Сборник решений ASM, AFM, APM

ИНТЕГРАЦИЯ И УПРОЩЕНИЕ СРЕД VDI

ЗАДАЧА

Среды VDI часто используются для того, чтобы пользователи могли подсоединиться к корпоративным средам без необходимости использования тяжелых, дорогих конечных устройств. Однако их использование влечет за собой другие проблемы, скрытые в архитектуре технологии этого типа.

Каждая среда VDI требует наличие элемента аутентификации пользователя, элемента, представляющего возможности, доступные каждому пользователю, и наконец элемента, действующего в качестве «брокера» и управляющего доступом к VDI.

В среде с множеством решений VDI существует необходимость дублировать эту архитектуру для каждого решения, что влечет за собой возрастание расходов на первичное внедрений и увеличение

АЛЬТЕРНАТИВЫ

- Наличие решений VDI от нескольких разработчиков, что приводит к возрастанию капитальных и эксплуатационных расходов, что сложно оправдать.
- Использование собственных элементов в решениях VDI снижает гибкость решения с точки зрения пользователей и может привести к росту издержек.

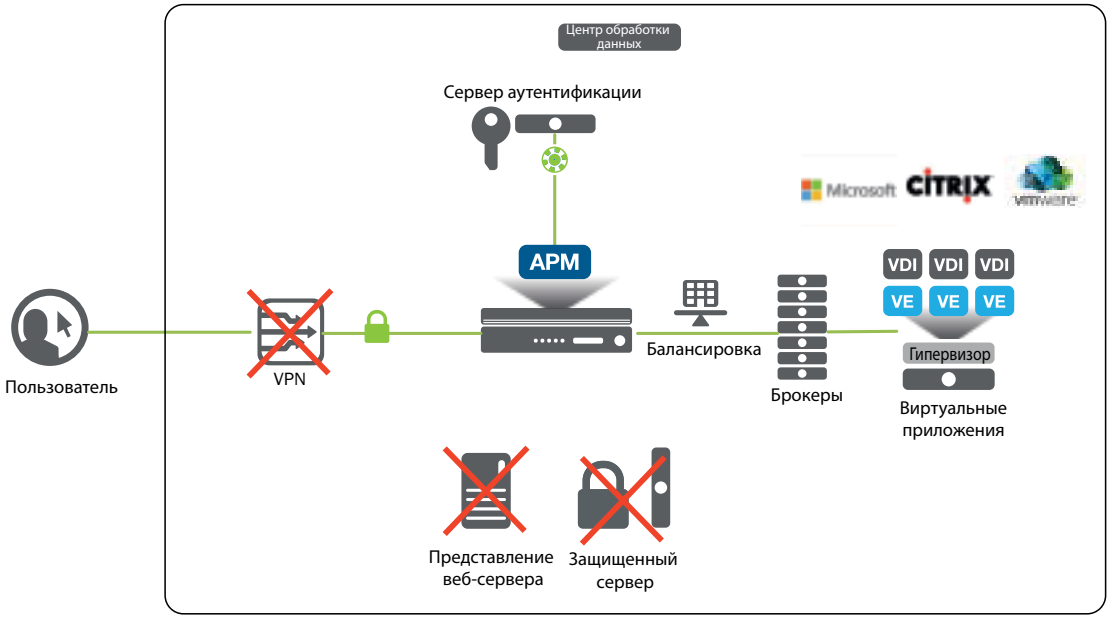
F5 | РЕШЕНИЕ APM

Решение APM (Программа управления политикой доступа) от F5 выполняет аутентификацию пользователей и устанавливает в сети защищенные протоколом SSL VPN-туннели, заменяя решение шлюзов безопасности в средах VDI.

Кроме того, APM предоставляет пользователю различные варианты на экране, объединяя функциональные возможности в единую платформу, таким образом избавляя от необходимости внедрения этого элемента в решение VDI.

Решение APM не зависит от внедрения решения VDI, позволяя стандартизировать вид и функции решения для клиента, отображая на экране один и тот же формат и варианты.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ИНТЕГРАЦИЯ И УПРОЩЕНИЕ СРЕД VDI



МИГРАЦИЯ СРЕД EXCHANGE

ЗАДАЧА

Миграция версий и сред Exchange может быть очень сложной. Пользователям приходится осуществлять миграции постепенно и синхронизировать изменения, произведенные на серверах, с изменениями в компьютерах пользователей.

Если услуга Exchange не имеет настроек по умолчанию, миграция может оказаться еще более сложной.

Миграция на Exchange 2013 предполагает изменение инфраструктуры клиента. Необходимо принимать во внимание защиту удаленного доступа, подготовку инфраструктуры для консолидации функций сервера, виртуализации и все это представляет собой основные трудности для компаний, которые также сталкиваются с потерей обслуживания до завершения миграции.

АЛЬТЕРНАТИВЫ

- Проведение миграции пользователей из одной среды в другую вручную, а также синхронизация с изменениями на внутренних серверах.

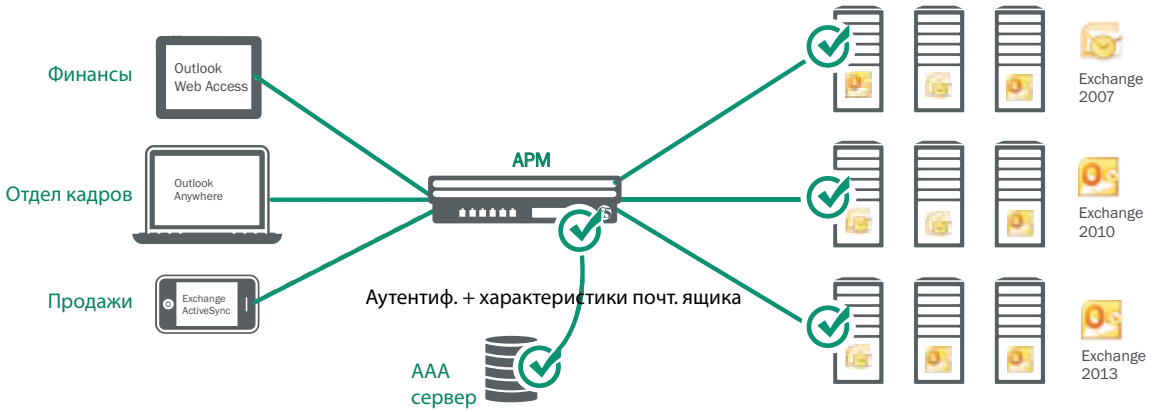
F5 | РЕШЕНИЕ APM

Решение компании F5 выполняет предварительную аутентификацию пользователей, используя решение APM. Такие процедуры, предшествующие аутентификации, могут включать, например, дополнительные сертификаты проверки подлинности, разовые пароли или проверки безопасности на компьютере клиента.

После успешной аутентификации пользователя APM проверяет каталог на предмет конфигурации пользовательского почтового ящика и может использовать его для перенаправления доступа к соответствующей группе серверов. Это может использоваться, например, для выполнения миграции с Exchange 2007 на Exchange 2013 без внесения каких-либо изменений в компьютер клиента и необходимости остановки сервиса.

Благодаря партнерству с компанией Microsoft, выпуск Exchange компанией F5 легко может быть выполнен с применением шаблона на BIG-IP, который ориентирован на Exchange и позволит нам быстрее провести конфигурацию.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | МИГРАЦИЯ СРЕД EXCHANGE



ОБЪЕДИНЕНИЕ РЕШЕНИЙ В ОБЛАЧНЫХ СРЕДАХ

ЗАДАЧА

Организации гибридного типа применяют распределенную архитектуру, которая может охватывать многие домены безопасности. В любой момент времени пользователь может получить доступ к корпоративному центру обработки данных, облачной инфраструктуре компании или даже веб-приложению в виде программного обеспечения как услуги третьей стороны.

Это привело к отсутствию контроля доступа на уровне профиля, а такой на уровне управления. Недостаток контроля существует из-за разницы в доступе, основанном на профилях и правах доступа пользователей. Сложность управления пользовательским доступом существует из-за множества приложений, паролей и видов аутентификации.

АЛЬТЕРНАТИВЫ

- Различные разработки собственных решений, которые приводят к повышению затрат на техническое обслуживание и снижению гибкости решения.
- Специальные решения для приложений, которые не обладают масштабируемостью и не решают проблему сложности доступа для пользователей.

F5 | РЕШЕНИЕ APM

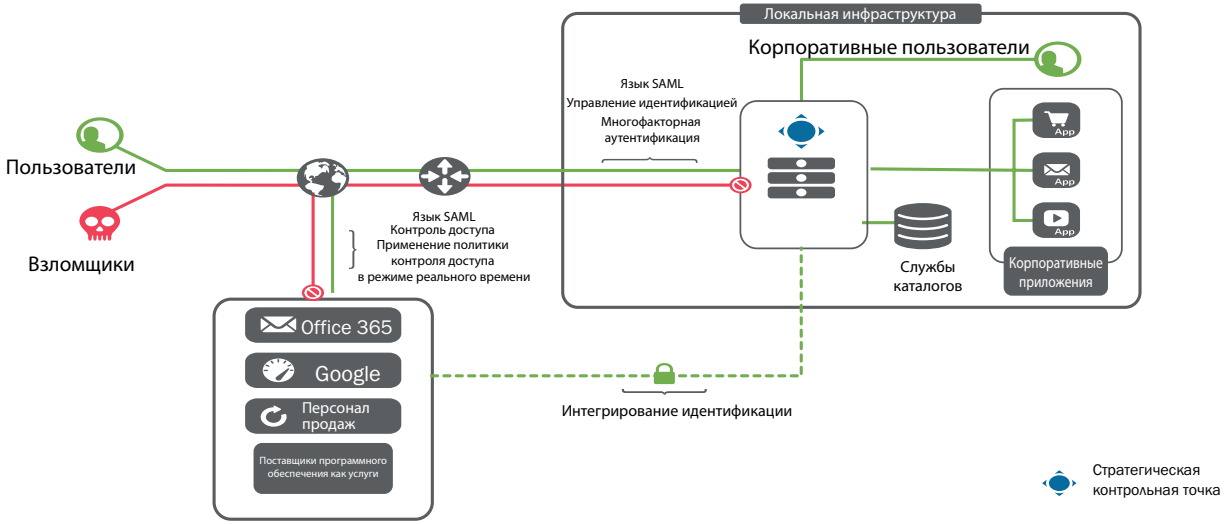
Решение APM (Программа управления политикой доступа) компании F5 обеспечивает единую точку доступа к приложениям независимо от их местоположения, упрощая, консолидируя и управляя защищенным доступом.

APM может обеспечить услуги единого входа в систему (SSO) и/или интегрирования идентификации и подготовки отчетов о типе трафика и доступе пользователей.

Кроме того, мы поддерживаем детализацию на уровне профилей и прав доступа пользователей, централизуя и применяя политики контроля доступа в единой точке инфраструктуры сети.

Мы поддерживаем все типы устройств и операционных систем.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ОБЪЕДИНЕНИЕ РЕШЕНИЙ В ОБЛАЧНЫХ СРЕДАХ



РАСШИРЕННЫЙ КОНТРОЛЬ ДОСТУПА

ЗАДАЧА

Услуги требуют идентификации пользователя для предотвращения несанкционированного доступа.

Рост частоты атак означает, что для доступа пользователя к определенным ресурсам требуется более высокий уровень интеллектуальности. Пароля уже недостаточно, необходимо также учитывать пользовательский контекст - где, как, когда происходит доступ и т. д.

АЛЬТЕРНАТИВЫ

- Одной альтернативой этой технологии является внедрение этой логики непосредственно в приложение, что требует персонализации, перепрограммирования, кодирования, тестирования и т. д. Эта альтернатива, помимо трудоемкости, не может быть продублирована на других приложениях.
- Другой альтернативой может быть использование прокси-серверов от определенных производителей, однако в этом случае отсутствует масштабируемость (и высокая доступность), они несовместимы с различными производителями программного обеспечения, (Это требует наличия пары прокси-серверов на производителя с разными политиками и т. д.) (IBM, SAP, Oracle, MS и т. д.) и промежуточные элементы с малой способностью управлять трафиком шифрования, точками отказа, OPEX++ и т. д.)

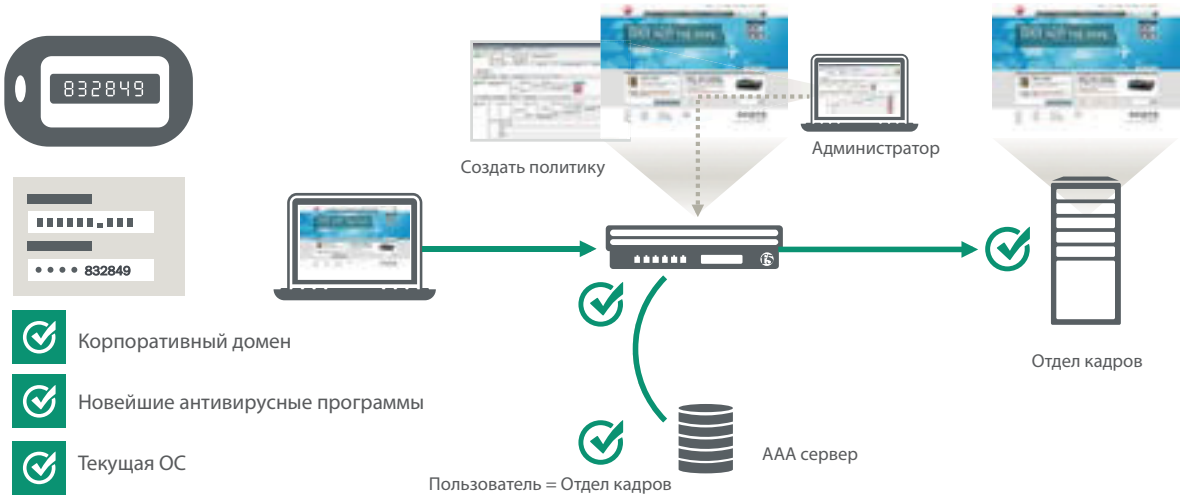
F5 | РЕШЕНИЕ APM

APM от F5 позволяет установить детализированные процедуры доступа к разным услугам, что приводит к персонализированному контролю доступа для каждого приложения и каждой группе пользователей.

Доступ к приложению учитывает контекст пользователя — кто он, откуда он запрашивает доступ и к какой группе принадлежит.

Это решение осуществляет проверку пользователя по разным типам хранилищ (LDAP, RADIUS, AD и т. д.), проверяет статус безопасности устройства, осуществляет аутентификацию с использованием усовершенствованных механизмов, например, SAML.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | РАСШИРЕННЫЙ КОНТРОЛЬ ДОСТУПА



Проверьте доступ пользователя на основе различных параметров: соответствие, административная группа, устройство, геолокация и т. д.
Добавьте двухфакторную аутентификацию на основании контекста Интеграция с управлением мобильными устройствами (MDM) и т. д

СООТВЕТСТВИЕ СТАНДАРТУ БЕЗОПАСНОСТИ PCI DSS

ЗАДАЧА

Консорциум лидеров индустрии платежных карт (PCI) сформировал набор Стандартов безопасности данных (DSS) для организаций, использующих платежные шлюзы на своих интернет-сайтах, или хранящих такие данные. Эти компании должны выполнять минимальные требования безопасности для предотвращения мошенничества. Компании, которые не выполняют это правило, могут быть оштрафованы или даже лишены возможности использовать платежный шлюз.

Одним из наиболее важных из 12 установленных требований является пункт 6. Изначально стандарт требовал разработки кода безопасности и его периодической проверки и т. д. Принимая во внимание сложность выполнения этого требования, при первом пересмотре стандарта он был изменен на возможность использования специализированного решения по обеспечению безопасности (межсетевой экран веб-приложения). Помимо своей оптимальности WAF лучше обеспечивает безопасность.

АЛЬТЕРНАТИВЫ

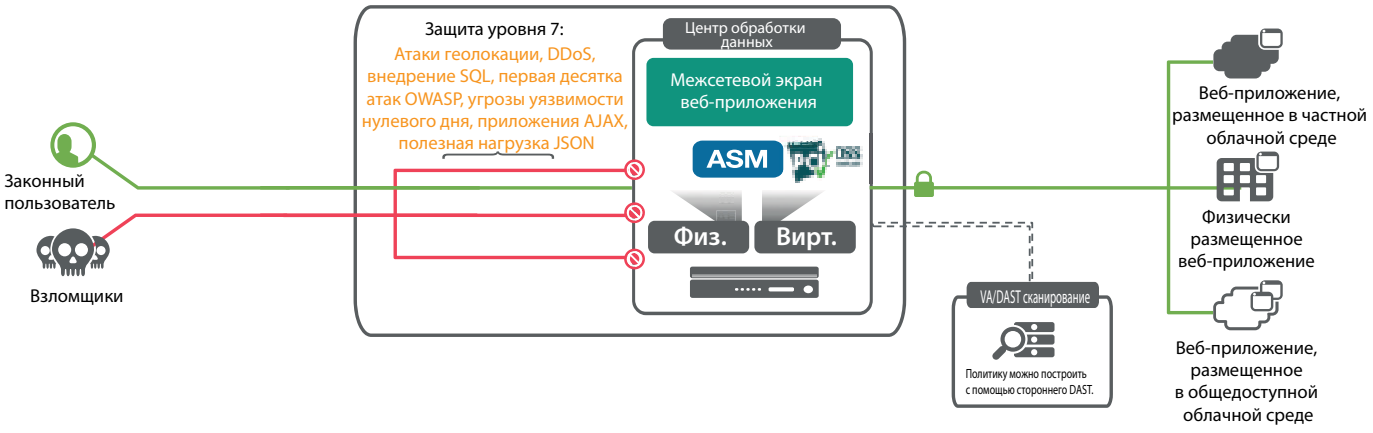
- Применение всех пунктов стандартов PCI DSS в процессе развертывания приложения намного дороже и менее безопасно. Специализированное, регулярно обновляемое устройство, вероятно не будет иметь уязвимостей защиты, в отличие от кодов, которые проверяются каждые шесть месяцев.
- Решения конкурентов помогают «усилить» нормативно-правовое соответствие, но необходимо помнить, что решение F5 широко распространено на рынке и благодаря своему стратегическому расположению в архитектуре клиента (в рамках КДП), технически является наиболее целесообразным.

F5 | РЕШЕНИЕ ASM

ASM (Система управления безопасностью приложений) компании F5 позволяет быстро и просто развертывать модуль межсетевой экран веб-приложения (WAF) и таким образом соответствовать стандартам PCI DSS. ASM развертывается прозрачным для приложений способом, таким образом обеспечивая защиту от атак на веб-приложения, например, OWASP и DDoS.

ASM также создает подробный отчет, в котором отражены аспекты стандарта PCI DSS, которым соответствует или не соответствует приложение.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | COMPLIANCE PCI DSS | СООТВЕТСТВИЕ СТАНДАРТУ БЕЗОПАСНОСТИ PCI DSS



ВЫЯВЛЕНИЕ DDOS-АТАКИ

ЗАДАЧА

Клиенты с одним исходящим интернет-провайдером (ISP) сталкиваются с необходимостью выбора компании с которой заключается договор на защиту против DDoS-атак.

Заключать договора на услуги защиты со всеми поставщиками является нецелесообразным с экономической точки зрения.

С другой стороны, заключение договора с одним поставщиков требует проведения локальной проверки общего трафика от всех поставщиков.

АЛЬТЕРНАТИВЫ

- Заключение договоров на услуги защиты со всеми поставщиками экономически невыгодно и не способствует повышению качества услуги.
- Размещение расширения абонентского конечного оборудования (CPE) для выявления атак в каждом ISP значительно повышает затраты и сложность решения.

F5 | РЕШЕНИЕ AFM + ASM

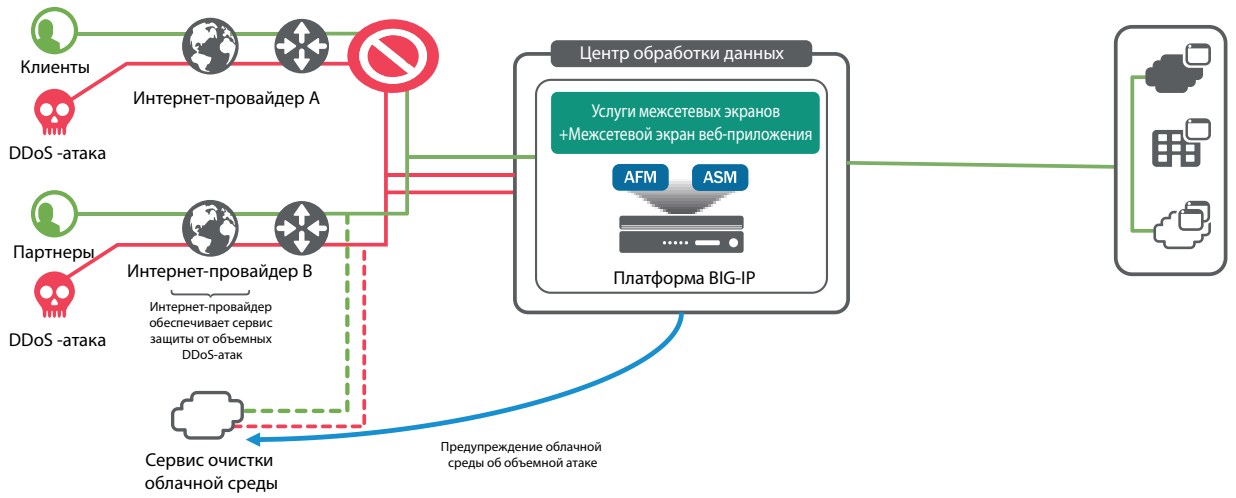
Модули AFM (Расширенная программа управления межсетевыми экранами) и ASM (Система управления безопасностью приложений) компании F5 позволяют обнаружить DDoS-атаки на уровнях от 3 до 7 по всем клиентским линиям Интернет, поэтому мы можем применить стратегию заключения договоров на защиту против объемных DDoS-атак с единым интернет-провайдером.

Как только было установлено, что в одном из интернет-провайдеров происходит атака, платформа F5 ограничивает атаку на уровнях 3-7, сводя ее к пропускной способности линии каждого провайдера, до минимума снижая использование защитных ограничений.

В случае фактической атаки платформа F5 может использовать «облачное предупреждение» для уведомления интернет-провайдера, с которым заключен договор на защиту DDoS, предоставив возможность объявления префиксов сервисов другим интернет-провайдерам, обеспечивая доступность сервисов.

Это решение также относится к ситуации атак на шифрованный трафик.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ВЫЯВЛЕНИЕ DDOS-АТАКИ



ВЫЯВЛЕНИЕ DDOS-АТАКИ НА УРОВНЕ 7 ДЛЯ АКТИВАЦИИ ЗАЩИТЫ ОБЛАЧНОЙ СРЕДЫ

ЗАДАЧА

Выявление DDoS-атак в сети поставщика услуг осуществляется с использованием протокола Net-Flow, уровня 3 (сеть) и уровня 4 (транспорт).

Выявления «низкоуровневых и медленных» атак на 7 уровне (приложение), хотя это эффективный способ смягчения их последствий, как только трафик выходит онлайн и проходит центр смягчения последствий (центры очистки) после оповещения BGP/DNS о перенаправлении трафика.

АЛЬТЕРНАТИВЫ

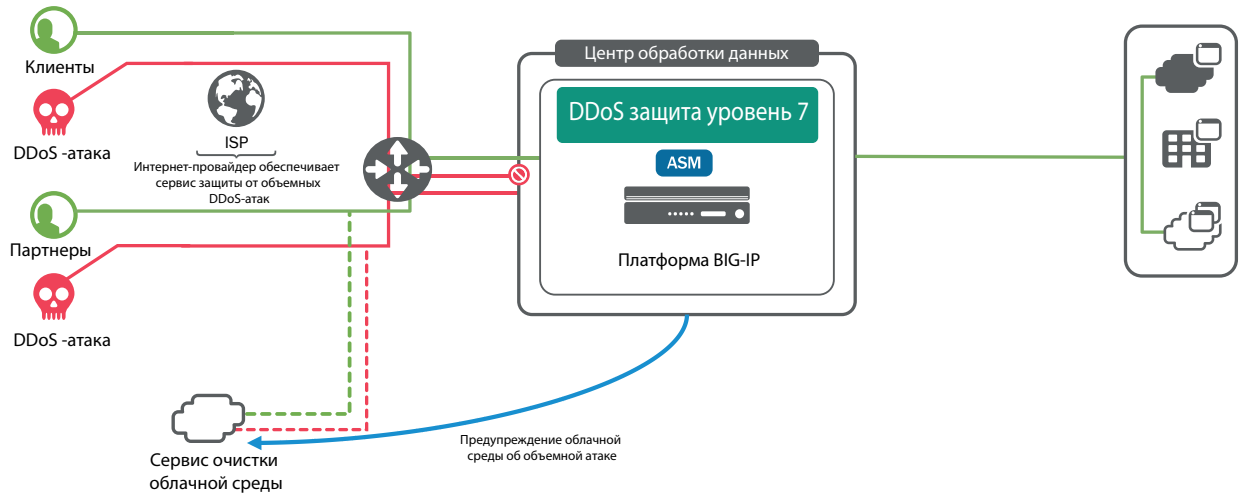
- Операторы сети могут обеспечить оборудование в абонентском пункте клиента для выявление DDoS-атак на 7 уровне, однако это абонентское конечное оборудование (CPE) предназначено специально для этой цели и значительно увеличивает стоимость сервиса.
- Альтернативой может быть постоянная передача трафика онлайн через оператора услуги, это намного дороже и значительно увеличивает задержку всего трафика, даже в случае отсутствия каких-либо атак.

F5 | РЕШЕНИЕ ASM

Решение ASM (Система управления безопасностью приложений) компании F5 развертывается при входе в центр обработки данных, оно определяет все типы DDoS-атак, специфичных для уровня 7, и защищает приложения. С помощью функциональной возможности «облачное предупреждение» ASM сигнализирует об атаке на сервис поставщика услуг, таким образом активируя защиту в облачной среде и минимизируя атаку до того, как она достигнет центра обработки данных.

Решение ASM способно минимизировать DDoS-атаки, специфичные для уровня 7, сводя их к доступной полосе пропускания в центре обработки данных, экономя расходы клиента на активацию услуги по защите облачной среды в случае, когда эти атаки не превышают доступную полосу пропускания.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ВЫЯВЛЕНИЕ DDOS-АТАКИ НА УРОВНЕ 7 ДЛЯ АКТИВАЦИИ ЗАЩИТЫ ОБЛАЧНОЙ СРЕДЫ



ВЫЯВЛЕНИЕ И УМЕНЬШЕНИЕ ПОСЛЕДСТВИЙ DDOS-АТАКИ НА УРОВНЕ 7 ДЛЯ ШИФРОВАННОГО ТРАФИКА

8

ЗАДАЧА

«Низкоуровневые и медленные» атаки шифрованного трафика (HTTP к SSL) на 7 уровне не могут быть выявлены защитными сервисами, которые предлагаются поставщиком услуг или в облачной среде, за исключением случаев, когда мы предоставляем поставщику услуг частные ключи шифрования.

АЛЬТЕРНАТИВЫ

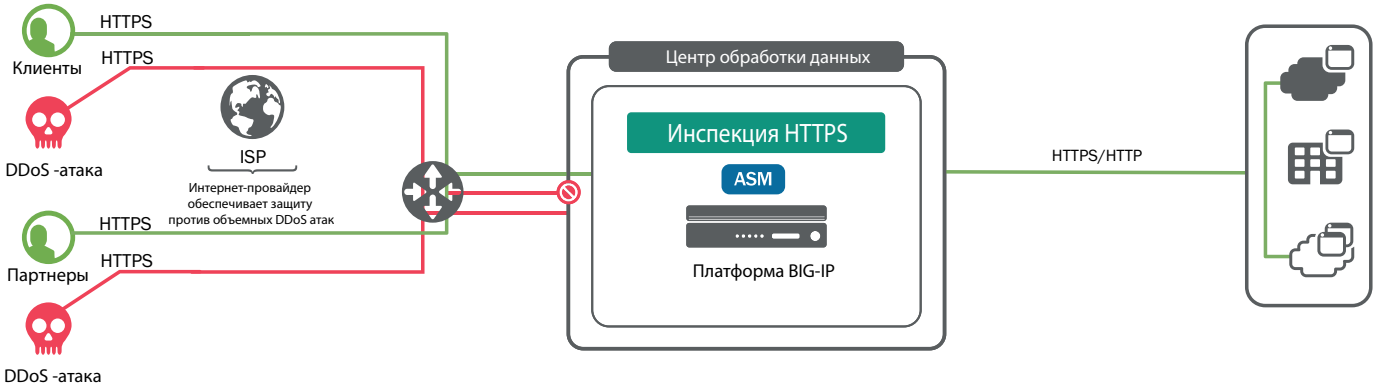
Услуги выявления и защиты шифрованного трафика на уровне 7, предлагаемые провайдером услуг или развернутые в облаке решения требуют частных ключей шифрования. Предоставление таких ключей третьей стороне может нарушать процедуры безопасности или конфиденциальность сервиса.

F5 | РЕШЕНИЕ ASM

Решение ASM (Система управления безопасностью приложений) позволяет локально расшифровывать трафик HTTPS (импортируя частные ключи шифрования) и анализировать возникающий HTTP-трафик, таким образом, идентифицируя все типы DDoS-атак, специфичные для уровня 7, и защищая приложения.

После очищения трафика возможно повторно зашифровать трафик к серверам приложений, даже при условии длины ключа, отличной от оригинала, при этом соответствуя стандартам безопасности сервиса.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ВЫЯВЛЕНИЕ И УМЕНЬШЕНИЕ ПОСЛЕДСТВИЯ DDOS-АТАК НА УРОВНЕ 7 ДЛЯ ШИФРОВАННОГО ТРАФИКА



ШЛЮЗ ОБРАТНОГО ПРОКСИ-СЕРВЕРА

ЗАДАЧА

Достаточно часто шлюзы и обратные прокси-серверы используются для предоставления внешним пользователям доступа к определенному типу приложений для внутреннего использования. Например, для этого часто используются серверы MSFT TMG ил ISA для обеспечения доступа к серверам Exchange / SharePoint или Apache с целью перезаписи URL, однако многие компании также используют такие решения для улучшения безопасности доступа; в таких устройствах трафик HTTPS дешифруется и направляется в незашифрованном виде на серверы или службы аутентификации, особенно с использованием цифровых сертификатов.

Основываясь на приведенных примерах, легко прийти к выводу, что речь идет о специальных решениях согласно типу приложения, ведущих к созданию очень однородных сред, компоненты которых никто не берется Больше точек отказа и большая сложность.

АЛЬТЕРНАТИВЫ

- Частичная обработка обратным прокси-сервером.

F5 | РЕШЕНИЕ APM

Модуль APM (Программа управления политикой доступа) от компании F5 позволяет разрешить все ситуации конфигурации, в которых возникает необходимость использования таких решений, как шлюз доступа или обратный прокси-сервер.

Аутентификация пользователя. Встроенная поддержка как основного, так и нетипичного метода аутентификации.

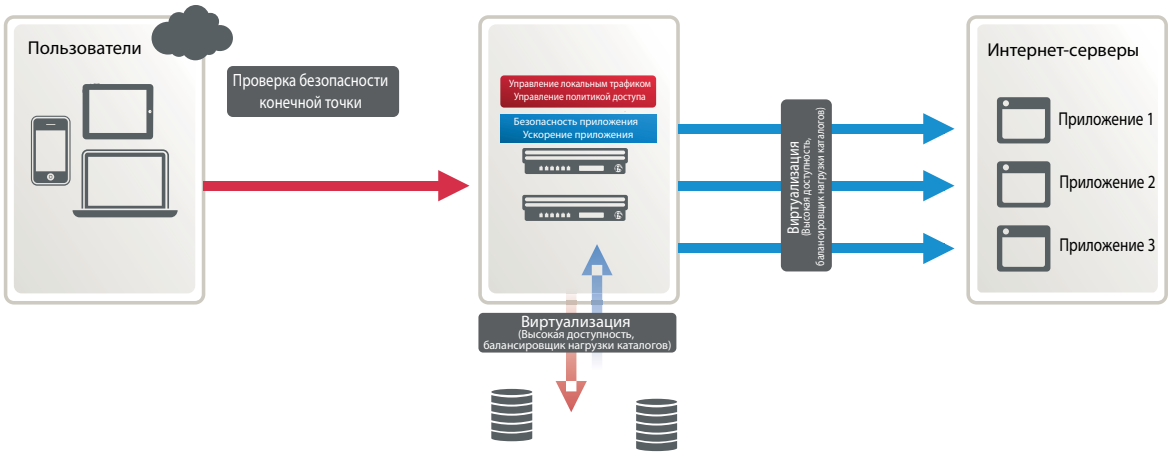
Услуги публикации и переписывания URL-адресов. Внешняя публикация сервисов и перенаправление их на внутренние сервисы и серверы, скрывая фактические внутренние адреса и URL.

Шифрование/дешифрование SSL трафика. Компания F5 включает платы ускорителя протокола SSL в свои аппаратные устройства для оптимального осуществления этих функций.

Публикация сервисов MSFT. Оптимизирует, ускоряет и обеспечивает безопасность выпуска услуг Microsoft, заменяя и улучшая архитектуру и решения серверов TMG или ISA.

Развертывание решений SSL-VPN для покрытия доступа пользователей к приложениям и корпоративным ресурсам с любого устройства и любого местоположения.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ШЛЮЗ ОБРАТНОГО ПРОКСИ-СЕРВЕРА



ЗАЩИТА ОТ БОТОВ В СРЕДАХ OWA

ЗАДАЧА

Электронная почта является одним из самых распространенных (и уязвимых) приложений в корпоративных средах. DoS/DDoS-атаки на интернет-порталы Exchange (OWA) основываются на идее предотвращения доступа пользователя, аутентифицированного Атака происходит путем попыток аутентификации пользователя, который неправильно вводит пароль доступа более 3 раз, что приводит к тому, что AD автоматически активирует метод защиты для блокировки доступа для этого пользователя. Как известно, когда речь идет о DDoS-атаке, она охватывает множество пользователей (иногда атака всех пользователей, зарегистрированных в AD компании).

Большой проблемой является тот факт, что такие атаки заранее предполагают, что ни одна компания не способна проверять, управлять и анализировать вся информацию в Exchange, а также существует опасность, связанная с раскрытием информации в почтовых ящиках.

АЛЬТЕРНАТИВЫ

- Вы можете настроить службу Active Directory для увеличения количества попыток, разрешенных для одного пользователя, до того как он будет заблокирован, или можете оставить его незащищенным, что не сможет защитить пользователей от DDoS-атак.

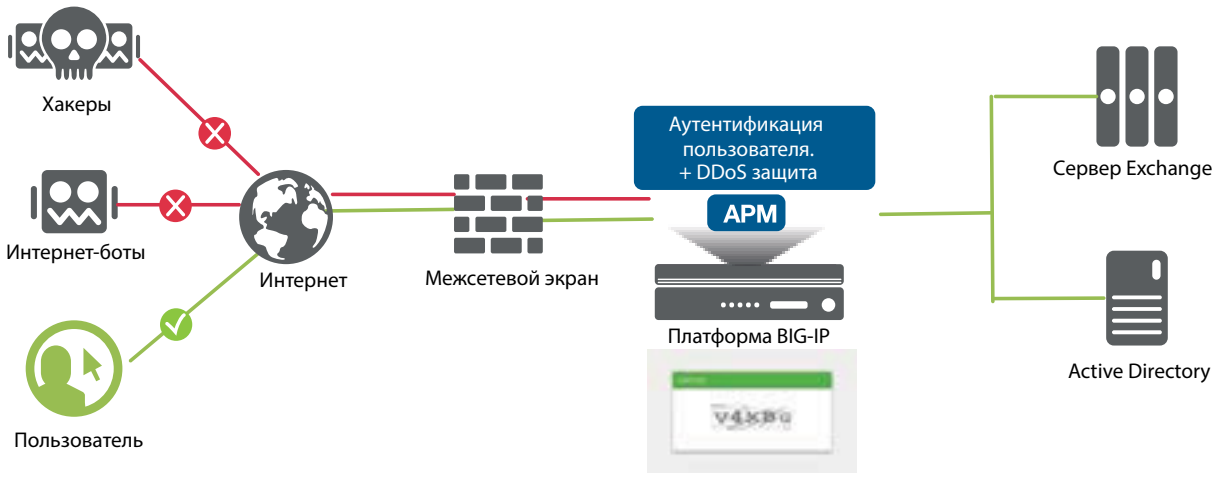
F5 | РЕШЕНИЕ APM

Компания F5 предлагает дополнить уровень управления расширенной аутентификацией пользователей. Это решение (APM - Программа управления политикой доступа) стремится консолидировать всех пользователей приложения (как внутренних так и внешних).

APM может обеспечить экран доступа пользователей, внешний вид которого подходит для приложения (например,

Exchange) и может управлять аутентификацией всех пользователей для данного приложения. Таким способом мы можем контролировать количество попыток аутентификации, разрешенных для одного пользователя (меньше, чем разрешено AD), чтобы избежать блокировки пользователей в AD. В случае превышения количества попыток, можно представить другие механизмы безопасности, например, двухфакторную аутентификацию OTP, Captcha и т. д.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ЗАЩИТА ОТ БОТОВ В СРЕДАХ OWA



ЗАЩИТА ИНФРАСТРУКТУРЫ DNS

ЗАДАЧА

Компании используют сервис DNS для предоставления пользователям доступа к веб-приложениям. Если сервис DNS недоступен (или есть сбой в работе), доступ к этим приложениям не гарантирован.

Очень важно оптимизировать и обеспечить безопасность инфраструктуры DNS для гарантии предоставления сервиса пользователям. Эксплуатация инфраструктуры DNS требует возможности ответа на большое количество запросов в секунду, а способность осуществлять быстрое масштабирование становится критически важным в ситуациях, когда приходится обрабатывать тысячи доменных имен.

Также необходимо обеспечить защиту пользователя и целостность сервиса от DDoS-атак, отравления кэша и туннелирования DNS.

АЛЬТЕРНАТИВЫ

- Решения на основе BIND дороги в эксплуатации в связи с необходимостью частых обновлений для противостояний постоянным угрозам.
- Традиционные решения DNS трудно и затратно масштабировать, не существует гибких и/или продвинутых интегрированных решений безопасности специально для DNS.

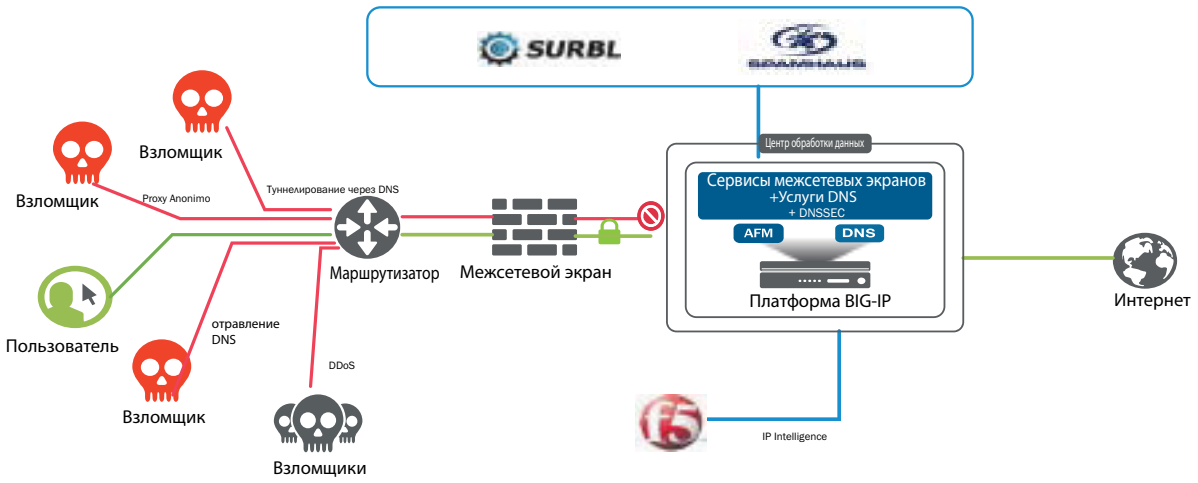
F5 | РЕШЕНИЕ DNS + AFM

BIG-IP DNS + AFM (Расширенная программа управления межсетевыми экранами) позволяет операторам услуг оптимизировать, обеспечить безопасность и монетизировать инфраструктуру DNS. Это решение предоставляет услуги кэширования LDNS, развертываясь на уровне устройств операторского класса с высокой производительностью, а также является гипермасштабируемым полномочным решением DNS, которое включает услуги межсетевых экранов DNS, которые используют аппаратное обеспечение для уменьшения последствий DDoS-атак на DNS. BIG-IP DNS + AFM обеспечивает интеллектуальную и масштабируемую инфраструктуру DNS, позволяющую быстро отвечать на запросы пользователей мобильных устройств. Управляя адаптируемыми и GSLB услугами, организации могут распределять соответствующие ресурсы для ответа на запросы DNS и гарантировать наилучшие впечатления пользователей. BIG-IP DNS также делает возможным использование DNS64 в средах Pv6 с отказоустойчивой инфраструктурой, оптимизируя трафик и повышая качество услуги для пользователей, таким образом защищая торговую марку и репутацию бизнеса.

Кроме того, BIG-IP DNS + AFM защищают инфраструктуру DNS от вредоносных атак зараженных пользователей или нежелательных запросов и ответов DNS. Интеллектуальный DNS от компании F5 имеет межсетевой экран, который проверяет и удостоверяет протоколы и сбрасывает или отказывает в приеме незапрашиваемых ответов. Он также уменьшает влияние атак путем блокировки доступа к вредоносным доменам.

И наконец, BIG-IP DNS предоставляет статистические данные и отчеты, а также включает функциональные возможности для высокоскоростной регистрации, позволяющей DNS осуществлять планирование производительности, оптимизацию и монетизацию сервисов.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ЗАЩИТА ИНФРАСТРУКТУРЫ DNS



ЗАЩИТА ПУБЛИЧНЫХ ПОРТАЛОВ

ЗАДАЧА

Города населенностью более 20 000 человек часто предоставляют услуги общего пользования в форме «единого портала услуг общего пользования». Осуществление транзакций в режиме реального времени (например, оплата налога на недвижимость и т. д.) требует наличия системы обработки транзакций. личная информация о плательщике являются важными данными, и это означает, что городская администрация должна обеспечить безопасность и конфиденциальность электронных транзакций.

Кроме того, городские власти имеют систему доступа для внутренних и внешних сотрудников, а в некоторых случаях и для горожан. Эта услуга требует идентификации пользователя для предотвращения неавторизованного доступа и для контроля доступа к различным услугам и приложениям на основе профилей пользователей. В связи с постоянно растущей частотой атак возникает необходимость в высокоинтелектуальных приложениях, которые дадут возможность пользователю получить доступ к определенному ресурсу – пароля больше недостаточно. Чрезвычайно важно учитывать контекст пользователя - где, каким образом, когда он входит в систему и т. д.

С этой же проблемой сталкиваются органы местного самоуправления, предоставляющие подобные услуги городским администрациям меньшего размера.

АЛЬТЕРНАТИВЫ

- Альтернативным решением для защиты веб-приложения может быть внедрение более безопасных процедур разработки приложений, что может привести к разногласиям в организации, значительным задержкам в разработке приложений и существенном повышении издержек на разработку, при этом отказ от каких-либо действий влечет за собой огромный риск для репутации компании.
- Одной альтернативой этой технологии является внедрение этой логики непосредственно в приложение, что требует персонализации, перепрограммирования, кодирования, тестирования и т. д. Эта альтернатива, помимо трудоемкости, не может быть продублирована на других приложениях.

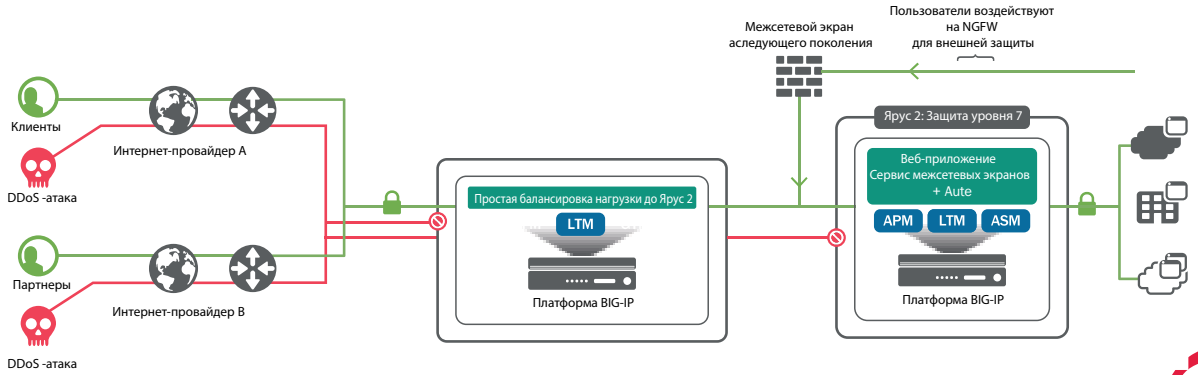
F5 | РЕШЕНИЕ ASM + APM

Двойная проблема обеспечения безопасности интернет-приложений и доступа пользователя решается путем дополнения инфраструктуры двумя функциональными возможностями от компании F5.

Модуль ASM (Система управления безопасностью приложений) компании F5 позволяет быстро и просто развертывать WAF прозрачным для приложений способом, и таким образом обеспечивать защиту против атак на интернет-приложения, например, OWASP и DDoS. С помощью этого модуля городские администрации и областные органы власти могут гарантировать жителям безопасность всех данных, предоставленных в веб-приложениях, и что эти данные не обнаружат взломщики. Эти модули защищают сеть от DDoS-атак на уровне 7, гарантируя сохранность имиджа органа власти. ASM предлагает функцию составления отчетов, которые содержат подробную информацию, касающуюся уровня безопасности приложения. Кроме того, компания F5 поддерживает интеграцию с ведущими разработчиками инструментов DAST, это означает, что ваш отчет может быть быстро включен, позволяя избежать большинства OWASP-атак.

APM (Программа управления стратегией доступа) от компании F5 позволяет установить детализированные процедуры доступа к разным услугам, что приводит к персонализированному контролю доступа для каждого приложения и каждой группе пользователей. Доступ к приложению учитывает контекст пользователя — кто он, откуда он запрашивает доступ и к какой группе принадлежит. RADIUS, AD и т. д.), проверяет статус безопасности устройства, осуществляет аутентификацию с использованием усовершенствованных механизмов, например, SAML, Kerberos, NTLM и т.д., а также поддерживает многофакторную аутентификацию в соответствии с контекстом пользователя.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА| ЗАЩИТА ПУБЛИЧНЫХ ПОРТАЛОВ



ПОСТОЯННО РАБОТАЮЩЕЕ РЕШЕНИЕ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

ЗАДАЧА

Пользователям мобильных устройств, находящимся в роуминге, требуется стабильное и безопасное VPN-соединение. Одной из самых больших проблем, с которой сталкиваются пользователи, особенно в роуминге. доступ с мобильного устройства, в один момент может быть подключен к сети Wi-Fi, через минуту к соединению 3G/4G. Каждый раз, когда соединение обрывается, клиенту VPN снова приходится подключаться.

АЛЬТЕРНАТИВЫ

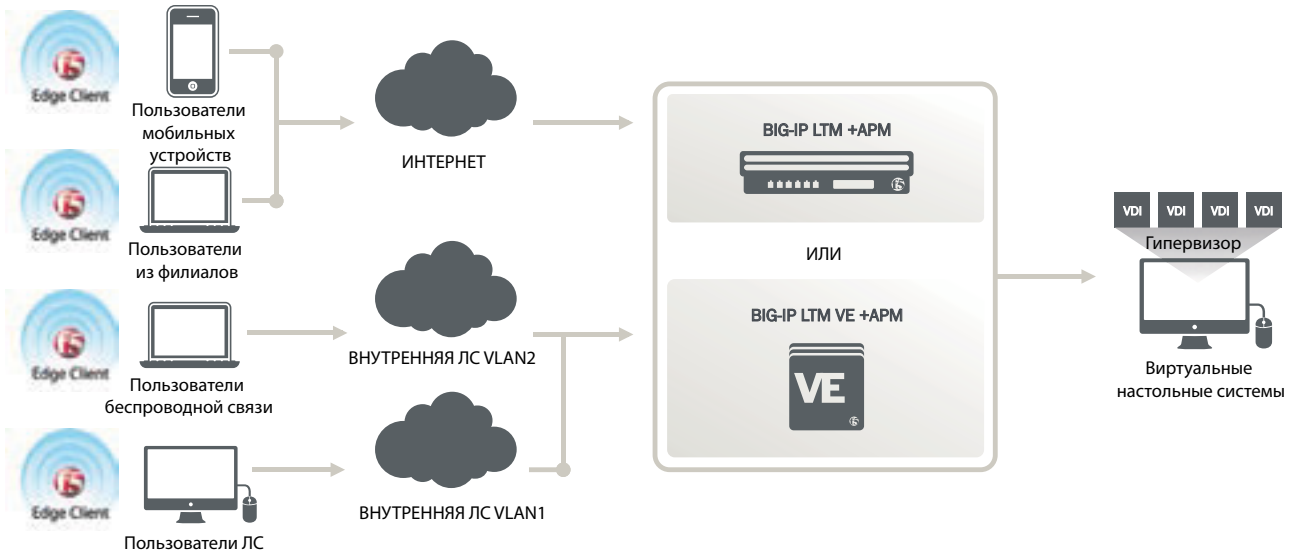
- Собственная разработка

F5 | РЕШЕНИЕ APM

Модуль APM от компании F5 позволяет развернуть решения для доступа VPN-SSL, чтобы охватить доступ к приложениям и корпоративным ресурсам с любого устройства и любого места.

С развертыванием Edge VPN-клиента от компании F5 для мобильных и настольных действий APM могут настроить постоянное подсоединение. Такая функциональная возможность позволяет автоматически подключаться с устройства клиента к корпоративной сети, при этом клиенту не нужно предпринимать каких-либо действий. После установления активного подключения к данным клиент Edge Gateway автоматически устанавливает туннель в корпоративную сеть.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ПОСТОЯННО РАБОТАЮЩЕЕ РЕШЕНИЕ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ



РЕШЕНИЕ ЕДИНОГО ВХОДА В СИСТЕМУ

ЗАДАЧА

Единый вход в систему – это удобный, практичный и безопасный концептуальный механизм аутентификации, который позволяет пользователю получить доступ ко многим приложениям с помощью одного набора учетных данных.

В настоящее время число используемых приложений (включая корпоративные) постоянно растет. Получение доступа к этим приложениям требует повторного введения учетных данных пользователя, что снижает производительность и впечатление пользователя.

Кроме того, решения программного обеспечения как услуги (SaaS), такие как Salesforce, Office 365, SharePoint Online и др., создают проблему безопасности, так так пользователи начинают пользоваться одним паролем для все приложений или записывают их, чтобы не забыть.

АЛЬТЕРНАТИВЫ

- Использование основанных на клиентах (приложениях или устройствах) решений SSO требует, чтобы эти клиенты были управляемыми, а также представляет проблемы совместимости (между приложениями, браузерами и т. д.).

F5 | РЕШЕНИЕ APM

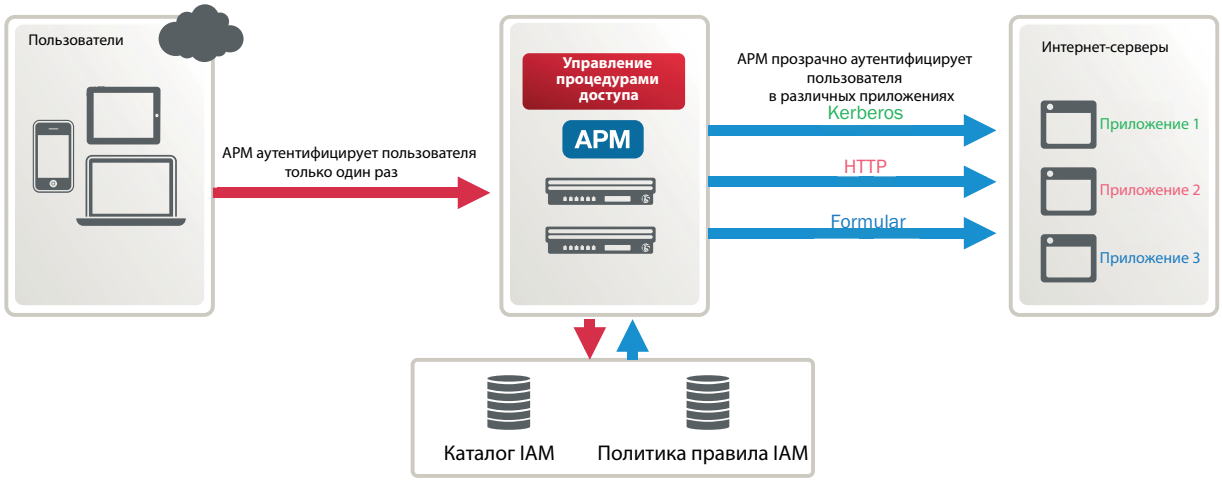
APM (Программа управления политикой доступа) от компании F5 позволяет аутентифицировать пользователя, используя множество параметров, в зависимости от контекста, для того, чтобы разрешить или отклонить доступ к определенному приложению.

После того, как пользователь был аутентифицирован APM, его учетные данные автоматически отправляются в приложения при попытке пользователя получить к ним доступ, таким образом устраняя необходимость повторного ввода. APM отправляет эти учетные данные в формате, требуемом каждым приложением, словно пользователь делает это самостоятельно.

APM применяет механизмы единого входа в систему (SSO) централизованным способом, прозрачным для приложений.

Например, APM можем аутентифицировать пользователя путем проверки цифрового сертификата, а затем аутентифицировать его в другом приложении с использованием интернет-формы, а для третьего приложения применить аутентификацию Kerberos.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | РЕШЕНИЕ ЕДИНОГО ВХОДА В СИСТЕМУ



ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ (WAF)

ЗАДАЧА

Во многих случаях безопасность компании очень зависит от безопасности веб-приложений, которые были разработаны другими отделами и которые вы не можете контролировать, или, что еще хуже, были разработаны внешними подрядчиками, которые больше внимания уделяли функциональным возможностям и скорости разработки, чем вопросам безопасности. Типичные атаки, например, известные как первая десятка OWASP-атак (внедрение SQL, межсайтовые сценарии и пр.) могут привести к утечке ценной информации компании с экономическими или даже юридическими последствиями для организации. Аналогично, специфические для Интернет (уровня 7) DDoS-атаки могут привести к потере обслуживания для клиентов. Кроме того, правила стандарта безопасности PCI DSS требуют применения устройств интернет-защиты для скрытия важного контента.

АЛЬТЕРНАТИВЫ

- Внедрение более безопасных политик для разработки приложений, что может привести к разногласиям в организации, значительным задержкам
- Отказ от каких-либо действий влечет за собой огромный риск и означает несоблюдение нормативных требований.

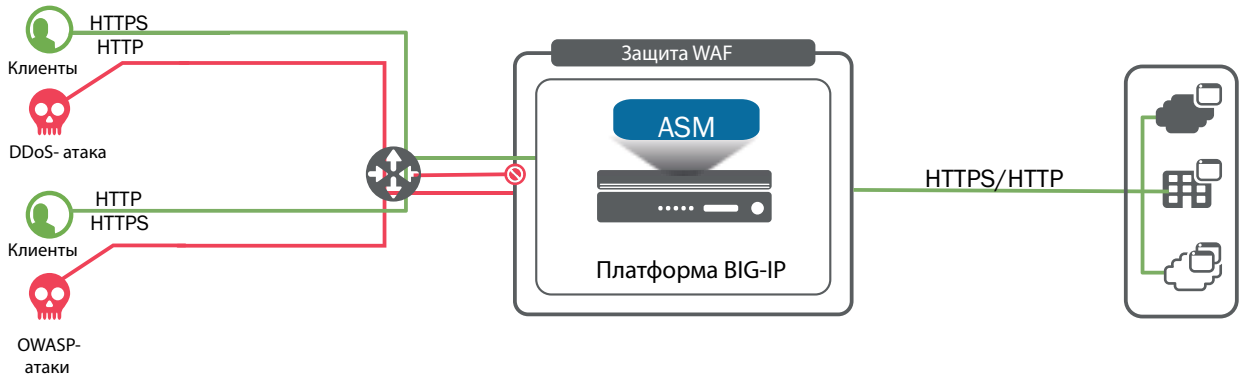
F5 | РЕШЕНИЕ ASM

Модуль ASM (Система управления безопасностью приложений) компании F5 позволяет быстро и просто развертывать WAF прозрачным для приложений способом, и таким образом обеспечивать защиту против атак на интернет-приложения, например, OWASP и DDoS. Он также включает модуль контроля соответствия со стандартом PCI DSS.

Вслед за первоначальным периодом изучения, в течение которого APM распознает нормальные шаблоны работы веб-приложения, активируется защита WAF. Она является специфичной для каждого URL-адреса, а пользователь может указывать порог включения автоматической защиты.

Оборудование можно настроить для работы с белыми и черными списками.

РЕФЕРЕНСНАЯ АРХИТЕКТУРА | ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ (WAF)



bako tech®

BAKOTECH – международная группа компаний, которая занимает лидирующие позиции в сфере фокусной Value Added IT-дистрибуции и поставляет решения ведущих мировых IT-производителей. Позиционируя себя как True Value Added IT-дистрибьютор, BAKOTECH предоставляет профессиональную до- и пост-продажную, маркетинговую, техническую поддержку для партнеров и конечных заказчиков.

BAKOTECH - официальный дистрибьютор решений F5.

f5.bakotech.com f5@bakotech.com