Zscaler™ PrivateAccess

Защищенный удаленный доступ к внутренним

корпоративным приложениям для цифровых корпораций.

Корпоративный рынок на пороге технологического сдвига. Внутренние приложения корпорации, работающие в ЦОД-е в пределах защищённого периметра (DMZ) перемещаются в публичные облака.

Миграция приносит целый ряд несомненных преимуществ в масштабировании, упрощении обслуживания, производительности и мн. Других, но это увеличивает размер защищенного периметра до размеров Интернета, что никак не стыкуется с традиционными принципами построения защищенного периметра. В то же время, количество «неуправляемых» пользовательских устройств с которых осуществляется доступ к внутренним приложениям неуклонно растет, заставляя ИТ искать разумный баланс между необходимостью предоставления доступа к критическим приложениям и минимизацией рисков.

Чтобы найти этот баланс, ИТ вынуждены периодически менять используемые технологии удаленного доступа, обнаружив, что они уже не удовлетворяют потребности пользователей и не соответствуют требованиям ИТ.

Традиционный защищенный периметр (DMZ) становится не эффективным инструментом в облачном окружении.

Традиционные DMZ наилучшее решение для защиты приложений размещенных в вашем ЦОД-е. Они предоставляют дополнительные уровни защиты для внутренней локальной сети, позволяя опубликовать в публичной сети приложения, предназначенные для доступа из вне и закрыть при этом доступ к внутренним приложениям. В случае перемещения приложения на платформу облачного провайдера, периметр расширяется до размеров сети Интернет и DMZ становиться бесполезной.

Перенос DMZ в облако – часто называемый «виртуальный DMZ», рекомендуемый некоторыми облачными провайдерами, это дорогое, довольно сложное с точки зрения проектирования и реализации решение. Реализация его требует установки стека оборудования в облачном ЦОД-е, организации виртуальной сети, которая как правило специфична для каждого провайдера и подключении к этой сети обоих стеков оборудования, в локальном и облачном ЦОД-ах. Сложность этого решения существенно замедляет адаптацию облачных технологий, требует дополнительных затрат на оборудование и вызывает разочарование у пользователей, начинающих работу с облачными приложениями.

Zscaler Private Access: Защищенный удаленный доступ в эпоху облачных сервисов

Zscaler Private Access (ZPA) инструмент для организации защищенного удаленного доступа к внутренним приложениям вне зависимости от того где они размещены в данный момент в ЦОД-е или Облаке. ZPA позволяет создать программно-определяемый периметр, базирующийся на принципах определенных Defense Information Systems Agency (в 2007 г.). ZPA существенно отличается по используемым технологиям от традиционной DMZ. Контроль доступа к внутренним приложениям в ZPA базируется на двух принципах

- нулевого уровня доверия (zero trust)
- должен знать (need-to-know)

при этом ключевыми критериями являются устройство и идентификатор пользователя.

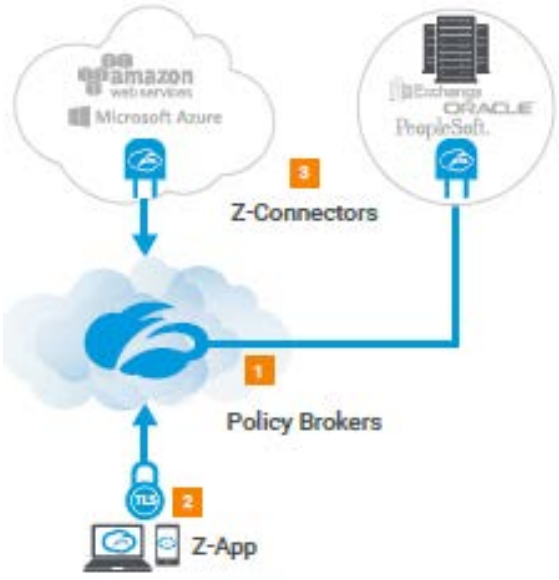
Архитектура ZPA организована на основе 4 ключевых правил:

- Подключение пользователя к приложению без «проброса» во внутреннюю сеть
- Не авторизованный пользователь не знает о существовании приложений (не видит их)
- Сегментация приложений без сегментации сети
- Защищенный удаленный доступ без использования VPN устройства

ZPA позволяет максимально просто (без изменения архитектуры и установки доп. оборудования) организовать защищенный удаленный доступ к внутренним приложениям. Контроль доступа будет осуществляться на основании политик определённых администратором. На каждое устройство, используемое пользователем устанавливается агент, называемый Z-App. Z-App обеспечивает правильность настройки устройства и создает микро-туннель до ближайшего устройства Zscaler в момент, когда пользователь обращается к приложениям.

Для организации доступа к приложениям, развернутым на облачных ресурсах или в ЦОД-е, там устанавливается программный шлюз, называемый Z-Connector, в виде виртуальной машины, который организует микро-туннель до облака Zscaler. Z-Connector инициирует только исходящее соединение, и не принимает какие либо входящие запросы на соединение и поэтому «не видим» для открытого Интернета, что лишает возможности хакеров проводить на него DDoS атаки. Решение о соединение микро-туннелей пользователя и приложения принимается Z-Broker на основании политик прописанных администратором. Решение ZPA является на 100% программно-определяемым, не требует установки каких-либо устройств и позволяет пользователям воспользоваться преимуществами облачных технологий и мобильных устройств обеспечиваю при этом безопасность приложений.

Архитектура сервиса ZPA



1 Z – Broker – Облачный брокер управляющий соединениями на основе политик

2 Z-App – Приложение устанавливаемое на устройстве пользователя

3 Z – Connector – Виртуальная машина устанавливаемая перед приложением в ЦОД-е или Облачной платформе

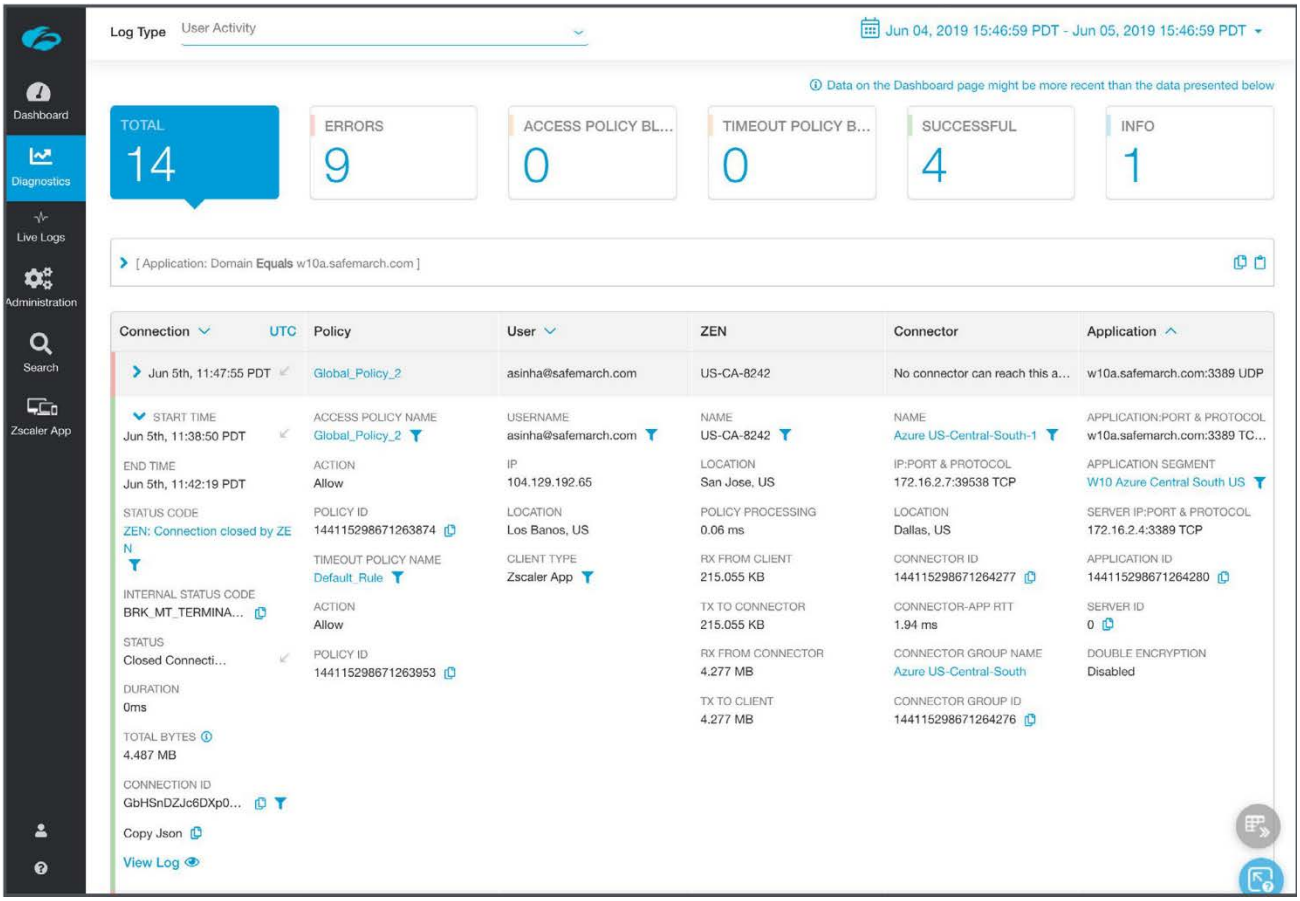
Преимущества использования ZPA для корпораций

Пользователи играют ключевую роль в выборе технологий, используемых в корпорации. ZPA предоставляет наиболее удобный интерфейс пользователям обеспечивая при этом выполнение требований ИТ по безопасности:

- Единый интерфейс для доступа к облачным и внутренним приложениям
- Сервис интегрирован с Okta и др. SSO провайдерами для обеспечения комфортного доступа
- Пользователь проключается к приложению через ближайший шлюз минимизируя сетевые задержки
- Администратор может установить период повторной аутентификации обеспечивая максимально комфортную работу удаленным пользователям

ZPA предоставляет ИТ централизованную платформу для авторизации пользователей и контроля доступа к приложениям:

- Политики, хранимые в облаке Zscaler, определяют права доступа пользователей к приложениям и применяются вне зависимости от местоположения пользователя
- Администратор создает и управляет политиками для пользователей, групп пользователей или групп приложений
- ИТ может сегментировать доступ к приложениям по группам, без необходимости сегментировать сеть или использовать несколько ACL



Снижение рисков внешних атак.

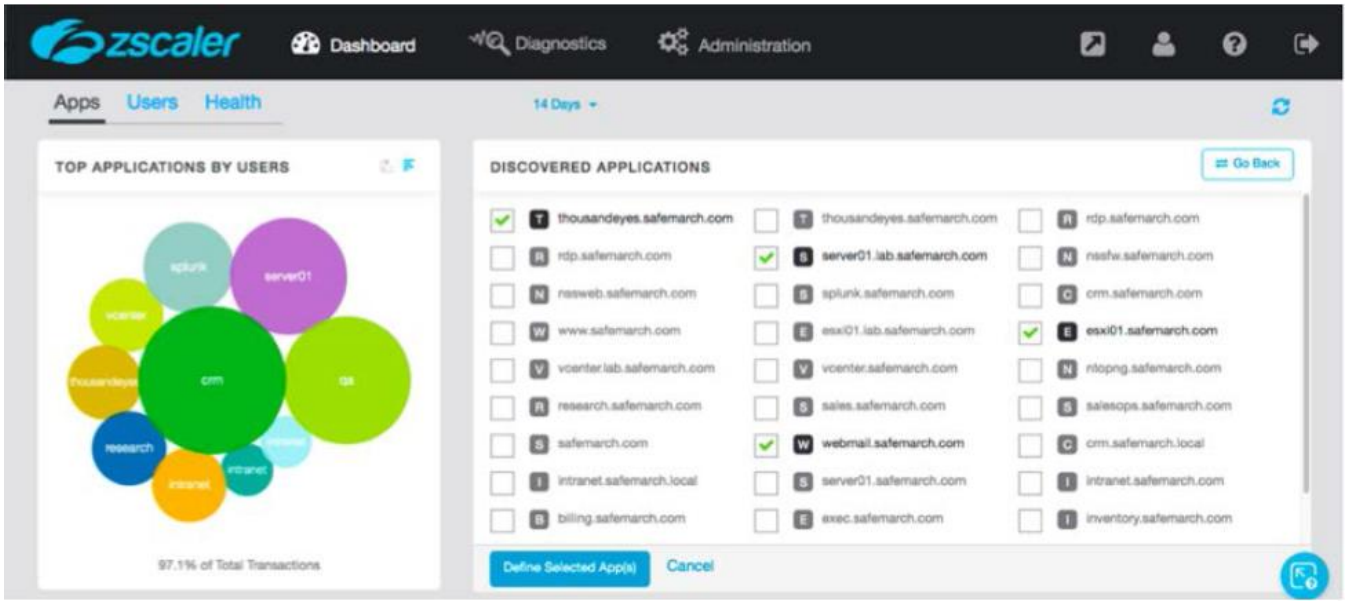
ZPA позволяет корпорации сократить до минимума пространство для атак внутренних приложений из Интернет:

- Пользователи не видимы из Интернет, что позволяет использовать неуправляемые устройства с минимальным риском
- Приложения не видимы для неавторизованных пользователей корпорации, исключен случайный доступ
- Приложения не видимы из интернета, что позволяет избежать риска DDoS атак
- Обмен данными осуществляется по защищенному микро-туннелю (TLS), что гарантирует защиту данных
- Возможность организации доступа к приложениям партнерам и третьим компаниям без предоставления доступа во внутреннюю сеть.

Отчетность по использованию приложений в реальном времени.

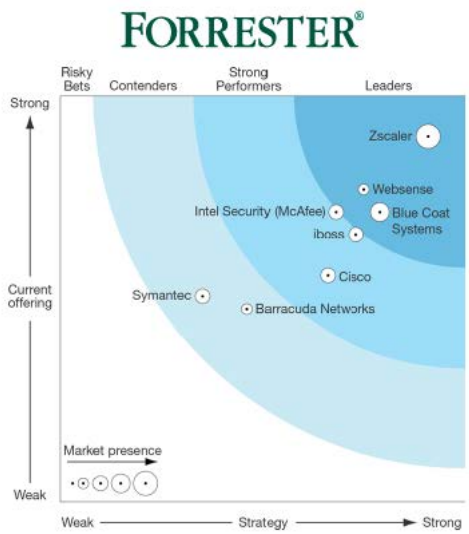
ZPA предоставляет администратору графический интерфейс позволяющий в любой момент сформировать отчет по использованию приложений в интересующем его разрезе.

- Обнаружить все облачные приложения, используемые пользователями компании и гранулярно ограничить доступ к ним
- Идентифицировать пользователей, наиболее часто использующих эти приложения
- Получить статистику по активности пользователей за интересующий период
- Получить информацию о времени отклика приложений, серверов и отдельных соединений
- Автоматически выгружать статистические отчеты в корпоративную SIEM



Мнения аналитиков о Zscaler:

В течении семи последних лет Zscaler сохраняет позицию лидера в Gartner Magic Quadrant в сегменте Secure Web Gateway



Forrester позиционирует Zscaler как безусловного лидера в сегменте безопасность веб контента

Правила лицензирования ZSCALER PRIVATE ACCESS

Услуги ZSCALER PRIVATE ACCESS продаются как **годовая подписка** на группу пользователей. Для удобства заказчиков все услуги объединены в три пакета(бандла):

- Browser only
- Professional
- Business

Сервисы ZSCALER PRIVATE ACCESS	Browser only	Professional	Business
Централизованное управление пользователями и приложениями – единая консоль, позволяющая в реальном времени управлять доступом пользователей к приложениям	✓	✓	✓
Защищенный доступ к браузерным приложениям– доступ ко всем веб-приложениям без их публикации в открытой сети Интернет.	✓	✓	✓
Защищенный доступ к корпоративным приложениям – доступ к неограниченному числу «внутренних» приложений (расположенных в частном/публичном/гибридном облаке или ЦОД –е) без их публикации в открытой сети Интернет.	✓	✓	✓
Обнаружение (публикация) приложений и серверов	✓	✓	✓
Закрытая корпоративная сеть, защищенная от DDoS-атак – приложения видны только пользователям, авторизованным на доступ к ним	✓	✓	✓
Единая консоль для управления и создания политик – политики для всех пользователей корпоративной сети создаются и применяются с одной консоли	✓	✓	✓
Пассивный мониторинг состояния приложений – состояние приложения (время ответа) мониторинг начинается с момента обращения пользователя к нему	✓	✓	✓
Базовая проверка пользовательского устройства – проверка пользовательского устройства на корректность реестра, целостность файловой системы и наличия сертификатов.	✓	✓	✓
Микросегментация приложений (до 5 приложений) – гранулярный контроль доступа пользователя или группы пользователей к 5 определенным приложениям, каждое из приложений может использовать несколько серверов и/или портов	✓	✓	
Zscaler App – легковесное приложение (клиент под Windows, Mac, iOS, Android), устанавливаемое на пользовательское устройство для организации доступа к корпоративным приложениям		✓	✓
Защищенный доступ к корпоративным приложениям – доступ к неограниченному числу «внутренних» приложений (расположенных в частном/публичном/гибридном облаке или ЦОД –е) без их публикации в открытой сети Интернет.		✓	✓
Микросегментация приложений (до 3 000 приложений) – гранулярный контроль доступа пользователя или группы пользователей к 10 000 определенных приложений			✓
Непрерывный мониторинг состояния приложения – непрерывный мониторинг состояния приложения, контроль доступности портов, отправление сообщения в случае недоступности порта.			✓
Выгрузка журналов – автоматическая выгрузка журналов в SIEM систему заказчика	$	$	✓
Использование PKI сертификата, предоставленного заказчиком			✓
Двойное шифрование – шифрование микротоннеля с использованием PKI сертификата заказчика	$	$	$
Отчет в реальном времени – получение отчетов о работе пользователей в реальном времени.			✓

Дополнительные материалы можно найти на сайте вендора:

Подробнее о продукте Zscaler Private Access - https://www.zscaler.com/products/zscaler-private-access

Интерактивное демо, можно в течение 7 дней, на базе развернутого решения изучить функциональность решения - https://www.zscaler.com/zpa-interactive