспечения дополнительного уровня безопасности и контроля для удаленного доступа.
- VERDE Connection Broker может быть не защищен.
- Удаленный компьютер должен оставаться включенным.

* Поддержка будет добавлена Q3 2020.

Additional resources: See Appendix A

Сценарий 9: VERDE VDI – сеансы и удаленные ПК: Перенаправление портов



Профиль:

- Сеть офисов малого и среднего размера
- Нет инфраструктуры VPN
- Нужен доступ к существующим ПК в офисе
- Нужен доступ к внутренним ресурсам
- Нужен доступный VDI

Общее описание:

VERDE VDI может быть развернут для обеспечения гибридных сеансов VDI и удаленного доступа к компьютеру через одного и того же безопасного посредника соединений VERDE.

VERDE VDI обеспечивает безопасную, простую в использовании инфраструктуру виртуальных рабочих столов корпоративного уровня. VERDE VDI поставляет виртуальные рабочие столы Windows и Linux.

Функция удаленного доступа VERDE может быть настроена администратором для определения критериев подключения, позволяющих удаленному пользователю подключаться к своему физическому ПК или ноутбуку в офисе. Весь трафик данных надежно шифруется и передается через устройство удаленного доступа VERDE, тем самым защищая физические ПК от несанкционированного удаленного доступа.

Мониторинг и контроль могут быть выполнены с помощью консоли VERDE.

Клиенты могут по желанию включить функцию шлюза VERDE обеспечить дополнительный уровень безопасности и контроля для удаленного доступа. Функция VERDE Gateway является частью VERDE VDI.

Процесс установки:

См. шаги из сценариев 7 и 8.

Поддерживаемые устройства:*

- Тонкие клиенты **RX-RDP**, **RX420**(RDP), **RX300**
- **LEAF OS**
- Клиент VERDE Windows

Платформа:

- VERDE VDI с удаленным доступом*

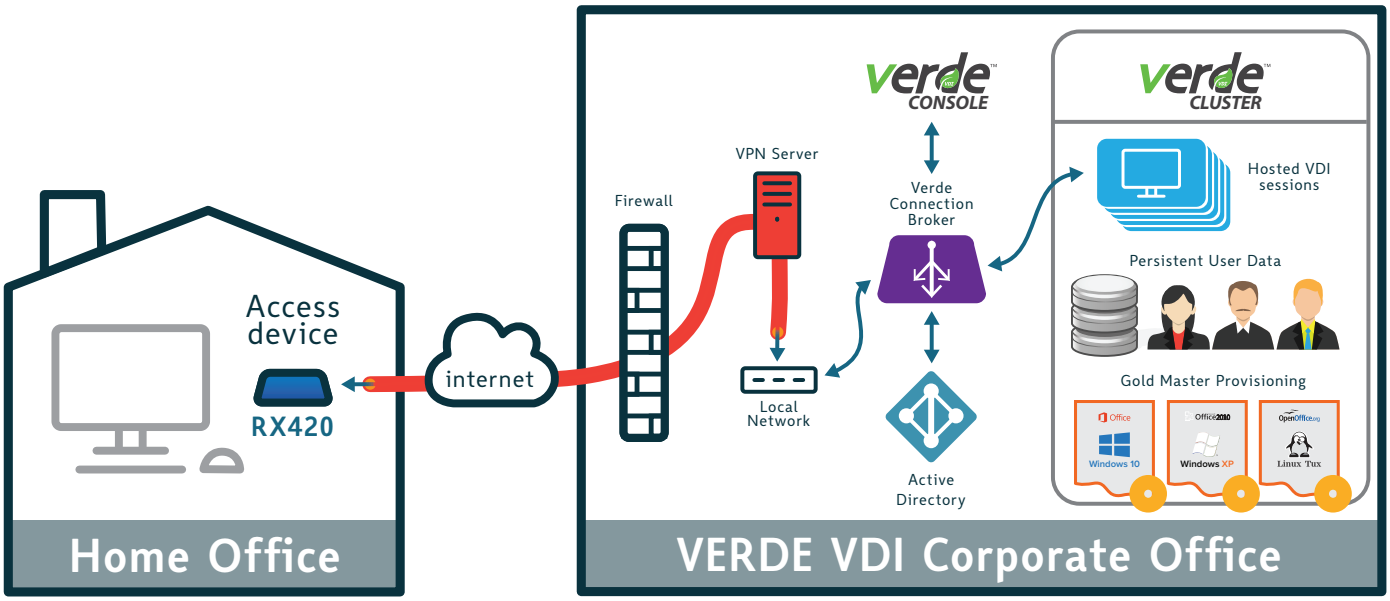
Особенности реализации:

- Полностью зашифрованный SSL трафик от устройства доступа NComputing к VERDE.
- Гибкое развертывание с гибридными сеансами VDI и удаленным доступом к физическим компьютерам.
- Обширный мониторинг и контроль с помощью консоли VERDE.
- (Необязательно) Функция шлюза VERDE для обеспечения дополнительного уровня безопасности и контроля для удаленного доступа.
- VERDE Connection Broker может быть не защищен.
- Удаленный компьютер должен оставаться включенным.

* Support will be included in June 2020 release.

Additional resources: See Appendix A

Сценарий 10: VERDE VDI – VM Только сеансы: VPN



Профиль:

- Сеть офисов малого и среднего размера
- Есть инфраструктура VPN
- Нужен доступный VDI

Общее описание:

Платформа виртуализации VERDE VDI от NComputing представляет собой специально разработанное универсальное решение, обеспечивающее безопасную, простую в использовании инфраструктуру виртуальных рабочих столов корпоративного уровня по очень доступной цене. VERDE VDI поставляет виртуальные рабочие столы Windows и Linux и идеально подходит для малого и среднего бизнеса.

Клиенты, которые развертывают VERDE VDI, могут получить удаленный доступ к своему сеансу VDI к брокеру соединений VERDE через клиентов NComputing с поддержкой VPN..

VPN позволяет устанавливать безопасные соединения с удаленной компьютерной сетью для получения доступа к защищенным ресурсам в этой сети, как если бы они были непосредственно подключены к серверам. Клиенты NComputing со встроенным VPN позволяют сотрудникам получать безопасный доступ к своим виртуальным рабочим столам VERDE VDI в частной сети.

Процесс установки:

1. Обязательное условие - настройка и развертывание VERDE VDI - интерактивное руководство по установке
2. Настройте и инициализируйте VPN-сервер: этот шаг включает в себя настройку IP-адреса VPN-сервера, создание пула DHCP, который будет использоваться для подключения клиентов, и выбор желаемого типа шифрования.
3. Создайте учетные записи пользователей: имя пользователя, пароль и выберите, будет ли пользователь иметь доступ к локальной сети или только к маршрутизатору.
4. Настройте тонкий клиент NComputing со встроенным VPN-клиентом. Как правило, все, что требуется, это адрес VPN-сервера, имя пользователя и пароль.

Поддерживаемые устройства:

- Тонкие клиенты **RX-RDP**, **RX420**(RDP), **RX300**
- **LEAF OS***
- Клиент VERDE Windows

Платформа:

- VERDE VDI

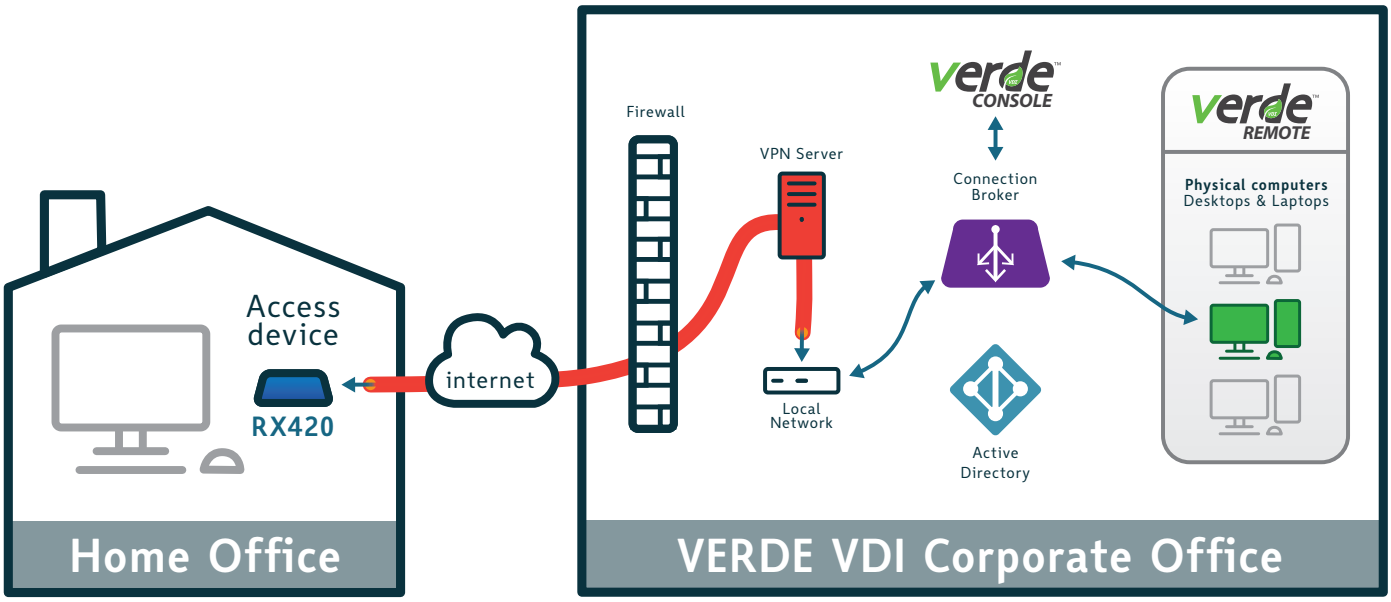
Особенности реализации:

- Полный доступ к ресурсам локальной сети.
- Дополнительные уровни защиты через VPN-туннель.
- Истинное решение VDI, более простое в настройке и развертывании
- Затраты меньше по сравнению с другими решениями VDI.
- Необходимо иметь достаточное количество мест для лицензий VPN.

* Поддержка буде добавлена Q3 2020.

Additional resources: See Appendix A

Сценарий 11: VERDE VDI – Только удаленные ПК: VPN



Профиль:

- Сеть офисов малого и среднего размера
- Есть инфраструктура VPN
- Нужен доступ к существующим физическим ПК в офисе

Общее описание:

VERDE Remote Access - это простое в развертывании виртуальное устройство Linux, которое устанавливается в среде клиента. Это позволяет пользователям дома подключаться к своему ПК в корпоративном офисе и использовать его так, как если бы они сидели перед ним.

Функция удаленного доступа VERDE настраивается администратором для определения критериев подключения. Весь трафик данных надежно зашифрован, защищая физические ПК от несанкционированного удаленного доступа.

Администратор может легко отслеживать состояние подключения компьютеров и, при необходимости, принудительно отключать или выключать их.

Одним из основных преимуществ функции удаленного доступа VERDE является отсутствие необходимости в расширенной аппаратной инфраструктуре по сравнению со стандартным развертыванием VDI.

Клиенты, которые развертывают удаленный доступ VERDE, могут безопасно получить доступ к своему физическому ПК / ноутбуку удаленно через клиентов NComputing с поддержкой VPN.

Процесс устрановки:

1. Настройка и развертывание VERDE VDI
2. Настройте и инициализируйте VPN-сервер. Этот шаг включает настройку IP-адреса VPN-сервера, создание пула DHCP, который будет использоваться для подключения клиентов, и выбор желаемого типа шифрования.
3. Создайте учетные записи пользователей. Введите имя пользователя и пароль, а также установите права доступа: ко всей локальной сети или только к маршрутизатору.
4. Настройте тонкие клиенты для подключения. Как правило, все, что требуется, это адрес VPN-сервера, имя пользователя и пароль.

Поддерживаемые устройства:*

- Тонкие клиенты **RX-RDP**, **RX420**(RDP), **RX300**
- **LEAF OS**
- Клиент VERDE Windows

Платформа:

- VERDE VDI с удаленным доступом*

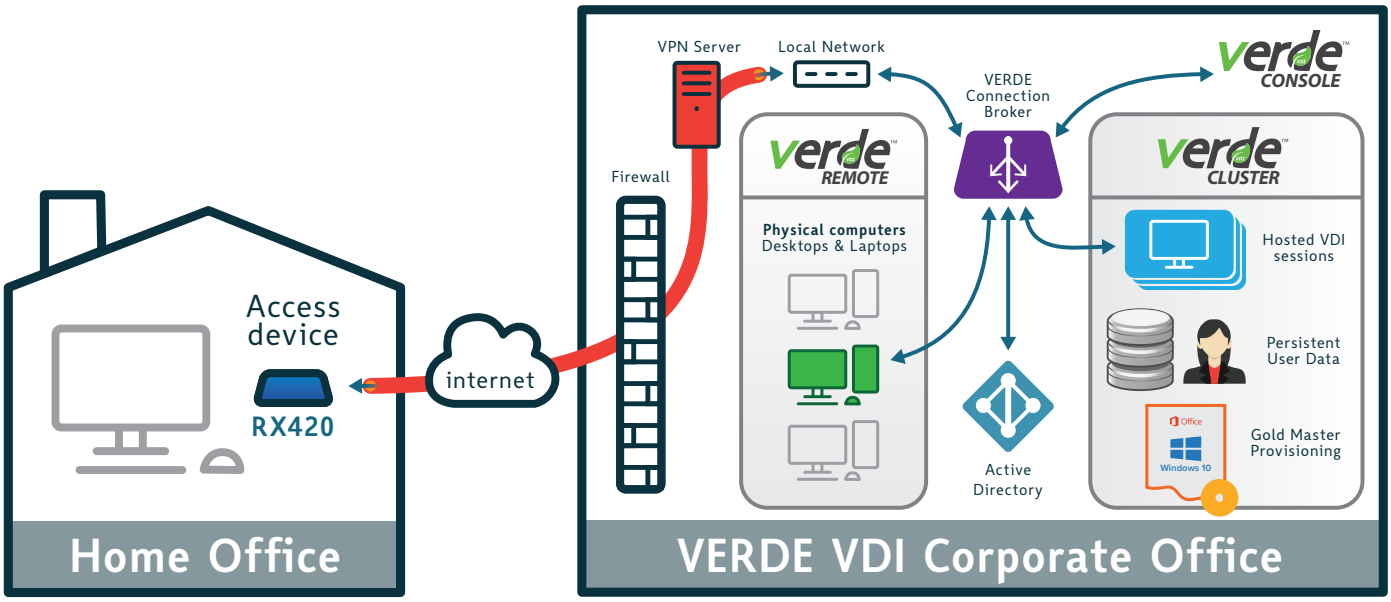
Особенности реализации:

- Полный доступ к ресурсам локальной сети.
- Дополнительные уровни защиты через VPN-туннель.
- Минимальная инфраструктура по сравнению с полным VDI.
- Необходимо иметь достаточное количество лицензий для мест VPN.
- Удаленный компьютер должен оставаться включенным.

* Поддержка будет добавлена Q3 2020.

Additional resources: See Appendix A

Сценарий12: VERDE VDI – Сеансы ВМ и удаленные ПК: VPN



Профиль:

- Сеть офисов малого и среднего размера
- Есть инфраструктура VPN
- Нужен доступ к физическим ПК в офисе
- Нужен доступ к внутренним ресурсам
- Нужен доступный VDI

Общее описание:

VERDE VDI может быть развернут для обеспечения гибридных сеансов VDI и удаленного доступа к компьютеру через того же защищенного брокера соединений VERDE с инфраструктурой VPN.

VERDE VDI обеспечивает безопасную, простую в использовании инфраструктуру виртуальных рабочих столов корпоративного уровня. VERDE VDI поставляет виртуальные рабочие столы Windows и Linux.

Функция удаленного доступа VERDE настраивается администратором для определения критериев подключения. Весь трафик данных надежно зашифрован, защищая физические ПК от несанкционированного удаленного доступа.

Мониторинг и контроль могут быть выполнены с помощью консоли VERDE.

Процесс установки:

См. шаги сценариев 10 и 11.

Поддерживаемые устройства*:

- Тонкие клиенты **RX-RDP**, **RX420**(RDP), **RX300**
- **LEAF OS**
- Клиегнт VERDE Windows

Платформа:

- VERDE VDI с удаленным доступом*

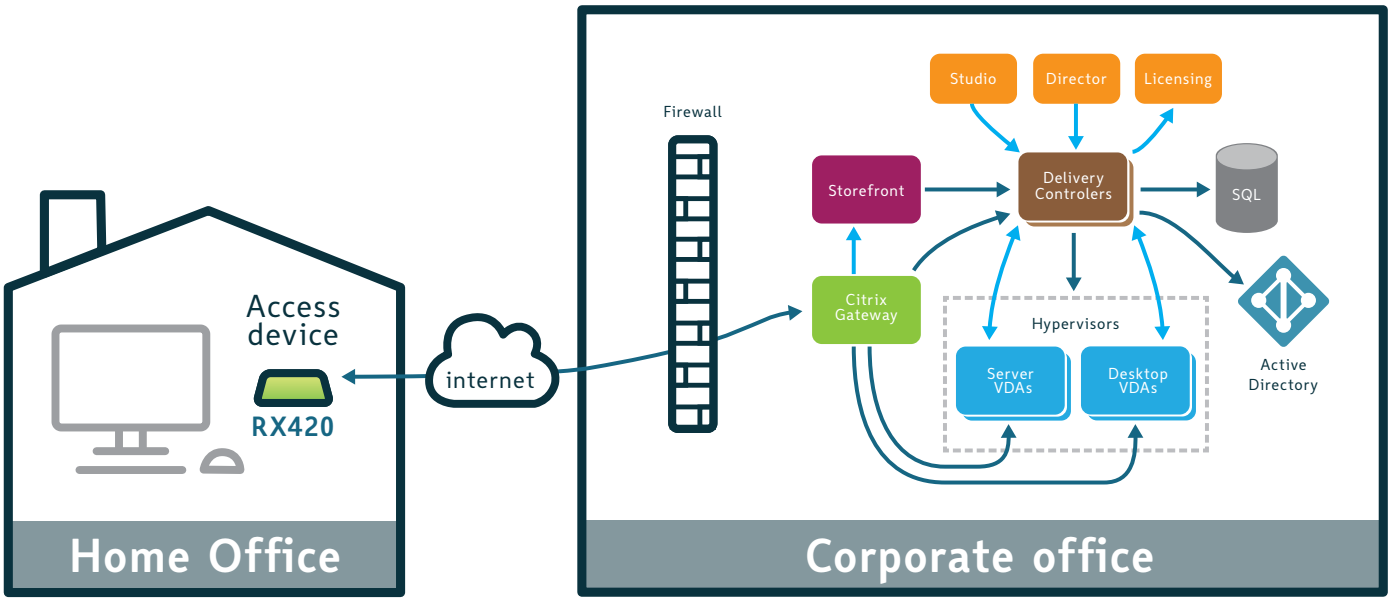
Особенности реализации:

- Полный доступ к ресурсам локальной сети.
- Дополнительные уровни защиты через VPN-туннель.
- Гибкое развертывание с гибридными сеансами VDI и удаленным доступом к физическим компьютерам.
- Минимальная инфраструктура по сравнению с полным VDI.
- Обширный мониторинг и контроль для с помощью консоли VERDE.
- Необходимо иметь достаточное количество лицензий для мест VPN.
- Удаленный компьютер должен оставаться включенным

* Поддержка будет добавлена Q3 2020.

Additional resources: See Appendix A

Сценарий 13: Citrix VDI –On-premise



Профиль:

- Средние и крупные организации
- Локальное развертывание Citrix VDI
- Нужен удаленный доступ к виртуальным приложениям и рабочим столам или Citrix Workspace.

Общее описание:

Традиционное развертывание Citrix для приложений и рабочих столов состоит из контроллеров доставки, серверов StoreFront, высокодоступной базы данных SQL, консолей Studio и Director, сервера лицензий и шлюза Citrix Gateway. Эти компоненты являются частью плоскости управления для среды и развернуты в центре обработки данных или облаке, управляемом клиентом или партнером.

Citrix Gateway объединяет инфраструктуру удаленного доступа для обеспечения единого входа во все приложения, находящиеся в центре обработки данных, в облаке или в виде SaaS. Это позволяет людям получить доступ к любому приложению с любого устройства через один URL. Citrix Gateway прост в развертывании и прост в администрировании. Наиболее типичная конфигурация развертывания - найти устройство Citrix Gateway в DMZ. Тонкие клиенты RX-HDX, RX-HDX +, RX420 (HDX) и EX400 оптимизированы для работы с развертываниями Citrix.

Поддерживаемые устройства:

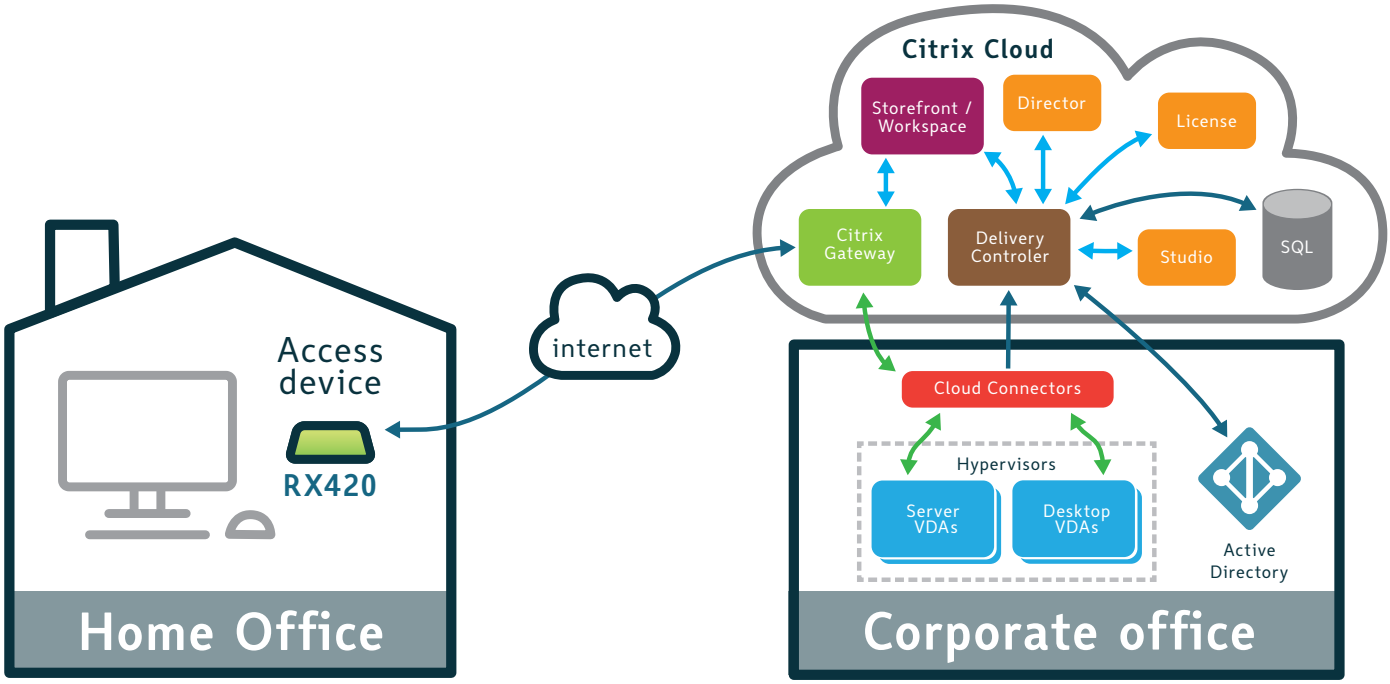
- Тонкие клиенты **RX-HDX**, **RX-HDX+**, **RX420**(HDX), EX400

Особенности реализации:

- Безопасный доступ через Citrix Gateway; VPN или перенаправление портов не требуется.
- Клиенты NComputing имеют встроенное приложение Citrix Workspace для поддержки виртуальных приложений и рабочих столов для локального или облачного развертывания.
- Простая настройка устройств NComputing.
- Более сложная настройка, развертывание и поддержка внутренней инфраструктуры.
- Высокая стоимость; значительные капитальные вложения.

Additional resources: See Appendix A

Сценарий 14: Citrix – Citrix Cloud



Профиль:

- Средние и крупные организации
- Облачное развертывание Hyprid или Citrix Cloud
- Нужен удаленный доступ к виртуальным приложениям и рабочим столам или Citrix Workspace.

Общее описание:

Citrix Cloud - это облачная платформа, состоящая из различных сервисных предложений. Многие из этих сервисов функционируют как плоскость управления, которая постоянно поддерживается Citrix с рабочими нагрузками и данными, находящимися в центре обработки данных или облаке по выбору клиента. Такой подход позволяет клиентам сосредоточиться на самой стратегической части ИТ и доставки ресурсов с безопасностью, доступностью и функциональностью, которые требуются бизнесу.

Используя эту платформу клиенты не занимаются установкой, настройкой, обновлением, мониторингом или масштабированием базового продукта плоскости управления, поскольку все это остается за Citrix для управления и обслуживания.

Заказчик может развернуть Citrix Gateway на месте или в Citrix Cloud. Citrix Gateway позволяет сотрудникам получать доступ к любому приложению с любого устройства через один URL-адрес. Тонкие клиенты NComputing RX-HDX, RX-HDX +, RX420 (HDX) и EX400 оптимизированы для развертываний Citrix, независимо от того, является ли это локальным, гибридным облачным или развертыванием Citrix Cloud.

Поддерживаемые устройства:

- Тонкие клиенты **RX-HDX**, **RX-HDX+**, **RX420**(HDX), EX400

Особенности реализации:

- программное обеспечение Citrix, управляется и размещается в Citrix Cloud
- Безопасный доступ к сервису Citrix Gateway из любой точки мира.
- Простая настройка и развертывание
- Простая настройка устройства NComputing.
- Низкие начальные затраты, но более высокая стоимость владения с течением времени.

Additional resources: See Appendix A

Appendix A: Дополнительные ресурсы

Совместимость устройств NComputing:

- NComputing access device comparison matrix
- vSpace Pro compatibility matrix
- VERDE VDI compatibility matrix

Сценарии 1, 3, 10, 11, 12:

- 3rd party OpenVPN access server & hosting solution (not affiliated with *NComputing*)
  - https://openvpn.net/virtual-appliances/
  - https://www.turnkeylinux.org/openvpn
  - https://doc.zentyal.org/en/vpn.html

Сценарий 2:

- **KB article:** How to access vSpace Pro host machines with port forwarding

Сценарий 4:

- Microsoft guide on Deploy your Remote Desktop environment

Сценарий 5:

- **KB article:** How to access RDSH host machines with port forwarding

Сценарий 6:

- Windows Virtual Desktop overview
- Getting started with Windows Virtual Desktop
- WVD Walkthrough guide

Сценарии 7, 9:

- VERDE VDI datasheet
- VERDE VDI installation guide
- VERDE VDI documentation

Сценарий 13:

- Citrix Gateway documentation
- Citrix Virtual Apps and Desktops Technical Overview

Сценарий 14:

- Citrix Virtual Apps and Desktops Service Reference Architecture and Deployment Methods