

* This Russian version is translated from the English version by Google Translator
* Эта русская версия переведена с английской версии Google Translator.



ZoTrus WAF Шлюз автоматизации

Автоматически внедряйте защиту WAF с помощью шифрования https.

<https://www.zotrus.com>



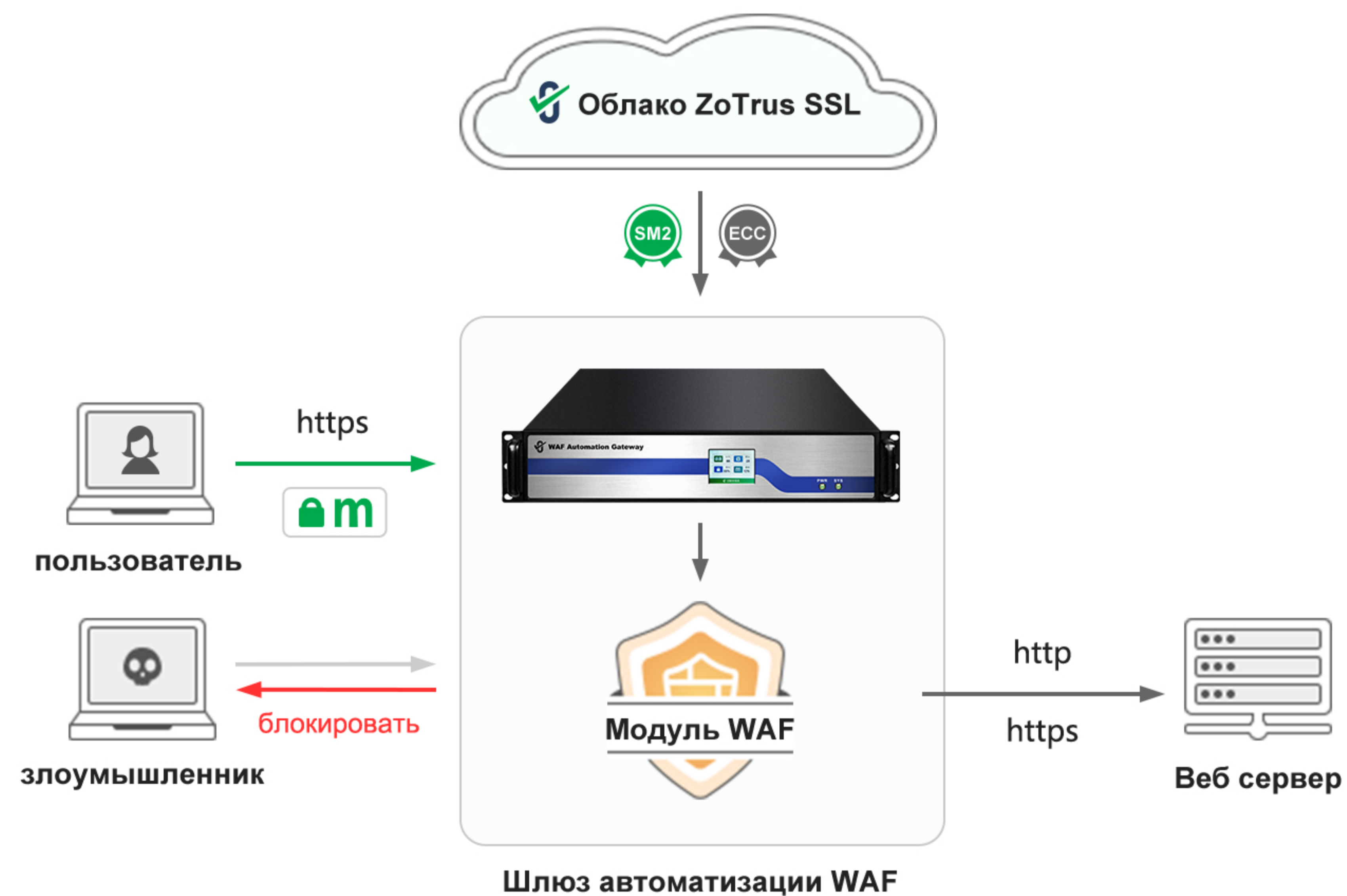
Знакомство с продуктом

ZoTrus WAF Automation Gateway — еще один инновационный продукт, защищающий безопасность веб-сайта на основе SM2 HTTPS Automation Gateway, который прошел сертификацию коммерческого криптографического продукта для повышения функции защиты WAF, что является первым в Китае, и представляет собой новое поколение оборудования WAF, которое объединяет защиту WAF, ускорение шифрования https, разгрузку и пересылку https, модуль алгоритма SM2, автоматизацию сертификата SSL, балансировку нагрузки и другие функции, реализуя при этом высококачественный брандмауэр веб-приложений для защиты безопасности веб-сайта. Он автоматически поддерживает защиту WAF в режиме шифрования HTTPS, поскольку безопасность веб-сайта требует как защиты WAF, так и шифрования HTTPS для обеспечения безопасности передачи конфиденциальных данных на веб-сайте, и именно шифрование HTTPS алгоритма адаптивного шифрования, а алгоритм SM2 является предпочтительным для достижения шифрования HTTPS. ZoTrus WAF Automation Gateway инновационно предоставляет как услуги защиты WAF, так и услуги автоматизации шифрования HTTPS, обеспечивая при этом безопасность шифрования данных «в пути» и «на суше».

ZOTRUS



ZOTRUS

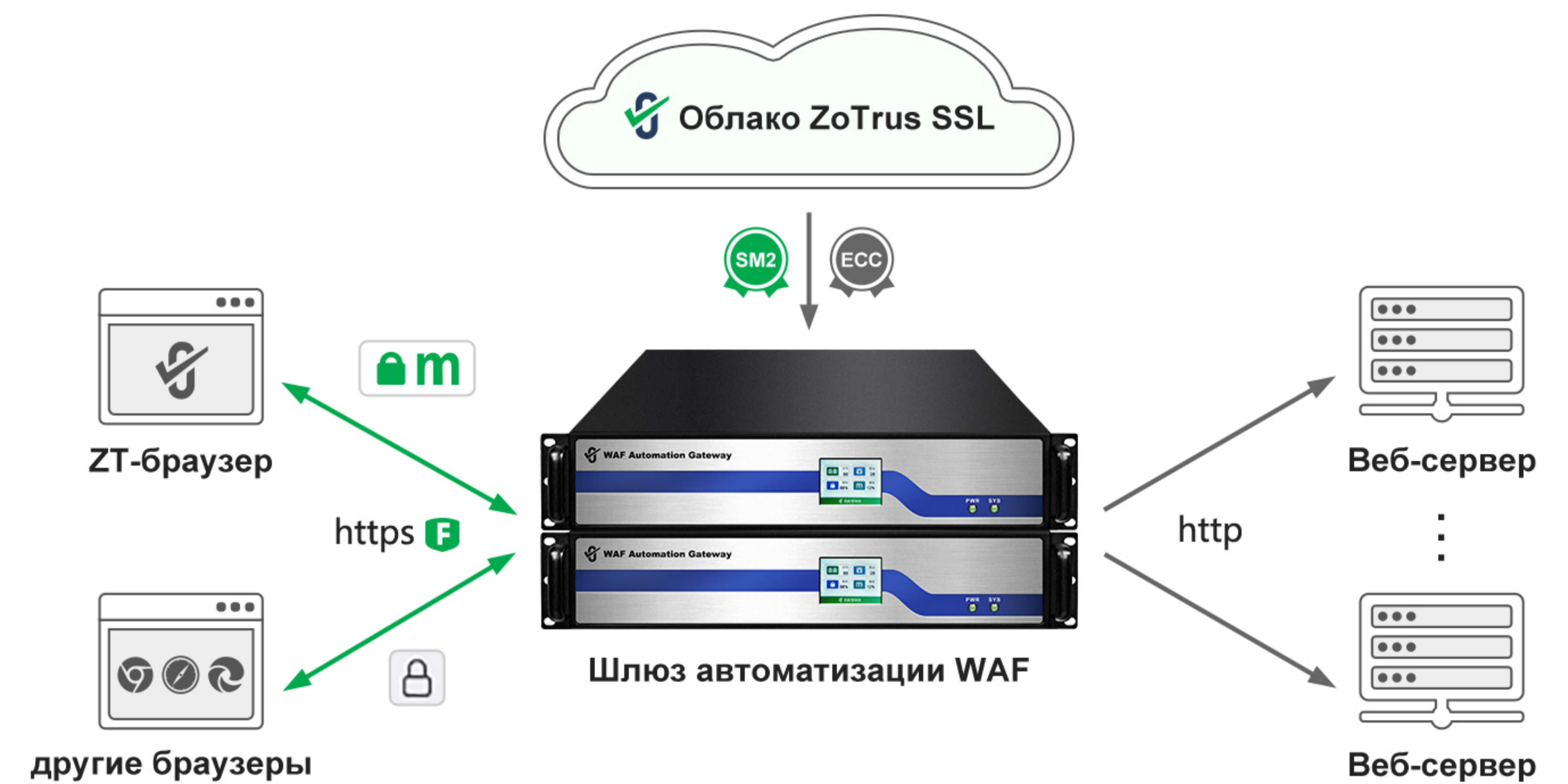


Самые большие возможности и характеристики ZoTrus WAF Automation Gateway — это нулевое применение SSL-сертификатов, нулевая установка SSL-сертификатов, автоматическая реализация защиты WAF с шифрованием HTTPS, адаптивные алгоритмы шифрования. Браузеры, поддерживающие алгоритм SM2 и прозрачность сертификатов SM2, используют алгоритм SM2 для реализации шифрования https, браузеры, не поддерживающие алгоритм SM2, используют алгоритм ECC для реализации шифрования https. Это инновационное решение с интеграцией клиент-облако, WAF Automation Gateway имеет встроенный клиент SM2 ACME, который автоматически подключается к системе ZoTrus Cloud SSL для завершения автоматического применения, развертывания и обновления двойных SSL-сертификатов, гарантируя нулевое изменение бизнес-системы для автоматического достижения шифрования https, для обеспечения защиты WAF с бесперебойной службой шифрования https для бизнес-систем с количеством доменов до 255.

2

Основные функции

Существует три основные функции шлюза автоматизации ZoTrus SM2 WAF: (1) защита WAF; (2) поддержка шифрования SM2 HTTPS; (3) автоматизация шифрования HTTPS. Это не только устройство WAF, но и шлюз автоматизации шифрования HTTPS, нет необходимости подавать заявку на сертификат SSL от CA, автоматически настраивает сертификат SSL с двойным алгоритмом, автоматически реализует защиту WAF с шифрованием HTTPS, и исходный веб-сервер не имеет никаких изменений, просто разверните шлюз автоматизации WAF перед исходным сервером, он может автоматически реализовать защиту WAF с шифрованием https и предоставлять службы защиты WAF и службы автоматизации шифрования https 24 часа в сутки, 365 дней в году. Рекомендуется развернуть развертывание двух машин по умолчанию, которое является горячим резервом друг для друга. Когда оно доступно, два шлюза работают в режиме балансировки нагрузки, а когда оно недоступно, один шлюз может взять на себя всю работу.



Функция защиты WAF шлюза автоматизации ZoTrus WAF разработана и оптимизирована на основе системы ModSecurity с открытым исходным кодом и поддерживает общие функции брандмауэра веб-приложений, такие как: блокировка SQL-инъекций, блокировка межсайтового скриптинга (XSS), предотвращение атак с использованием уязвимостей включения локальных файлов, предотвращение атак с использованием удаленных файлов (включая уязвимости), предотвращение атак с использованием уязвимостей удаленного выполнения команд, блокировка внедрения PHP-кода, блокировка вредоносного доступа, нарушающего протокол HTTP, предотвращение атак с использованием уязвимостей заражения удаленного прокси-сервера, уязвимости Shellshock, попытки атак с использованием неизмененного идентификатора сеанса, сканирование вредоносных веб-сайтов, утечка исходного кода или информации об ошибках, черные спискиhoneypot, блокировка IP-адресов на основе атрибуции IP-адреса и т. д. Поддерживается до 12 различных типов пользовательских правил для достижения персонализированной защиты, например, разрешение IP-адресу доступа к определенному веб-сайту и каталогу веб-сайта.

Сегодня все браузеры отображают HTTP-сайты как «небезопасные», HTTPS-шифрование является обязательной настройкой для обеспечения безопасности веб-сайта, конечно же, это необходимая функция устройства WAF, а нововведением ZoTrus WAF Automation Gateway является автоматическая настройка SSL-сертификата с двойным алгоритмом путем подключения к системе ZoTrus Cloud SSL для подачи заявки на двойной SSL-сертификат, проверки доменного имени, получения выданного SSL-сертификата, установки SSL-сертификата и включения SSL-сертификата.

Автоматически настроенный сертификат ECC SSL пользуется глобальным доверием и поддерживает прозрачность сертификатов, он выдается промежуточным корневым сертификатом бренда ZoTrus - ZoTrus ECC DV SSL CA, его корневой сертификат CA является старейшим в мире корневым сертификатом CA алгоритма ECC - Sectigo ECC, и вся цепочка использует алгоритм ECC, скорость шифрования в 18 раз выше, чем у сертификата SSL алгоритма RSA, что обеспечивает быстрый доступ конечных пользователей к веб-сайту.

Автоматически настроенный сертификат SSL SM2 соответствует закону о криптографии и пользуется доверием всех браузеров SM2. В настоящее время это единственный сертификат SSL SM2 в мире, который поддерживает прозрачность сертификата SM2. Он выдан промежуточным корневым сертификатом бренда ZoTrus - SM2 SSL Pro CA, его корневой сертификат CA - Guizhou SM2 CA, у которого у Guizhou CA есть лицензия CA, выданная MIIT и SCA, вся цепочка использует алгоритм SM2, скорость шифрования в 20 раз выше, чем у алгоритма RSA, для быстрого доступа конечных пользователей к веб-сайту.

Файл цепочки сертификатов автоматически настроенного двойного SSL-сертификата имеет наименьший размер, что экономит трафик IDC и трафик мобильных телефонов пользователей, экономит энергопотребление IDC и энергопотребление мобильных телефонов пользователей, а также является более экологичным.

Десять основных функций и один дополнительный модуль шлюза автоматизации WAF ZoTrus:

01

Высокопроизводительная защита брандмауэра веб-приложений

Основанный на ведущей в отрасли системе с открытым исходным кодом ModSecurity и глубокой оптимизации, он поддерживает широко используемую функцию брандмауэра веб-приложений, обеспечивает очистку веб-трафика после выгрузки зашифрованного трафика https и перенаправляет обычный и защищенный трафик на внутренний веб-сервер.

02

Нулевая реконструкция для https-шифрования

Исходному серверу не нужно устанавливать SSL-сертификат, не нужно устанавливать клиентское программное обеспечение SM2 ACME, не требуется реконструкция для реализации шифрования SM2 https, адаптивный алгоритм шифрования, поддержка алгоритма RSA/ECC/SM2 для реализации шифрования https.

03

Автоматически настраивать SSL-сертификаты

По умолчанию двойные SSL-сертификаты (ECC/SM2) автоматически настраиваются для доменного имени веб-сайта, установленного пользователем бесплатно. Пользователям не нужно подавать заявку на SSL-сертификат от CA, и им не нужно устанавливать и настраивать SSL-сертификат.

04

Высокопроизводительная разгрузка https

Полностью взять на себя функцию шифрования SSL исходного сервера, значительно снизив нагрузку на производительность исходного сервера, позволив использовать исходный сервер для бизнес-системы и значительно повысить скорость отклика клиентского доступа.

05

Мультиплексирование клиентских подключений

Внедрение технологии динамического пула соединений и технологии мультиплексирования для объединения большого количества клиентских запросов на соединение, сохранения большинства серверных TCP-соединений и их непрерывной поддержки, значительного сокращения количества клиентских соединений, которые необходимо обрабатывать исходному серверу (до 90%), а также ускорения обработки соединений и улучшения возможностей обработки бизнес-данных исходного сервера.

Десять основных функций и один дополнительный модуль шлюза автоматизации WAF ZoTrus:

06

07

08

09

10

Сжатие данных при передаче через Интернет

Используйте стандартный алгоритм сжатия GZIP или Deflate для сжатия HTTP-трафика, снижения потребления полосы пропускания и затрат, улучшения отклика сервера и эффективности полосы пропускания, сокращения времени доступа и загрузки конечных пользователей, улучшения пользовательского опыта и повышения удовлетворенности.

Кэш обратного прокси

Используйте кэш-память и структуру хранения пакетов для кратковременного кэширования содержимого веб-сайта, снижения нагрузки на исходный сервер от доступа пользователей, а также повышения производительности обработки исходного сервера и удобства доступа пользователей.

Механизм сохранения сеанса

Механизм сохранения сеанса на основе Cookie и Source IP может выбирать конкретный сервер, к которому подключился пользователь, и осуществлять бесшовную обработку пользовательских запросов. И количество новых подключений может быть сокращено, а системные накладные расходы связанных устройств и серверов могут быть эффективно сокращены.

Многоалгоритмическая балансировка нагрузки

Поддержка семи- и четырехуровневых протоколов для выделения различных ресурсов сервера для пользователей, поддержка нагрузки трафика на основе такой информации, как URI, HOST, COOKIE, USER_AGENT и таких факторов, как IP-адрес, тип приложения и содержимое, а также поддержка преобразования NAT.

Безопасность Аутентификации

Интегрированная функция аутентификации безопасности, поддержка использования двусторонней аутентификации (стандарт SKF) для сертификатов USB-ключа SM2, выданных центрами сертификации Китая, полная поддержка функции двусторонней аутентификации браузера ZT и поддержка клиентского программного сертификата алгоритма SM2/RSA для безопасной аутентификации.

3

Показатели эффективности

ZOTRUS

Шлюз автоматизации ZoTrus WAF представляет собой эффективное, безопасное, прозрачное, простое в развертывании, полностью автоматическое инновационное решение с нулевой реконструкцией для реализации защиты WAF с шифрованием https, которое позволяет эффективно расширить полосу пропускания сетевых устройств и серверов, увеличить пропускную способность и расширить возможности обработки сетевых данных, повысить гибкость и удобство использования сети, а также улучшить пользовательский опыт пользователей, посещающих веб-сайт.

Эффективность защиты WAF шлюза автоматизации ZoTrus WAF была протестирована авторитетным сторонним программным обеспечением для онлайн-тестирования WAFER, а его возможности обнаружения и различения поведения атак соответствуют уровню A (самому высокому уровню) с показателем истинно положительных срабатываний 97,34% и показателем ложных срабатываний 0 (он не будет перехватывать ложные срабатывания, не являющиеся атаками), что может удовлетворить потребности приложений по защите безопасности веб-сайтов.

WAFER Report 2024.05.29

| Type | Total Requests | Detected | Error | % |
|-----------------|----------------|----------|-------|--------|
| True Positives | 413 | 402 | 0 | 97.34% |
| False Positives | 72 | 0 | 0 | 0% |

Performance Scores

| | |
|-------------------------------|------------------------------------|
| Detection Ability A | Distinguishing Ability A |
|-------------------------------|------------------------------------|

Фактический результат теста на эффективность защиты показывает, что SQL-инъекция запустила в общей сложности 128 атак и заблокировала 126 раз. Также было 2 ложных отрицательных результата, то есть пропущенных блоков, с показателем истинно положительных результатов 98,44%. Для межсайтового скриптинга было запущено в общей сложности 149 атак и заблокировано 147. Также было 2 ложных отрицательных результата, то есть пропущенных блоков, а показатель истинно положительных результатов составил 98,66%. Для атак Command Injection было запущено в общей сложности 41 атака и заблокировано 37. Также было 4 ложных отрицательных результата, то есть пропущенных блоков, с показателем истинно положительных результатов 90,24%. Для SSI-инъекции было запущено в общей сложности 24 атаки и заблокировано 24. Ложных отрицательных результатов нет, а показатель истинно положительных результатов составляет 100%. Другие результаты тестов не анализируются по отдельности. Для атак, которые не блокируются, модуль Gateway WAF должен постоянно совершенствоваться в правилах защиты WAF, а правила должны регулярно обновляться. Конечно, клиент также должен уделять внимание анализу журналов WAF и постоянно настраивать правила защиты на основе атак.

| Attack Type | Total | True Positives | False Negatives | True Positive Rate |
|-----------------------------|-------|----------------|-----------------|--------------------|
| SQL Injection | 128 | 126 | 2 | 98.44% |
| Cross Site Scripting | 149 | 147 | 2 | 98.66% |
| Command Injection | 41 | 37 | 4 | 90.24% |
| SSI Injection | 24 | 24 | 0 | 100% |
| File Upload | 29 | 29 | 0 | 100% |
| Directory Traversal | 20 | 17 | 3 | 85% |
| Buffer Overflow | 10 | 10 | 0 | 100% |
| LFI (Local File Inclusion) | 10 | 10 | 0 | 100% |
| RFI (Remote File Inclusion) | 2 | 2 | 0 | 100% |

Шлюз автоматизации ZoTrus WAF предоставляет полностью независимые и управляемые программные и аппаратные интеграционные продукты, включая систему WAF с открытым исходным кодом, программную систему шлюза безопасности SSL с полностью независимыми правами интеллектуальной собственности, криптографическую карту аппаратного ускорителя алгоритма SM2/ECC/RSA, сертифицированную CCPC, самоуправляемую операционную систему, поддерживает чипы ЦП, такие как Haiguang, Loongson и Phytium, использует поддержку независимых материнских плат, поддерживает независимые сетевые карты и т. д. Полностью автономный и управляемый программный и аппаратный интегрированный шлюз автоматизации WAF может удовлетворить требования приложений этих отраслей, которые предъявляют чрезвычайно высокие требования к контролю информационной безопасности.

Каждый шлюз автоматизации ZoTrus WAF поддерживает автоматическую настройку до 255 сертификатов ECC SSL (один сертификат) и поддерживает до 255 пар сертификатов SM2 SSL (один сертификат подписи и один сертификат шифрования), конфигурация сертификатов с двойным алгоритмом поддерживает до 255 доменных имен веб-сайтов для достижения защиты WAF с адаптивным шифрованием https с двойным алгоритмом. Количество веб-сайтов, которые могут поддерживать шифрование https, ограничено количеством новых подключений, пропускной способностью и параллелизмом, поддерживаемыми оборудованием шлюза и картами шифрования.

Каждый шлюз автоматизации ZoTrus WAF имеет гарантийный срок 5 лет и автоматически настраивает всемирно доверенный сертификат ECC DV SSL и сертификат соответствия криптографии SM2 DV SSL не более чем для 255 доменных имен веб-сайтов в течение 5 лет. Исходя из расчета 988 юаней в год за двойной алгоритм и двойной сертификат SSL каждого веб-сайта, стоимость автоматически настроенного сертификата SSL составляет 1,25 миллиона юаней ($=5 \times 255 \times 988$, что эквивалентно 172 тыс. долларов США), а также эксклюзивную в мире сверхценную защиту WAF с решением автоматизации шифрования https!

ZoTrus WAF Automation Gateway в настоящее время предоставляет 4 продукта с различными спецификациями, которые могут использоваться для облачных высокопроизводительных центров обработки данных, серверов крупных и средних предприятий и серверов малых организаций для автоматической реализации защиты WAF с шифрованием https, особенно требований приложений нулевой реконструкции для реализации защиты WAF с шифрованием https. Параметры индекса производительности продукта различных моделей показаны в таблице ниже. Для пользователей с различными требованиями к индексу продукты могут быть настроены в соответствии с требованиями.



| Модель | MG-2-1 | MG-2-8 | MG-2-9 |
|--|---------------------------------|--|--|
| Процессор | Intel Atom | Intel Xeon (dual) | Hygon 5380 |
| Производительность WAF | Уровень A | Уровень A | Уровень A |
| Настроить правило WAF | Да | Да | Да |
| Правило регулярного обновления | Да | Да | Да |
| Включая ECC SSL Кол-во | 20 | 100 / 255 | 100 / 255 |
| Включая SM2 SSL Кол-во | 20 | 100 / 255 | 100 / 255 |
| Двойная поставка SSL | 5 лет | 5 лет | 5 лет |
| Тип SSL ECC | DV SSL | DV SSL | DV SSL |
| Тип SSL SM2 | OV SSL | OV SSL | OV SSL |
| Уникальный ключ/сертификат для каждого веб-сайта | Да | Да | Да |
| Период действия SSL-сертификата | 90 дней | 90 дней | 90 дней |
| Цикл обновления сертификата | Каждые 80 дней | Каждые 80 дней | Каждые 80 дней |
| Тип WTIV | ЭМ | ЭМ | ЭМ |
| Пропускная способность SM2 https | 800 Mbps | 9 Gbps | 9 Gbps |
| Пропускная способность ECC https | 800 Mbps | 9 Gbps | 9 Gbps |
| Запрос SSL SM2 | 30 K/S | 120 K/s | 60 K/s |
| Запрос ECC SSL | 40 K/S | 130 K/s | 90 K/s |
| Макс. одновременный | 250K | 1.5M | 1M |
| Сетевой интерфейс | 6xG | 6xG + 4x10G | 6xG + 4x10G |
| Размер шасси | 155*240*40 (мм) | 2U | 2U |
| Власть | Одиарный источник питания 60 Вт | Двойной блок питания 550 Вт | Двойной блок питания 550 Вт |
| Стоимость сертификата (5 лет) | 490K RMB | 2.44M / 6.23M RMB | 2.44M / 6.23M RMB |
| Сохранить значение HR (5 лет) | 120K RMB | 600K / 1.5M RMB | 600K / 1.5M RMB |
| Подходящая область применения | МСП, колледжи и университеты | Крупное корпоративное публичное облако E-gov Cloud | Крупные предприятия , правительственные / финансовые E-gov Cloud |

ZOTRUS

4

Решения по развертыванию

<https://www.zotrus.com>

ZoTrus WAF Automation Gateway поддерживает несколько методов сетевого развертывания, поддерживает кластерное развертывание нескольких устройств, поддерживает автоматическую стыковку с ZoTrus Cloud SSL System для автоматической настройки двойных SSL-сертификатов, необходимых для шифрования https для Gateway, а также поддерживает локализованное развертывание ZoTrus Cloud SSL System для облака электронного правительства или публичного облака, которое автоматически выдает двойные SSL-сертификаты для локальных пользователей облака, а локальное устройство WAF Automation Gateway автоматически подключается к локально развернутой Cloud SSL System. Чтобы обеспечить высокую доступность Gateway, настоятельно рекомендуется развертывание на двух машинах для обеспечения бесперебойного предоставления защиты WAF и служб шифрования https 24*365.



1. Предоставление услуги автоматизации шифрования HTTPS для локальных веб-серверов (веб-сайтов)



Чтобы обеспечить защиту WAF, пользователь должен развернуть устройство WAF перед веб-сервером, а устройство WAF может защищать трафик HTTP/HTTPS и пересылать обычный открытый текстовый трафик и расшифрованный открытый текстовый трафик на последующий веб-сервер. Однако, если пользователь покупает традиционное устройство WAF, ему необходимо подать заявку на сертификат SSL от CA и вручную развернуть его на устройстве WAF, что очень долго и трудоемко. С ZoTrus WAF Automation Gateway пользователю не нужно подавать заявку на сертификат SSL от CA, а ZoTrus WAF Automation Gateway автоматически подключается к системе сервиса ZoTrus Cloud SSL для автоматической настройки двойных сертификатов SSL для веб-сайта пользователя и автоматически реализует зашифрованную HTTPS защиту WAF.

Один сетевой порт шлюза автоматизации ZoTrus WAF подключен к исходному публичному сетевому интерфейсу, и настроен публичный IP-адрес исходного веб-сервера, а исходный веб-сервер подключен к другим портам, и по умолчанию может быть подключено максимум 8 веб-серверов, и эти веб-серверы настроены с частными IP-адресами. Весь сетевой трафик данных ускоряется, выгружается и передается через шлюз, а пакеты данных, которые соответствуют протоколу приложения безопасности политикой WAF, будут пересылаться на соответствующий внутренний веб-сервер в соответствии с политикой балансировки нагрузки, поддерживающей пересылку открытого текста HTTP и зашифрованную пересылку HTTPS.

Этот метод развертывания превращает исходный веб-сервер, открытый в Интернете, в сервер интрасети, защищает безопасность веб-сервера и переносит все рабочие нагрузки HTTPS-шифрования и дешифрования, за которые отвечает исходный веб-сервер, на шлюз, что позволяет сэкономить 20–30 % вычислительной мощности веб-сервера, благодаря чему веб-сервер может лучше обеспечивать вычислительную мощность для бизнес-системы.

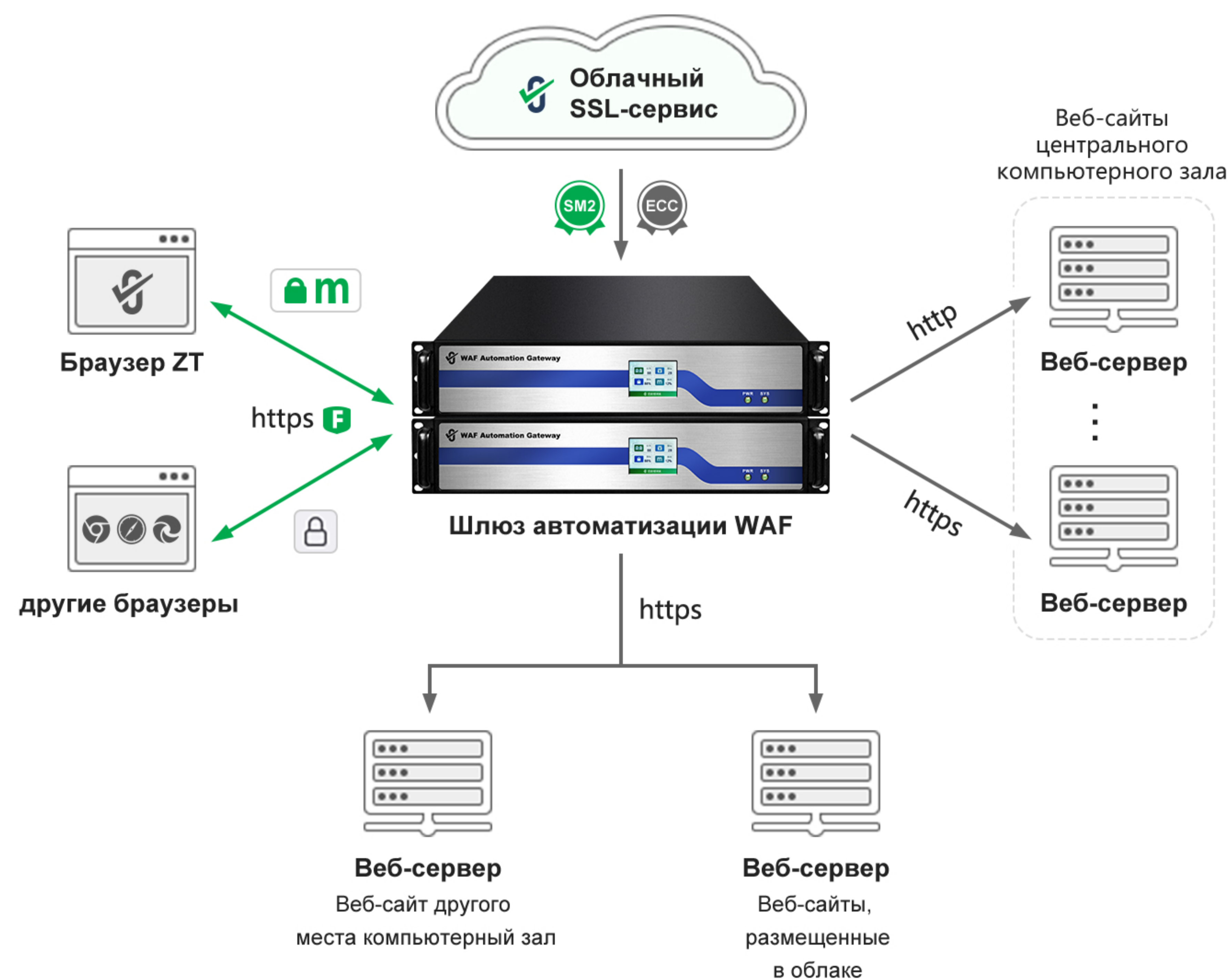
Этот метод развертывания подходит для пользователей, у которых есть собственный компьютерный зал и собственный веб-сервер, и которым необходимо добавить шлюзовое устройство в компьютерный зал, которое изменит IP-адрес исходного веб-сервера, переназначит частный IP-адрес исходному веб-серверу, настроит исходный публичный IP-адрес для шлюза, при этом шлюз поддерживает IP V4 и IP V6, и исходное разрешение доменного имени не нужно менять, а веб-серверу не нужно поддерживать IP V6.

Режим развертывания по умолчанию — это режим горячего резервирования двух шлюзов, и два шлюза находятся в активно-активном режиме, в котором оба шлюза действуют как хосты и обрабатывают трафик услуг одновременно, а также являются резервными серверами друг для друга. Два шлюза разделяют трафик услуг и не тратят ресурсы впустую. Когда один из шлюзов имеет проблему и не может продолжать работу, другой шлюз берет на себя всю работу, чтобы обеспечить непрерывную и надежную работу бизнес-системы. Гарантия на шлюз составляет 5 лет, и если в течение 5 лет произойдет сбой, шлюз будет заменен бесплатно, чтобы обеспечить бесперебойную защиту WAF и автоматизацию шифрования HTTPS в течение 5 лет.

ZOTRUS



2. Предоставление услуги автоматизации шифрования HTTPS для веб-серверов (веб-сайтов), которые не являются локальными



Для пользователей, которым необходимо не только реализовать защиту WAF и службы автоматизации шифрования HTTPS на локальных серверах, но и иметь веб-серверы в филиалах или несколько веб-сайтов, развернутых в облаке, которым также нужна защита WAF и служба автоматизации HTTPS, ZoTrus WAF Gateway поддерживает как режим локальной пересылки, так и удаленный режим возврата к источнику. Независимо от того, находится ли веб-сервер (веб-сайт) в чужой компьютерной комнате или на облачном хосте, пока шлюз может получить к нему доступ через публичную сеть или интранет, эти веб-сайты являются серверами возврата к источнику, аналогичными службам CDN, и шлюз может предоставлять защиту WAF и службы автоматизации шифрования HTTPS для всех них. Двойные шлюзы предоставляют защиту WAF и службы автоматизации шифрования HTTPS для 255 веб-сайтов, и большему количеству веб-сайтов необходимо приобретать больше шлюзов.

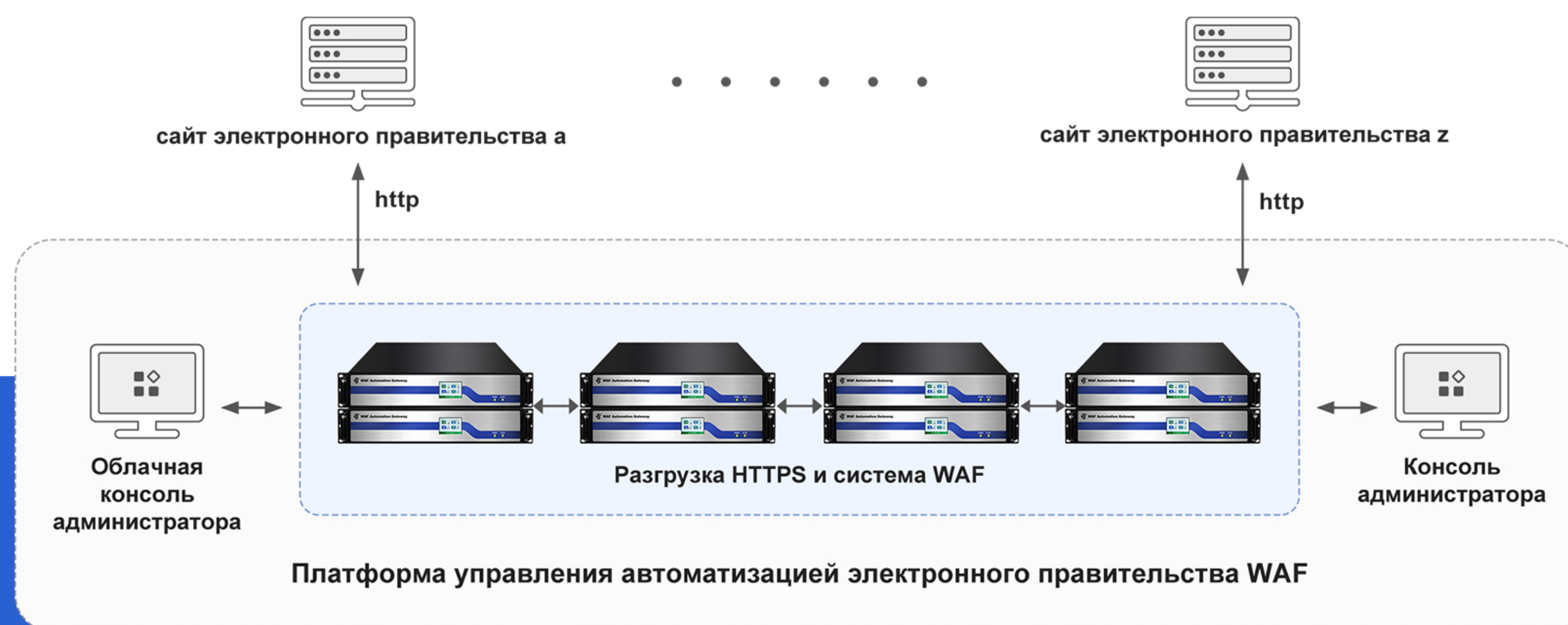
Чтобы обеспечить безопасность данных системы веб-сайта, которая не находится в центральном компьютерном зале, соединение back-to-origin от шлюза к другому серверу местоположения должно быть зашифровано с помощью HTTPS для достижения полного шифрования ссылки. ZoTrus Technology предоставляет самоподписанный сертификат back-to-origin SSL со сроком действия 5 лет для веб-сайтов back-to-origin бесплатно, а исходному веб-сайту не нужно разворачивать глобально доверенный сертификат SSL со сроком действия всего один год.

Этот метод развертывания также подходит для поставщиков услуг, которые предоставляют услуги по разработке веб-сайтов, веб-хостингу и продаже SSL-сертификатов, а также разворачивают несколько шлюзов для предоставления услуг по защите WAF и автоматизации шифрования HTTPS для своих собственных бизнес-систем, а также услуг по защите WAF и автоматизации шифрования HTTPS для своих клиентов, независимо от того, где размещен веб-сайт клиента, необходимо только, чтобы он был доступен по протоколу HTTP или HTTPS.

3. Решение для автоматического развертывания кластера управления облачной платформой WAF

Для различных облачных платформ, таких как облачные платформы электронного правительства и публичные облачные платформы, существуют десятки тысяч или даже миллионы веб-сайтов, которым нужна защита WAF и шифрование HTTPS, и единственное решение может быть сделано только путем автоматизации. Необходимо развернуть несколько шлюзов автоматизации WAF для формирования кластерного массива - HTTPS Offloading и WAF System, и несколько шлюзов автоматизации WAF работают вместе, чтобы делиться бизнес-трафиком и служить шлюзами горячего резерва друг для друга. Когда шлюз выходит из строя, службы, работающие на нем, будут взяты на себя другими шлюзами, чтобы обеспечить адекватный и своевременный ответ на планирование услуг. Режим кластера подходит для развертывания избыточных сетевых сред с упором на чрезвычайно высокую пропускную способность.

В отличие от других традиционных решений по развертыванию устройств WAF, инновация заключается в том, что оно автоматически настраивает SSL-сертификаты с двойным алгоритмом, автоматически реализует шифрование HTTPS и разгрузку, а также защиту WAF, и не требует ручной подачи заявки и ручного развертывания SSL-сертификатов с двойным алгоритмом из CA после покупки устройств WAF на облачной платформе и ежегодного обновления приложения и развертывания. Это решение включает 5 лет автоматического применения и развертывания SSL-сертификатов с двойным алгоритмом и 5 лет автоматической защиты WAF с шифрованием HTTPS, что соответствует требованиям соответствия коммерческой криптографии облачной платформы и всемирно доверенным приложениям для защиты веб-сайтов HTTPS.

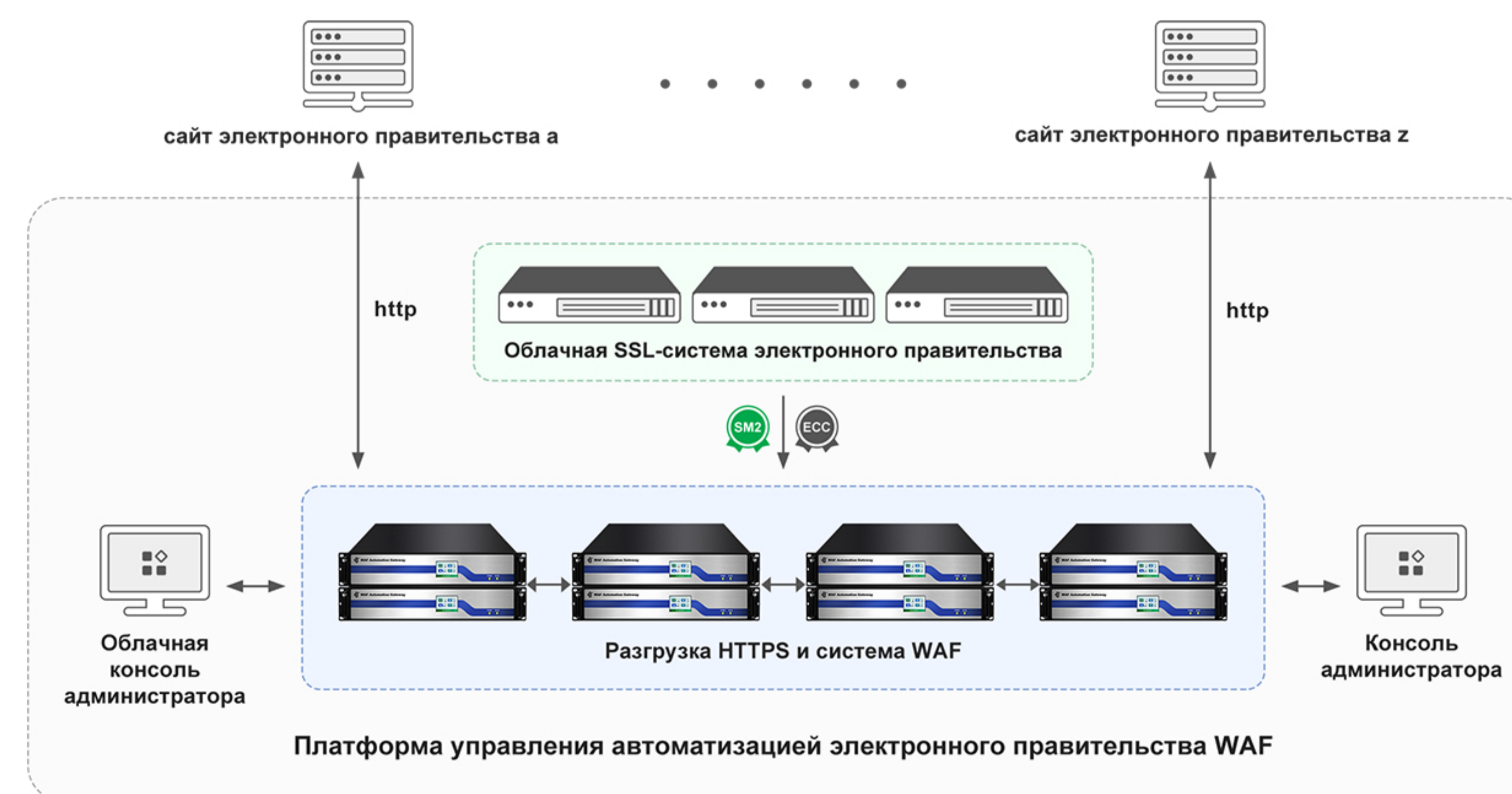


4. Локальное развертывание облачной SSL-системы

По умолчанию ZoTrus WAF Automation Gateway автоматически подключается к ZoTrus Cloud SSL System для включения шифрования https после получения двойных SSL-сертификатов. Для клиентов облачной платформы, которые хотят самостоятельно выпускать собственные бренды двойных SSL-сертификатов, которые автоматически развертываются на шлюзе, они могут развернуть ZoTrus Cloud SSL System локально для реализации автоматической выдачи двойных SSL-сертификатов с помощью выделенного промежуточного корневого сертификата SSL с индивидуальным брендом. Локально развернутая система называется E-government Cloud SSL System или Public Cloud SSL System.

Система SSL-сертификатов электронного правительства Cloud представляет собой локально развернутую систему CA для выпуска SSL-сертификатов, совместимых с криптографией и поддерживающих прозрачность сертификатов SM2. Развертывание всей системы заключается в реализации полностью независимой и контролируемой выдачи и управления SSL-сертификатами SM2 для веб-сайта электронного правительства и относительно независимой выдачи SSL-сертификатов ECC. Для достижения независимой и контролируемой выдачи SSL-сертификатов электронного правительства, прежде всего, должен быть промежуточный корневой сертификат для выдачи SSL-сертификатов, чтобы все системы электронного правительства могли надежно осознавать, что все системы электронного правительства доверяют только SSL-сертификатам, выданным их собственными промежуточными корневыми сертификатами, эффективно предотвращая различные атаки SSL типа «человек посередине» на веб-сайты электронного правительства и другие атаки на поддельные веб-сайты электронного правительства.

ZOTRUS





Резюме



Связаться с нами: +86-755-2660 4080
Электронная почта: help@zotrus.com

ZoTrus WAF Automation Gateway — эксклюзивная глобальная инновация, позволяющая добиться нулевых изменений исходного сервера для реализации защиты WAF и автоматизации шифрования https, адаптивного шифрования https с двойным алгоритмом SM2/ECC, просто настройте доменное имя веб-сайта и IP-адрес при запуске, немедленно включите защиту WAF, службу шифрования и ускорения https, безопасную доставку TCP/DTLS, автоматическую подготовку двойных сертификатов SSL, соответствие глобальному доверию и криптографии, высокоскоростное динамическое кэширование и сжатие, мультиплексирование соединений, сохранение сеансов и балансировку нагрузки и т. д. Гарантируя высокую производительность, он обеспечивает самое высокое в отрасли соотношение производительности и цены.

Шлюз автоматизации ZoTrus WAF — это plug-and-play, развернутый на передней стороне сервера веб-сайта, не только обеспечивающий защиту WAF, но и исходный сервер веб-сайта может быть легко обновлен с http на https без каких-либо изменений, и именно шифрование SM2 https соответствует требованиям криптографии, а шифрование ECC https совместимо со всеми браузерами, которые не поддерживают алгоритм SM2. Его мощная способность ускорения и разгрузки https обеспечивает мощную поддержку модуля WAF, а функция пересылки после защиты WAF обеспечивает дополнительную поддержку повышения производительности для сервера веб-сайта, не только не увеличивает нагрузку на шифрование и дешифрование https, но и улучшает возможности внешнего реагирования и способность обрабатывать запросы пользователей. Плавное переключение нулевой реконструкции, нулевого обслуживания и нулевого воздействия шлюза автоматизации ZoTrus WAF является первым выбором и обязательным для защиты WAF, автоматизации шифрования SM2 https и обновления безопасности системы с http на https.