Citrix NetScaler — основа безопасности центров обработки данных нового поколения

CITRIX®

www.citrix.com

Введение

Сегодня безопасность центров обработки данных важнее, чем когда-либо. К обычным задачам и проблемам – включая обширные нормативные требования, увеличение целенаправленных атак и непрекращающееся снижение эффективности моделей защиты, ориентированных на периметр сети, – теперь добавилась необходимость учитывать динамично развивающиеся корпоративные облачные архитектуры и плоские сети, имеющие меньше естественных «узких мест». Добавьте к этому неизменное стремление к оптимизации затрат, и вам станет ясно, что в основе более эффективной системы безопасности должна лежать существующая инфраструктура центра обработки данных.

Citrix NetScaler, лучший контроллер доставки приложения (ADC) для построения корпоративных облачных сетей, представляет собой именно такое решение. Уже являясь стратегическим компонентом в тысячах корпоративных центров обработки данных, NetScaler предлагает набор всех необходимых функций для обеспечения безопасности. Более того, он сводит к минимуму для предприятий необходимость вложений в большое число дорогих автономных решений по обеспечению безопасности. NetScaler не только обеспечивает критически важную безопасность приложений, сети или инфраструктуры и управление идентификационной информацией пользователей и доступом, но также обеспечивает поддержку богатой экосистемы партнерских продуктов, предназначенных для смежных доменов безопасности.

Функции по обеспечению безопасности центров обработки данных

Безопасность приложений
- NetScaler Application Firewall
- Защита от потери данных
- Защита от атак на 7 уровне сетевой модели

Безопасность сети/инфраструктуры
- Бескомпромиссное SSL-шифрование
- Защита DNS-сервера
- Защита от атак на 4 уровне сетевой модели

Управление идентификационной информацией пользователей и доступом

Система безопасности / партнерская экосистема

Это создает надежную основу для экономически выгодной системы безопасности центров обработки данных нового поколения.

NetScaler обеспечивает безопасность приложений

Специалисты в области безопасности не без основания тратят значительное количество времени, сил и средств на обеспечение безопасности на уровне приложений. Ведь атаки, направленные на уязвимые службы уровня приложений, ненадежные бизнес-системы и ценные данные, подтвердили свою успешность.

Соответственно, NetScaler включает множество средств защиты на уровне приложений, в том числе полнофункциональный межсетевой экран, работающий на уровне приложений, защиту от потери данных и меры, направленные против DoS-атак и других атак на 7 уровне сетевой модели.

NetScaler Application Firewall

Обычным межсетевым экранам не хватает прозрачности и гибкости, необходимой для защиты более чем от 70 % интернет-атак, использующих уязвимости на уровне приложений. На этом основана работа NetScaler Application Firewall, комплексного решения по обеспечению безопасности веб-приложений, прошедшего сертификацию ICSA и позволяющего блокировать известные и неизвестные атаки на веб приложения и службы. Application Firewall основан на гибридной модели безопасности и позволяет анализировать весь трафик в обоих направлениях, в том числе и при использовании SSL-шифрования, что обеспечивает защиту от широкого спектра угроз безопасности, не требуя внесения изменений в приложения.

Гибридная модель безопасности. Сочетание позитивной и негативной моделей безопасности обеспечивает самую полную защиту от всех видов атак. Позитивная модель позволяет автоматически блокировать трафик всех приложений, кроме разрешенных, для защиты от новых, еще неизвестных эксплойтов. Негативная модель в свою очередь обеспечивает защиту приложений от известных угроз с помощью сигнатур атак.

Защита XML. Кроме блокирования распространенных угроз, которые могут быть использованы для атак на XML-приложения (например, межсайтовый скриптинг, внедрение команд и т. д.), Application Firewall включает богатый набор средств защиты специфичный для XML. К таким средствам относятся: проверка схем для тщательной проверки сообщений SOAP и полезных нагрузок XML, возможность блокирования вложений XML, содержащих вредоносный код, защита от методов внедрения операторов XPath, позволяющих получить неавторизованный доступ, а также возможность блокирования соответствующих DoS-атак (например, рекурсии чрезмерной глубины).

Передовые методы защиты динамических элементов. В дополнение к профилю защиты по умолчанию расширенный профиль позволяет обеспечить базовую защиту приложений, обрабатывающих пользовательское содержимое. Многочисленные методы защиты с поддержкой сессий обеспечивают безопасность динамических элементов приложений (например, файлов cookies, полей форм и сессионных URL-адресов), тем самым предотвращая атаки, направленные на доверительные отношения между клиентом и сервером (например, подделка межсайтовых запросов). Динамические элементы приложений регулируются позитивной моделью безопасности, которая позволяет обеспечить их безопасность без явного указания каждого динамического элемента в списке. Необходимость указывать только исключения облегчает конфигурирование и управление изменениями.

Индивидуальные политики безопасности. Прогрессивная самообучающаяся платформа автоматически определяет ожидаемое поведение корпоративных веб-приложений и дает понятные рекомендации по поводу политики. Затем администраторы могут привести политику безопасности в соответствие с уникальными требованиями каждого приложения и предотвратить возможные ложные срабатывания.

Гарантированное соответствие требованиям регулирующих органов. Application Firewall позволяет предприятиям соответствовать требованиям в области безопасности данных, например стандарту безопасности данных в индустрии платежных карт, в котором явным образом рекомендуется использование межсетевых экранов для клиентоориентированных приложений по обработке информации о

кредитных картах. Можно создавать подробные отчеты, документирующие все средства защиты, предусмотренные политикой межсетевого экрана, которые относятся к нормативам PCI.

Бескомпромиссная производительность. Самое высокопроизводительное решение для безопасности веб-приложений в отрасли обеспечивает пропускную способность до 12 Гбит/с при комплексной защите, не снижая время отклика приложений. Кроме того, NetScaler повышает производительность приложений благодаря использованию прогрессивных технологий ускорения работы (например, кэширования содержимого) и возможностей разгрузки сервера (например, управления соединениями TCP, SSL-шифрования/дешифрования и сжатия данных).

Полностью интегрированная архитектура. Application Firewall не просто развернут на платформе NetScaler, а тесно интегрирован с ней. Обмен данными на уровне объектов и политик упрощает администрирование, а обмен процессами на уровне системы обеспечивает высокую производительность, избавляя от необходимости в обработке пакетов в несколько проходов.

Защита от потери данных

Неожиданная утечка конфиденциальных данных с сервера приложений может быть вызвана успешной атакой на приложение, недочетом в его архитектуре или ненадлежащим его использованием со стороны авторизованного пользователя. Активная защита от подобных утечек — это разумная мера предосторожности со стороны предприятия и неотъемлемая часть комплексной стратегии безопасности. NetScaler соответствует этому требованию благодаря понятной и удобной в использовании функции защиты от потери данных.

Проверка данных безопасных объектов является важной функцией NetScaler Application Firewall, которая обеспечивает настраиваемую администратором защиту конфиденциальной деловой информации, например номеров социального страхования, кодов приказов и телефонных номеров для определенной страны/региона. Сведения о формате данной информации передаются межсетевому экрану с помощью определяемого администратором регулярного выражения или пользовательской надстройки, которые также определяют правила, используемые для защиты от утечки. Если строка в запросе пользователя соответствует описанию безопасного объекта, межсетевой экран может предпринять соответствующие действия, в том числе:

- заблокировать ответ;
- замаскировать защищенную информацию;
- удалить защищенную информацию из ответа до его отправки пользователю.

Можно указывать различные действия для каждого отдельного правила безопасного объекта.

NetScaler также включает средства проверки кредитных карт для предотвращения случайной утечки номеров кредитных карт. Проверка информации в заголовке и данных о полезной нагрузке обеспечивает необходимую тщательность для того, чтобы предотвратить ошибочные отказы, а сравнение строк с использованием алгоритма дает точность, необходимую для предотвращения ошибочного доступа. Если обнаружен номер кредитной карты, а администратор не разрешил отправку номеров кредитных карт данному приложению, то можно заблокировать ответ полностью или замаскировать все цифры номера, кроме последних четырех (например, xxxx-xxxx-xxxx-5678).

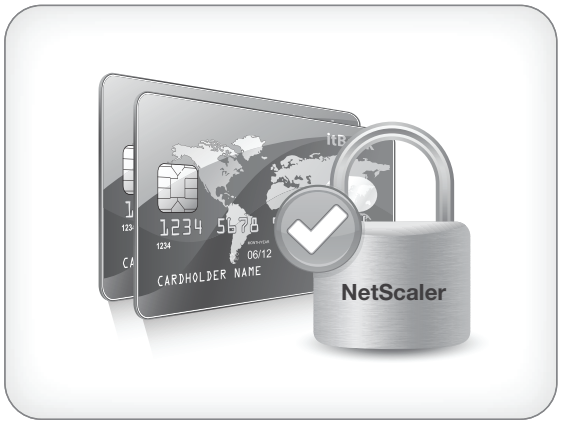

Рисунок 1. NetScaler защищает от утечек конфиденциальной информации потребителей.

В результате специалисты по ИТ-безопасности получают еще один мощный набор функций, который можно использовать не только для отслеживания случаев злоупотреблений и успешных атак, но и для существенного уменьшения причинённого вреда.

Дополнительная защита от атак на 7 уровне сетевой модели

NetScaler имеет несколько дополнительных механизмов защиты от атак на уровне приложений.

Проверка протокола HTTP. NetScaler крайне эффективно защищает от целого спектра атак на основе неверно сформированных запросов и запрещенного поведения по протоколу HTTP, что гарантирует соответствие стандарту RFC, и обеспечивает максимальную эффективность работы при использовании HTTP. Можно также включить в политику безопасности дополнительные пользовательские проверки, воспользовавшись интегрированным фильтром содержимого, пользовательской настройкой мер реагирования и функцией двусторонней перезаписи по протоколу HTTP. Возможные сферы применения: блокирование доступа пользователей к определенным разделам веб-сайта, если они подключаются не из разрешенных мест; защита от угроз на основе HTTP (например, Nimda, Code Red) и удаление из ответов сервера информации, которая может быть использована для совершения атаки.

Рисунок 2. Citrix NetScaler обеспечивает безопасность веб-приложений.

Защита от DoS-атак по протоколу HTTP. Применяется инновационный метод для предотвращения множественных запросов HTTP GET. При обнаружении атаки (на основании настраиваемого порога по количеству запросов в очереди) заданному проценту клиентов посылается несложная задача для расчета. Эта задача построена таким образом, что настоящие клиенты могут легко выполнить ее, а «глупые» DoS-боты не могут. Это позволяет NetScaler отличить ложные запросы от запросов настоящих пользователей приложения. Можно применить адаптивные лимиты времени и другие механизмы для защиты от других видов DoS-атак, например SlowRead и SlowPost.

Ограничение квоты (и не только). Одним из способов защиты от DoS-атак является предотвращение перегрузки сети и серверов путем дросселирования или перенаправления трафика, превышающего указанный лимит. Для этого с помощью средства управления квотами AppExpert запускаются политики NetScaler на основе подключения, запроса или скоростей передачи данных на/с определенного ресурса (например, виртуального сервера, домена или URL-адреса). К родственным функциям относятся:

- защита от скачков нагрузки для уменьшения воздействия скачков уровня трафика на серверы;
- формирование очередей в порядке приоритета, гарантирующее, что критически важные ресурсы получат преимущество перед менее важными ресурсами в периоды высокой нагрузки.

NetScaler обеспечивает безопасность сети и инфраструктуры

NetScaler также включает несколько функций по обеспечению безопасности сети и инфраструктуры. Наиболее значительные из этих функций — полная поддержка SSL-шифрования, защита DNS и защита от атак на 4 уровне сетевой модели.

Бескомпромиссное SSL-шифрование

Контроллеры доставки приложений должны иметь возможность обработки трафика с SSL-шифрованием для того, чтобы гарантировать, что действие политик доставки приложений распространяется на зашифрованный трафик, а также для разгрузки инфраструктуры серверов прикладного ПО. Однако наличие лишь базовой функциональности в этой области уже недостаточно, поскольку два фактора повышают требования к обработке SSL-трафика настолько, что ресурсы инфраструктуры не могут с ними справиться.

Во-первых, все больше предприятий следуют принципу SSL Везде. Обычно это связано со стремлением успокоить потребителей и защититься от таких средств взлома, как Firesheep. В таком случае шифрование используется не только в уязвимых частях приложения – таких, как страница входа в систему, – но и во всем поверхностном слое приложения. В результате сфера влияния SSL резко возрастает.

Вторая проблема связана с заменой 1024-битных ключей шифрования на 2048-битные ключи (большего размера). В соответствии с рекомендациями Национального института стандартов и технологий США (U.S. National Institute of Standards and Technology, NIST) основные поставщики браузеров планируют прекратить поддержку веб-сайтов, использующих ключи с длиной менее 2048 бит, после 31 декабря 2013 г. Это приведет к радикальному повышению надежности шифрования, но также увеличит нагрузку при обработке как минимум в 5 раз.

Устройства NetScaler позволяют решить обе эти проблемы. Благодаря отдельному оборудованию для ускорения SSL-шифрования с поддержкой ключей с длиной 2048 и 4096 бит, NetScaler отвечает основным требованиям к шифрованию, избавляя от необходимости искать компромисс между безопасностью и комфортностью работы пользователя.

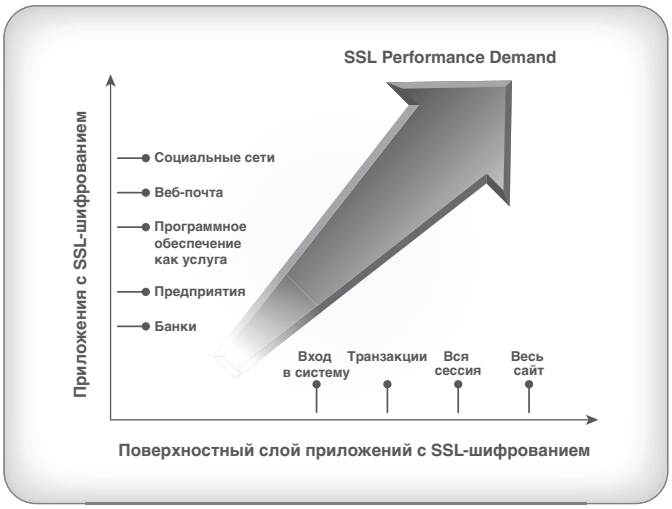

Рисунок 3. Применение SSL-шифрования повсюду повышает требования к безопасности и производительности.

Еще одна родственная функция — шифрование на основе политик. Эта функция позволяет администраторам настроить NetScaler на автоматическое частичное шифрование старых версий веб-приложений, которые ранее не поддерживали шифрование, а теперь поддерживают его.

Также доступны модели соответствующие стандарту FIPS 140-2, Уровень 2. Они предназначены для организаций, которые нуждаются в максимально надежном шифровании.

Защита DNS-сервера

Служба DNS — неотъемлемая часть инфраструктуры современного центра обработки данных. Отсутствие надежной защиты DNS-сервера ставит под угрозу готовность к работе и доступность ключевых служб и приложений.

Кроме полномасштабной балансировки нагрузки на внутренние DNS-серверы организации при работе в режиме прокси, NetScaler также может выполнять роль полномочного DNS-сервера (ADNS), напрямую обрабатывающего запросы имени и IP-адреса.

NetScaler обеспечивает безопасность при любом сценарии развертывания благодаря следующим функциям.

Высокая надежность. Реализация сервера DNS с помощью NetScaler изначально рассчитана на высокую надежность и основана не на ПО с открытым исходным кодом BIND, а следовательно, не подвержена уязвимостям, которые постоянно находят в BIND.

Соответствие требованиям RFC. NetScaler осуществляет полную проверку DNS-протокола и автоматически блокирует атаки на основе неверно сформированных DNS-запросов или других видов ненадлежащего использования DNS.

Ограничение квоты DNS по умолчанию. Для предотвращения атак на основе множественных DNS-запросов можно ограничить квоту или настроить блокировку запросов с заданными параметрами. Можно блокировать запросы на основе их вида и/или доменного имени. Эта функция позволяет предприятиям и поставщикам услуг, обслуживающим несколько доменов, создавать отдельные политики для каждого из них.

Защита от отравления кэша с помощью DNSSEC. Кража ответов — это серьезный класс угроз, связанный с внедрением хакерами поддельных записей на DNS-сервер, что приводит к отравлению его кэша. Эти записи направляют пользователя на контролируемый хакерами сайт, который распространяет вредоносное содержимое или иным образом пытается получить ценную информацию об учетных записях и паролях. NetScaler защищает от угроз данного вида двумя мощными средствами защиты.

- Встроенная поддержка DNSSEC может быть реализована для конфигураций ADNS и DNS-прокси. NetScaler позволяет подписывать ответы, чтобы впоследствии при разрешении имен клиентов можно было проверить достоверность и целостность ответа. Этот подход на основе стандартов предотвращает внедрение поддельных записей в уязвимый DNS-кэш.
- Рандомизация данных о транзакции DNS и информации об исходном порте усложняет внедрение необходимой хакеру информации в запрос и порчу DNS-записей.

Защита от атак на 4 уровне сетевой модели

NetScaler обеспечивает защиту от DoS-атак на сетевом уровне, предотвращая выделение серверных ресурсов до установки подключения к настоящему клиенту и получения действительного запроса.

Например, защита от синхронных атак на основе TCP обеспечивается, во-первых, благодаря выделению ресурсов только после завершения трехстороннего подтверждения связи между клиентом и устройством NetScaler по протоколу TCP, а во-вторых, благодаря производительной и надежной реализации файлов SYN cookies.

Кроме того, аппаратная платформа и архитектура операционной системы позволяет обрабатывать миллионы пакетов SYN в секунду, что гарантирует защиту самого устройства NetScaler от подобных атак.

Другие средства защиты на сетевом уровне включают: (a) списки контроля доступа к 3 и 4 уровню, которые позволяют разрешить трафик для необходимых приложений и блокировать весь остальной трафик; (b) функции ограничения квот, защиты от скачков нагрузки и формирование очереди в порядке приоритета, описанные выше; и (c) высокопроизводительный и соответствующий стандартам стек TCP/IP, который позволяет:

- автоматически блокировать неверно сформированный трафик, который может поставить под угрозу серверные ресурсы;
- предотвращать разглашение информации о подключении и хосте (например, адреса и порты серверов), которая может помочь хакерам осуществить атаку;
- автоматически блокировать множество видов DoS-атак, включая ICMP flood, pipeline, teardrop, land, fraggle, small/zero window и zombie connection.

Три A для доставки приложения

Надежность охвата сети, инфраструктуры и уровня приложений является необходимым, но не достаточным условием для эффективного обеспечения безопасности центра обработки данных. Специалисты по ИТ-безопасности также должны принимать во внимание пользовательский уровень. NetScaler обладает широким набором функций (AAA).

- **A** утентификация для проверки личностей пользователей
- **A** вторизация для проверки и указания ресурсов, к которым может иметь доступ каждый отдельный пользователь
- **A** удит для составления подробного отчета об активности каждого пользователя (например, для устранения неисправностей, составления отчетов и соответствия требованиям регулирующих органов)

Достоинства NetScaler не ограничиваются широким набором функций, например поддержкой изменения паролей и широкого набора механизмов аутентификации (например, локальной, RADIUS, LDAP, TACACS, с помощью сертификатов, NTLM/Kerberos и SAML/SAML2). Что еще более важно, NetScaler централизует и консолидирует эти службы для разных приложений. Вместо реализации и управления этими функциями для каждого приложения в отдельности администраторы могут управлять всеми сразу. К достоинствам такого подхода относятся следующие.

- **Повышенная производительность серверов.** Нагрузка на серверы снижается, а производительность приложений повышается благодаря высвобождению серверных ресурсов, изначально выделенных для выполнения задач AAA.
- **Повышенная безопасность старых версий приложений.** Критически важные функции по обеспечению безопасности могут быть добавлены в приложения, которые не имели функций AAA по умолчанию. Современные приложения также получают пользу от большего набора возможностей (например, возможности обеспечить более надежную аутентификацию или более гибкое журналирование без внесения изменений в приложение).
- **Согласованный уровень комфортности работы пользователя.** Единообразность уровня комфортности работы пользователя достигается благодаря стандартизации механизмов аутентификации, параметров (например, лимитов времени) и политик (например, по обработке неудачных попыток) в наборах приложений.
- **Технология единого входа (SSO).** Пользователям необходимо войти только один раз, так как NetScaler обеспечивает прозрачный доступ ко всем ресурсам на определенном домене.
- **Повышенная безопасность.** Многочисленные возможности по усилению безопасности включают: многофакторные или вторичные механизмы аутентификации, функцию безопасного выхода (например, когда срок действия аутентификационных файлов cookies автоматически истекает) и обеспечение согласованных политик для различных наборов пользователей и/или ресурсов.
- **Упрощение системы безопасности.** Единое (вместо десятков или сотен) место для реализации и управления службами AAA значительно облегчает администрирование и снижает вероятность ошибок, которые приводят к образованию брешей в защите организации.

Формирование системы безопасности с помощью партнерских продуктов NetScaler

Наличие богатой экосистемы партнерских продуктов повышает значимость NetScaler в качестве решения для обеспечения безопасности центров обработки данных. Вот некоторые ключевые примеры.

- **Учет и аналитика.** Технология NetScaler AppFlow, основанная на стандартах, добавляет в информацию на уровне TCP-протокола, уже полученную по протоколу IPFIX (стандарту IETF для протокола NetFlow), данные уровня приложений по каждому потоку. Ненавязчивая технология AppFlow избавляет от необходимости в проприетарных подключениях, программных агентах или дополнительных устройствах благодаря использованию существующей инфраструктуры NetScaler для сбора информации о том, кто использует ресурсы, какие, когда и в какой степени. Splunk — партнер Citrix Ready — собирает данные AppFlow с помощью решения Splunk for NetScaler with AppFlow для анализа и учета таких данных безопасности, как события виртуальной частной сети с SSL-шифрованием и межсетевого экрана, работающего на уровне приложений, нарушения политик и ресурсы, подвергающиеся атаке.
- **Управление информацией о безопасности и событиями (SIEM).** NetScaler App Firewall также поддерживает форматы Common Event Format (CEF) и syslog для экспорта данных для сторонних решений. Одна из наиболее распространенных сфер применения — обработка информации о событиях NetScaler и ведение журнала событий с помощью ведущих платформ SIEM (например, HP ArcSight и RSA enVision) для обеспечения безопасности работы и контроля за соответствием требованиям.
- **Управление уязвимостью.** Решения HailStorm и ClickToSecure от партнера Citrix Ready, компании Cenzic, позволяют провести динамическое тестирование веб-сайтов методом черного ящика для сбора информации об уязвимостях. В данном случае партнерство позволило упростить импорт результатов сканирования Cenzic в NetScaler Application Firewall для настройки правил по защите от угроз, использующих уязвимости, обнаруженные в приложениях и службах.

Вот еще несколько примеров партнеров и их технологий. RSA (адаптивная аутентификация), Qualys (управление уязвимостями), Sourcefire (система предотвращения вторжений и диагностика сети в реальном времени), TrendMicro (антивирус и средства сетевой безопасности) и Venafi (управление ключами/сертификатами). В конечном итоге эти и многие другие доступные партнерские решения позволяют предприятиям построить полную систему безопасности центра обработки данных на основе NetScaler.

Заключение

Постоянная нехватка средств и растущие требования к надежности центров обработки данных породили стремление предприятий к оптимизации затрат. Citrix NetScaler, лучший контроллер доставки приложения для построения корпоративных облачных сетей, идеально подходит в данной ситуации. NetScaler сочетает широкий набор функций по обеспечению безопасности на уровне приложений, сети и пользователей с богатой экосистемой взаимосовместимых партнерских продуктов и позволяет современным предприятиям использовать свою существующую инфраструктуру в качестве надежной и экономически выгодной основы для создания и расширения системы безопасности центров обработки данных следующего поколения.

Представительство Citrix Systems
в России и странах СНГ
Комплекс Москва Сити, Северная башня
Адрес: 123317, г. Москва,
ул.Тестовская д.10,
Тел. +7 495 662 1726
www.citrix.com

Citrix Systems
Citrix Systems, Inc. (NASDAQ:CTXS) – компания, которая в эру «облачных» технологий трансформирует индивидуальную и совместную работу бизнеса и ИТ. Предлагая ведущие на рынке «облачные», сетевые и виртуализационные технологии, Citrix открывает новые возможности в области мобильной работы и предоставления «облачных» услуг, существенно упрощая и делая более доступными сложные ИТ-процессы для более чем 260 000 предприятий. Каждый день Citrix соприкасается с 75% пользователей Internet и работает с более чем 10 000 компаний в 100 странах мира. Годовая выручка в 2012 году составил 2,59 миллиарда долларов США.