netskope

Netskope for Web

Используя функционал защищенного веб-шлюза следующего поколения (NG SWG), платформа Netskope блокирует вредоносные программы, обнаруживает новейшие угрозы, фильтрует веб-трафик по категориям, защищает данные, а также контролирует приложения и облачные сервисы по любому пользователю, площадке или устройству. Платформа Netskope объединяет в себе защищенный веб-шлюз (SWG), брокер безопасного доступа в облако (CASB) и систему предотвращения утечек данных (DLP) – и все это в единой консоли.

Основные моменты

- Средства гранулярного контроля на основе политик для веб-трафика и приложений (включая данные, действия и контекст)
- Обучающие оповещения о рисках, помогающие пользователям самим освоить работу с приложениями и облачными сервисами
- Производительность и масштаб облака – для проверки любого пользователя, устройства или площадки
- Предотвращение утечек данных для управляемых и неуправляемых приложений и веб-трафика
- Защита от вредоносного ПО и расширенных угроз, "песочница" и свыше 40 источников информации об угрозах
- Единая облачная консоль с согласованными средствами контроля на основе политик для функций SWG, CASB и DLP

Новый ландшафт веб-безопасности

Цифровая трансформация, стимулируемая облаками и мобильностью, продолжает набирать обороты, и уже 85% трафика, идущего через веб-шлюзы, приходится на приложения и облачные сервисы, согласно Netskope Cloud Confidence Index[1]. Вдобавок 83% веб-трафика шифруется[2], что создает новые слепые зоны и открывает лазейки для угроз и утечки данных через управляемые и неуправляемые приложения, облачные сервисы и веб-трафик.

Сегодня среднестатистическая компания использует более 1295 приложений и облачных сервисов, причем свыше 95% из них относятся к неуправляемым и не предоставляют никаких прав администратора[3]. Чтобы понимать и защищать контент и контекст, защищенные веб-шлюзы должны выйти за рамки традиционной фильтрации веб-запросов по URL-адресам и начать декодировать идущий через API трафик тысяч приложений и облачных сервисов. Кроме того, для установки системы веб-безопасности в разрыв нужна как производительность облака по запросу для проверки зашифрованного веб-трафика, так и масштаб облака с глобально распределенным доступом к облаку для удаленных офисов и мобильных пользователей.

Поскольку все больше бизнес-операций и данных переносятся в облако, решения для веб-безопасности также должны развиваться, сокращая задержки, уменьшая количество ретрансляций в веб-маршрутах и повышая эффективность. Одного только облачного SWG с безопасным доступом к стандартному интернету уже недостаточно для сегодняшних и завтрашних бизнес-операций. Нужны безопасность и скорость, чтобы обеспечить доступ к облачным приложениям и сервисам с малой задержкой и высокой пропускной способностью.

NETWELL
ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР
+7 (495) 662 39 66
WWW.NETWELL.RU

Облачный SWG с производительностью и масштабированием по запросу

Уже более 10 лет в ИТ-ландшафте преобладают аппаратные SWG, причем примерно три из четырех существуют и по сей день. Однако ситуация быстро меняется в сторону облачных SWG, описываемых следующей цитатой из отчета компании Gartner "Ключевые возможности защищенных веб-шлюзов".

Согласно тому же отчету Gartner за декабрь 2018 г., в возможностях SWG произошел серьезный сдвиг, и неудивительно, что случилось это благодаря цифровой трансформации. На схеме внизу показан уход от известных функций традиционных SWG к новым ключевым возможностям облачных SWG, и это подчеркивается в отчете наряду с прогнозируемым совокупным годовым темпом роста в 32%.

"САМЫЙ РАДИКАЛЬНЫЙ ФАКТОР НА ЭТОМ РЫНКЕ – ВЗРЫВНОЙ РОСТ ОБЛАЧНЫХ SWG-СЕРВИСОВ".

Ключевые возможности защищенных веб-шлюзов, Gartner, 27 декабря 2018 г.

SWG – защищенный веб-шлюз; CASB – брокер безопасного доступа в облако; DLP – система защиты от утечек данных

Источник: Ключевые возможности защищенных веб-шлюзов. Декабрь 2018 г.

В том же отчете Gartner далее отмечается: *"Функциональность CASB быстро становится важной составляющей решений SWG"*. Учитывая, что DLP — самая популярная функция решений CASB, предоставление единого решения SWG + CASB + DLP из облака, для облака и без ограничений — это как раз то, что нужно.

Гранулярный контроль на основе политик с помощью Cloud XD

Динамические веб-сайты сегодня используют тот же базовый язык, что и приложения и облачные сервисы. Возможность его декодирования крайне важна для SWG следующего поколения – ведь потоки данных в облаке текут как вода. Поскольку менее 5% приложений являются управляемыми и дают права администратора, данные, циркулирующие в неуправляемых приложениях, становятся огромной проблемой для облачных SWG, учитывая, что пользователи могут находиться где угодно и использовать любые устройства. Это заставляет комбинировать возможности SWG, CASB и DLP при включении в разрыв, чтобы обеспечить полноту картины и гранулярный контроль на основе политик в тысячах приложений.

Вместо грубых политик "разрешить/запретить" средства гранулярного контроля на основе политик учитывают контент и контекст пользователя, приложения, экземпляра, степени риска, данных и действий. Действие в отношении конфиденциальных данных в корпоративном экземпляре приложения может иметь смысл, но такая же активность в личном экземпляре может означать утечку или кражу данных сотрудником, который вот-вот уволится.

Источники:
1. Netskope Threat Research Labs, 2019 г.
2. Google HTTPS Encryption Transparency Report, сентябрь 2019 г.
3. 2019 Cloud Security Report, Cybersecurity Insiders

Богатый контекст CASB+SWG+DLP для политик

Netskope Cloud XD обеспечивает полноту картины и гранулярный контроль на основе политик для веб-трафика, приложений и облачных сервисов. Cloud XD декодирует язык облака и веб-сервисов, обеспечивая интеллектуальный консолидированный обзор использования облачных сервисов и веб-ресурсов. В отличие от традиционных решений для веб-безопасности, которые заваливают администраторов журналами по каждой HTTP(S)-транзакции, Cloud XD синтезирует данные о веб-активности и извлекает из них сведения о посещении веб-сайтов и страниц пользователями, позволяя углубиться в мелкие детали.

Одна платформа и консоль с унифицированными средствами контроля на основе политик

Облако ускоряет бизнес и улучшает безопасность, а Netskope дополняет эти преимущества единой консолью и унифицированными средствами контроля на основе политик, чтобы включаемое в разрыв сочетание инструментов SWG + CASB + DLP обеспечило веб-защиту нового поколения. Платформа Netskope дает ряд преимуществ заточенным под облако организациям, включая ориентированную на данные структуру для защиты данных и пользователей в любом месте; умную облачную аналитику для безопасной работы с облаком и веб-ресурсами; а также передовую глобальную мощную архитектуру для оперативной и масштабируемой защиты.

Netskope защищает ряд крупнейших мировых компаний, устанавливая в разрыв самый передовой в отрасли функционал прокси для проверки веб-трафика, приложений и облачных сервисов без ограничения производительности или масштаба и без увеличения задержки. Если вы опасаетесь компрометации или утечки данных через неуправляемые приложения или веб-сайты, а также возникающих там новейших угроз, то Netskope может обеспечить вам некоторое спокойствие.

ПРИМЕР ИСПОЛЬЗОВАНИЯ И ОБЗОР	ВОЗМОЖНОСТИ ЗАЩИЩЕННОГО ВЕБ-ШЛЮЗА СЛЕДУЮЩЕГО ПОКОЛЕНИЯ:
Визуализация и контроль веб-трафика, приложений и облачных сервисов Netskope предоставляет API-прокси для пользовательских приложений. Это позволяет понимать контент и контекст тысяч приложений, на что не способны традиционные решения SWG. Простые в развертывании облачные решения с прямым или обратным прокси — при включении в разрыв — обеспечивают визуализацию и гранулярный контроль на основе политик для веб-трафика, приложений и облачных сервисов.	• Обнаружение в ходе анализа (при включении в разрыв) или с помощью журналов с возможностью шифрования полей персональных данных в целях конфиденциальности • URL-фильтрация по более чем 100 категориям для более чем 200 языков, покрывающих 99,9% активного интернет-пространства • Рейтинги динамических веб-страниц по 70 категориям + пользовательские категории, категории приложений и категории YouTube • Включаемый в разрыв CASB, обеспечивающий визуализацию и гранулярный контроль на основе политик для более чем тысячи управляемых и неуправляемых приложений • Cloud Confidence Index™ (CCI) – рейтинги риска для более чем 36 000 приложений и облачных сервисов с использованием более 50 атрибутов CSA • Производительность облака для проверки зашифрованного трафика
Обнаружение вредоносного ПО и угроз Многоуровневая облачная защита включает в себя защиту от вредоносных программ, анализ скриптов до их выполнения, эвристику, песочницу и обнаружение аномалий на основе машинного обучения под управлением команды Netskope Threat Research Labs.	• Свыше 40 источников информации об угрозах + пользовательский хэш индикаторов компрометации и URL-каналы • Анализ поведения пользователей и сущностей (UEBA) для обнаружения компрометации доступа и аномалий • Облачная песочница, сторонняя поддержка песочниц Checkpoint, Juniper, Palo Alto Networks • Предоставление богатых метаданных 90 дней (по умолчанию), дольше – по контракту • Экспорт данных через REST API + обмен сведениями об угрозах в формате исходного кода
Предотвращение утечек данных (DLP) Политики "разрешить/запретить" не подходят для бизнес-подразделений, где принято свободное использование приложений с публикацией, передачей, выгрузкой или загрузкой данных в один клик. Средствам контроля на основе политик нужно понимать контент и контекст, а значит, без DLP тут не обойтись. Netskope предоставляет признанную систему DLP для веб-трафика, приложений и облачных сервисов.	• Облачная система DLP с 3000+ идентификаторами данных, поддержкой 1000+ типов файлов и 40+ готовых шаблонов политик • Обнаружение данных разными методами, включая пользовательские регулярные выражения, цифровые отпечатки, точное сопоставление данных, анализ близости, совпадение по шаблонам и ключевым словам, извлечение метаданных и оптическое распознавание символов (API-режим) • Система DLP может оповещать, разрешать, блокировать, выдавать сообщения для ознакомления сотрудников с корпоративными правилами поведения, заменять файлы заглушками, токенизировать или шифровать данные (структурированные и неструктурированные), отправлять на хранение для судебных нужд или в карантин • Основанное на машинном обучении обнаружение данных, передаваемых между корпорат. и личными экземплярами приложений, для выявления инсайдеров и утечек данных
Расширенная веб-аналитика и отчетность Средства контроля на основе политик определяет и задает Netskope Cloud XD, который интеллектуально и с акцентом на пользователя визуализирует использование веб-сайтов, приложений и облачных сервисов для аналитики и отчетности. Cloud XD синтезирует данные о веб-активности и извлекает из них те сведения о посещении веб-сайтов и страниц	• Решение позволяет сотрудникам центров безопасности (SOC) быстро расследовать оповещений, понимая контент и контекст действий на веб-сайтах, в приложениях и облачных сервисах • Аналитика в режиме реального времени позволяет строить сводные дашборды и отчеты • Детализация по конкретному пользователю, сайту и странице • Гибкий механизм ситуативных запросов, позволяющий 90 дней (больше – по отдельному контракту) извлекать богатые метаданные о действиях на веб-сайтах и в приложениях • Функционал экспорта данных и открытый API интегрируются со сторонними решениями
Прямое подключение к интернету Netskope позволяет удаленным офисам и мобильным пользователям выходить напрямую в интернет, где бы они ни находились. Как вариант, Netskope for Private Access для доступа к сети по принципу нулевого доверия может заменить традиционные VPN, соединяющие пользователей напрямую с частными приложениями, базами данных или ресурсами в публичных облаках и ЦОДах.	• Туннели IPsec и GRE для удаленных офисов + облегченный управляющий клиент для мобильных пользователей. • Высокопроизводительные программно-определяемые глобально распределенные ЦОДы с оптимизированными веб-маршрутами и ретрансляциями, чтобы обеспечить малую задержку (обычно менее 20 мс для любого пользователя) • Заточенная под облако микросервисная архитектура, призванная обеспечивать производительность и масштабирование сервисов безопасности по запросу • Избавление от затрат и проблем с производительностью, связанных с ретрансляцией веб-трафика + устройства веб-безопасности

netskope

Netskope Security Cloud обеспечивает непревзойденную прозрачность, защиту данных и противодействие угрозам в режиме реального времени, когда вы заходите в облачные сервисы, на веб-сайты и в частные приложения из любой точки мира и с любого устройства. Netskope разбирается в облаках как никто другой и ставит данные во главу угла, помогая ИБ-командам найти правильный баланс между защитой и скоростью, которые нужны им для дальнейшего движения по пути цифровой трансформации. Взгляните на свой периметр по-новому вместе с компанией Netskope.

©2019 Netskope, Inc. Все права защищены. Netskope – зарегистрированный товарный знак, а Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index и SkopeSights – товарные знаки Netskope, Inc. Все другие товарные знаки являются товарными знаками соответствующих владельцев. 09/19 SB-201-4