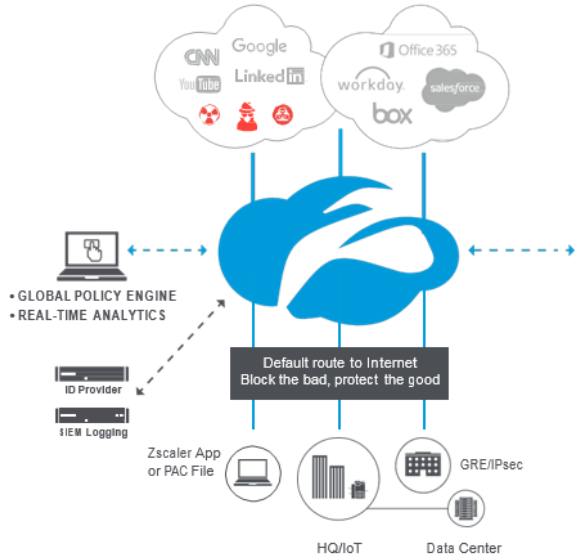
Zscaler™ Internet Access

Zscaler Internet Access – это Безопасный Интернет Шлюз предоставляемый как услуга. По сути это безопасный доступ в интернет, все что Вам необходимо сделать перенаправить трафик своего маршрутизатора на ближайший Вам ЦОД Zscaler (для РФ в Москве). Мобильные пользователи могут сделать это установив легковесное приложение от Zscaler или PAC файл. И вне зависимости от того где находится пользователь в данный момент – в кафе в Милане, в гостинице в Санкт-Петербурге или в своем офисе – он будет надежно защищен от интернет угроз.

Zscaler Internet Access располагается между пользователем и ресурсами Интернет и анализирует каждый байт проходящего через него трафика, используя для этого комбинацию самых передовых технологий, даже если он зашифрован по SSL. Благодаря этому вы защищены от всех Веб и Интернет угроз. Интернет шлюз Zscaler поддерживает такие технологии защиты, как «облачная песочница(Sandbox)», брандмауэр (Firewall) последнего поколения, предотвращение потери данных (DLP), контроль облачных приложений (Cloud application visibility and Control), благодаря которым есть возможность пользоваться сервисами, которые нужны на сегодняшний день, и подключать дополнительные услуги по мере необходимости.



Интернет шлюз как услуга:

Осуществляет проверку проходящего трафика по всем портам и протоколам, включая SSL.

ACCESS CONTROL	THREAT PREVENTION	DATA PROTECTION
Cloud Firewall URL	Adv. Protection	Data Loss Prevention
Filtering	Cloud Sandbox	Cloud Apps (CASB)
Bandwidth Control	Anti-Virus	File Type Control
DNS Filtering	DNS Security	

Просто перенаправьте трафик в облако Zscaler. Для офиса, можно создать туннель с пограничного маршрутизатораyou. Для мобильного устройства, можно установить приложение или PAC файл.

Все это возможно благодаря Zscaler Cloud Security Platform (далее платформы Zscaler), крупнейшей в мире облачной платформе безопасности, ежедневно обслуживающей более 30 миллиардов запросов. В ходе развития архитектуры этой географически распределенной, включающей в себя сотни устройств, платформы, компанией зарегистрированы более 100 патентов. Это позволяет обеспечить производительность и масштабируемость индустриального уровня.

Полная инспекция проходящего трафика

Шлюз анализирует весь проходящий через него трафик, без исключения. Благодаря запатентованной технологии ByteScanTM анализируется каждый байт входящего и исходящего трафика, включая шифрованный по SSL, с задержкой на устройстве не более 1 мкС.

«За Облачная» быстрота реагирования

Для Вас вместе с Zscaler работают миллионы пользователей. Любая киберугроза, обнаруженная где-либо будет немедленно заблокирована для всех пользователей платформы Zscaler. Ежедневно Zscaler проводит более 120 тыс. обновлений своей платформы для нейтрализации вновь обнаруженных киберугроз.

Корреляция угроз в реальном времени

Динамический расчет рисков для каждой веб-страницы на основе анализа каждого объекта, размещенного на странице и страницы в целом.

60+ источников данных о киберугрозах

Для того чтобы своевременно обнаружить и заблокировать вновь появляющиеся киберугрозы, команда Zscaler ведет непрерывный мониторинг более 60 источников информации об их появлении. Среди этих источников частные и коммерческие компании, сообщества профессионалов по безопасности и аналитические агентства.

ZSCALER INTERNET ACCESS

Функциональность интегрированная в Интернет Шлюз

Контроль доступа

Облачный Брандмауэр Анализ содержимого пакетов (DPI) и контроль доступа по всем портам и протоколам.	**URL фильтрация** Блокировка или ограничение доступа к вебсайтам для пользователя или группы пользователей по категории сайта или адресу.	**Управление полосой пропускания** Создание политик управления полосой пропускания и приоритизация бизнес-критичного трафика над остальным трафиком	**DNS фильтрация** Контроль запросов к DNS и блокировка их перенаправления на вредоносные сайты.

Защита от вирусов

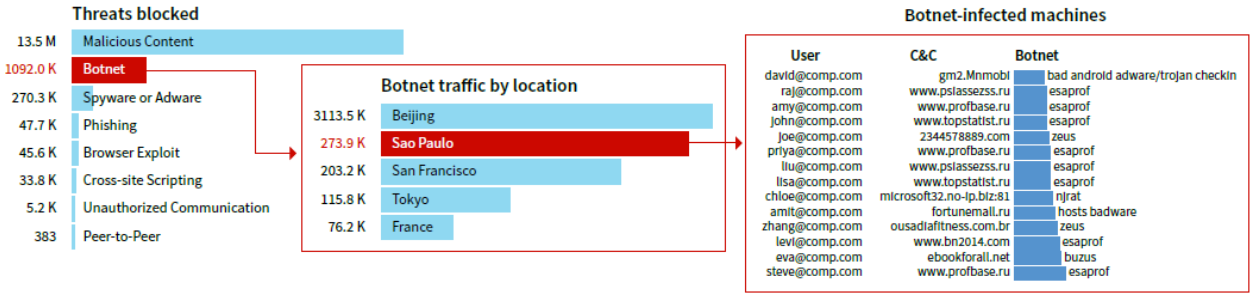
Антивирус Сигнатурный анализ трафика на предмет наличия в нем вирусов, шпионского ПО и других зловредных вложений.	**Защита от новейших угроз** Защита в реальном времени от киберугроз исходящих от веба контента, таких как браузерные эксплойты, скрипты, зеро-пикселы iFrame и обнаружение активности ботнетов и «шифровальщиков».	**Облачная песочница (SandBox)** Блокирование угроз «нулевого дня» путем изоляции подозрительных файлов и анализа их поведения. Доступно для любого пользователя, масштабируется «по требованию».	**Защита DNS** Идентификация и перенаправление подозрительных «командно-управляющих» соединений на движок Zscaler для инспекции их содержимого.

Защита данных

Предотвращение утечки данных (DLP) Анализ трафика всех пользователей на содержание ключевых слов, включая сжатый и шифрованный (по SSL), с использование стандартных или определенных пользователем словарей.	**Контроль типа передаваемых файлов** Ограничение приема/передачи файлов пользователями, в зависимости от типа файла, местоположения пользователя и адреса приема/передачи	**Отчетность и аналитика в реальном времени** Использование Интернет шлюза Zscaler позволяет сделать процесс расследования максимально быстрым и простым. За секунды вы сможете получить полную статистику по каждому пользователю и связанные с ним события и угрозы.

Отчетность и аналитика в реальном времени

Использование Интернет шлюза Zscaler позволяет сделать процесс расследования максимально быстрым и простым. За секунды вы сможете получить полную статистику по каждому пользователю и связанные с ним события и угрозы. За несколько кликов вы сможете изолировать устройства, содержащие ботнетов или понять где и когда использовались приложения, не удовлетворяющие требованиям компании по безопасности.



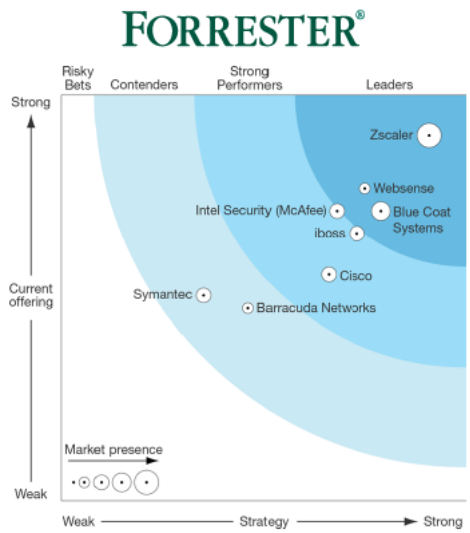
Управление журналами данных

Платформа Zscaler не сохраняет данные передаваемые/принимаемые от пользователя, единственное что сохраняет платформа — это журнал событий. Он храниться в памяти платформы и может быть сохранен на диск только в месте, указанном заказчиком. Благодаря этому заказчик может формировать отчеты в соответствии с требованиями законодательства страны пребывания. Технология Zscaler NanologTM Streaming Service, используемая в платформе NetScaler, позволяет предавать журналы в SIEM заказчика в реальном времени, для генерации интегральной отчётности компании, включающей в себя данные из различных источников.

Лучшая производительность и безопасность в сегменте облачных решений

Платформа Zscaler начиная с 2011 позиционируется ведущими аналитическими агентствами (Gartner, Forrester) в сегменте лидеров. По мнению аналитиков Интернет шлюз Zscaler обеспечивает высочайший уровень безопасности без необходимости приобрести, развернуть и управлять стеком аппаратных устройств. Перенеся стек безопасности в облако Zscaler защищает пользователей от интернета угроз за счет глубокой инспекции проходящего трафика и управления доступом на основе политик. Что помогает им осуществить прорыв к облачным технологиям, например, существенно упростив развертывание Office365 и мобильных приложений.

В течении семи последних лет Zscaler сохраняет позицию лидера в Gartner Magic Quadrant



Forrester позиционирует Zscaler как безусловного лидера в сегменте безопасность веб контента

Правила лицензирования ZSCALER INTERNET ACCESS

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

- Professional
- Business
- Transformation

Сервисы ZSCALER INTERNET ACCESS	Professional	Business	Transformation
Доступ к облачной платформе			
Data Centers Доступ в независимости от местоположения, высокая доступность, SLA по задержкам	✓	✓	✓
Traffic Forwarding GRE туннель, IPsec, proxy, PAC файл или мобильное приложение Zscaler	✓	✓	✓
Authentication SAML, secure LDAP, Kerberos, hosted	✓	✓	✓
Real-Time Cloud Security Updates Ежедневное обновление информационной базы о киберугрозах (более 120,000/в день) из 60+ проверенных источников	✓	✓	✓
Real-Time Reporting and Logging Генерация отчетов о проходящих транзакциях по аккаунту заказчика за секунды. Выбор местоположения для хранения журналов (US или EU).	✓	✓	✓
SSL Inspection Полная инспекция SSL трафика с соблюдением установленных SLA. Дискретные политики для исключения определенного контента.	**Add-on***	✓	✓
Nanolog Streaming Service Передача журналов по всем пользователям в SIEM развернутый на стороне пользователя в реальном времени	**Add-on***	✓	✓
Услуги обеспечения безопасности			
URL and Content Filtering Дискретные политики фильтрации по пользователю, группе, офису, времени и объему трафика. Динамическая классификация контента, для «неизвестных» вебсайтов.	✓	✓	✓
File Type Control Контроль типа файлов по пользователю, офису и источнику	✓	✓	✓
Inline Antivirus & Antispyware Инспекция входящего/исходящего трафика на предмет «зловредных» вложений на базе сигнатур	✓	✓	✓
Reputation-Based Threat Protection Блокировка ботнетов, командно-управляющих соединений и фишинга	✓	✓	✓
Standard Cloud Firewall Дискретная фильтрация по IP адресу, порту и протоколу	✓	✓	✓
Advanced Cloud Firewall Брандмауэр нового поколения, фильтрация по приложению, пользователю и местоположению; журналирование информации по использованию.	**Add-on***	**Add-on***	✓
Bandwidth Control Управление полосой пропускания, возможность выделения гарантированной полосы пропускания для бизнес критических приложений	**Add-on***	✓	✓
Standard Cloud Sandbox Защита от угроз «нулевого дня», изоляция и проверка .exe and .dll файлов из неизвестных и подозрительных источников	✓	✓	✓
Advanced Cloud Sandbox Защита от угроз «нулевого дня», изоляция и проверка всех типов файлов; возможность задержания доставки файла до завершения проверки; подробные отчеты		**Add-on***	✓
Advanced Threat Protection Анализ рисков на базе глубокого анализа контента; блокировка шифровальщиков, кросс-скриптов, кражи куки файлов и анонимайзеров	**Add-on***	✓	✓
Cloud Application Visibility & Control Обнаружение, мониторинг активности и контроль доступа к веб приложениям	**Add-on***	✓	✓
Mobile Application Reporting & Control Гранулярное управление доступом к облачным приложениям с мобильных устройств. Защита мобильных устройств от киберугроз вне зависимости от местоположения.		✓	✓
Web Access Control Обнаружение устаревших версий веб браузеров и плагинов в соответствии с установленными политиками.	**Add-on***	✓	✓
Data Loss Prevention Сканирование исходящего трафика на предмет утечки конфиденциальных данных	**Add-on***	**Add-on***	**Add-on***

* - Некоторые из услуг, не входящие в пакет, могут быть приобретены за дополнительную плату, такие услуги имеют отметку add-on.

Дополнительные материалы можно найти на сайте вендора:

Подробнее о продукте Zscaler Internet Access - https://www.zscaler.com/products/zscaler-internet-access

Как Zscaler помогает ускорить работу с Office 365 - https://www.zscaler.com/solutions/office-365-deployment

Для тех, кто уже использует облачные приложения - https://www.zscaler.com/solutions/sd-wan-security