

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



ZoTrus HTTPS Шлюз автоматизации

Автоматическое управление сертификатами SSL для реализации шифрования https

<https://www.zotrus.com>

1

Знакомство с продуктом

ZoTrus HTTPS Automation Gateway (Аббревиатура.: ZoTrus Gateway) - это высокопроизводительное аппаратное шлюзовое устройство для обеспечения безопасности веб-сайтов, созданное по технологии ZoTrus с использованием высокопроизводительных шифровальных карт, прошедших сертификацию продукта SSL VPN / Security Gateway class Security Level 2 в Китае для коммерческой криптографии. Это аппаратный шлюз, включающий ускорение шифрования https, разгрузку и переадресацию https, модуль алгоритма SM2, автоматическое управление сертификатами SSL и балансировку нагрузки, он предназначен для ускорения и разгрузки https с множеством функций в одной встроенной высокопроизводительной аппаратной шифровальной плате профессионального уровня для обеспечения высокоскоростного шифрования операции и переадресацию сетевых пакетов, а также профессионально оптимизировал встроенную операционную систему, сетевой протокол, протокол SSL/TLS, алгоритм ECC и алгоритм SM2 для достижения ведущих в отрасли экстремальных показателей производительности, таких как: Скорость новых подключений по протоколу HTTPS может достигать 60 000 раз в секунду, пропускная способность по протоколу HTTPS может достигать 17 Гбит/с, а количество одновременных подключений по протоколу HTTPS может достигать 3 миллионов подключений.



ZOTRUS

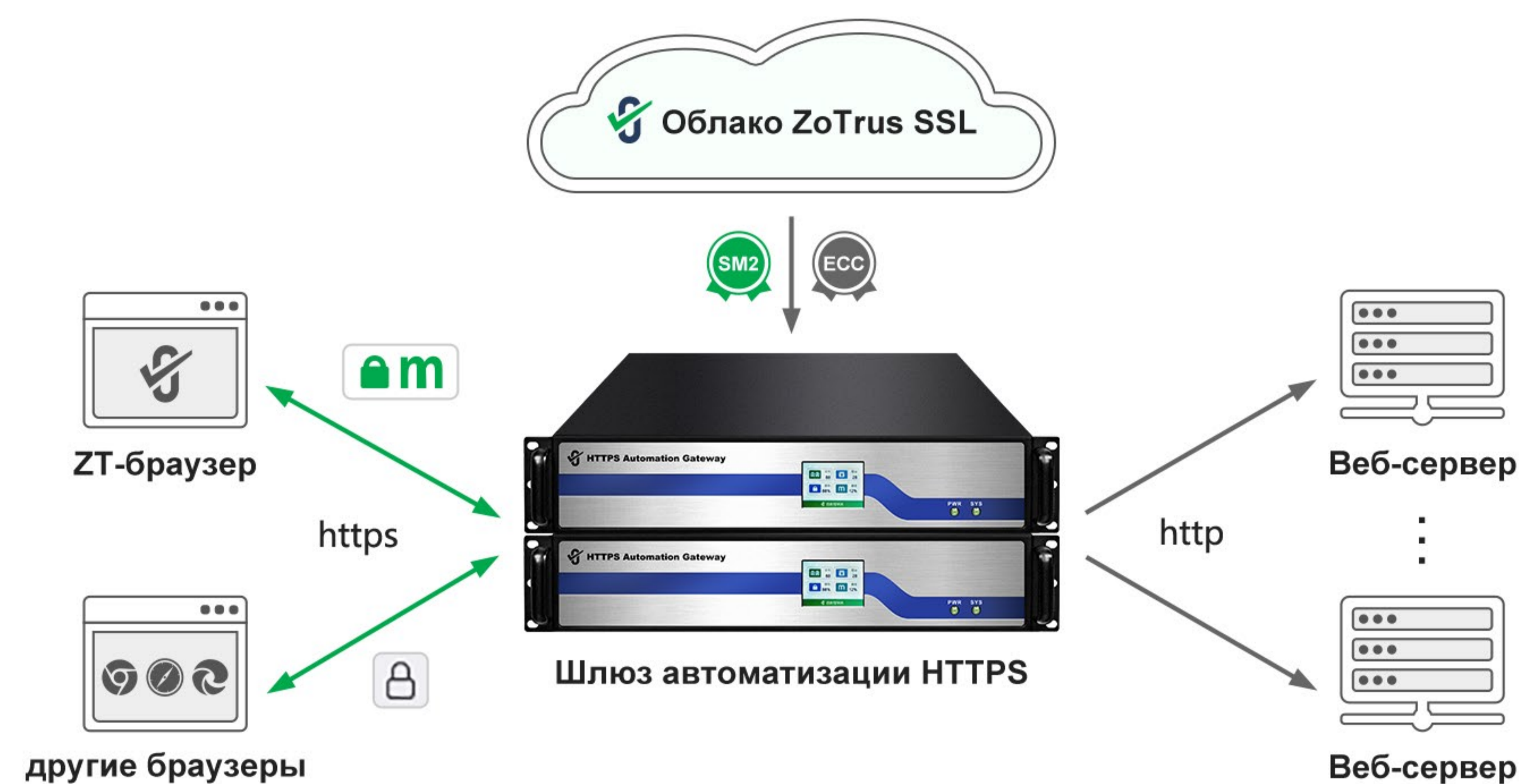


Самыми важными функциями и характеристиками шлюза автоматизации HTTPS ZoTrus являются отсутствие применения сертификатов SSL, отсутствие установки сертификатов SSL, автоматическая реализация шифрования HTTPS, адаптивные алгоритмы шифрования. Браузеры, поддерживающие алгоритм SM2 и прозрачность сертификата 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 клиента и облака. Шлюз автоматизации SM2 HTTPS имеет встроенный клиент SM2 ACME, который автоматически подключается к облачной системе SSL ZoTrus для выполнения автоматического применения, развертывания и обновления двойных сертификатов SSL, гарантируя нулевое изменение бизнес-системы для автоматического достижения шифрования https, бесперебойного предоставления службы шифрования https и службы защиты WAF для бизнес-систем с до 255 различными доменными именами.

2

Основные функции

Основная функция шлюза автоматизации HTTPS ZoTrus — отсутствие реконструкции исходного веб-сервера, отсутствие необходимости установки SSL-сертификата на веб-сервере, отсутствие необходимости установки программного обеспечения клиента ACME на веб-сервер и отсутствие необходимости обновления веб-сервера. серверное программное обеспечение для поддержки алгоритма SM2, просто разверните шлюз автоматизации HTTPS перед исходным сервером, после чего он сможет автоматически внедрять шифрование https и предоставлять услуги шифрования https и службу защиты WAF 24 часа 365 дней. Рекомендуется использовать развертывание двух компьютеров по умолчанию в качестве горячего резерва друг для друга. Когда он доступен, два шлюза работают в режиме балансировки нагрузки, а когда он недоступен, всю работу может взять на себя один шлюз. Бесплатный браузер SM2, поддерживающий алгоритм SM2 и прозрачность сертификата SM2. ZT Browser использует алгоритм SM2 для реализации шифрования https SM2 преимущественно, а другие браузеры, которые не поддерживают алгоритм SM2 и прозрачность сертификата SM2, используют алгоритм ECC для реализации шифрования https.



Сегодня все браузеры отображают веб-сайт HTTP как «Небезопасный», а шифрование HTTPS является обязательным условием безопасности веб-сайта. Сертификат с двойным алгоритмом и двойным SSL, необходимый для шифрования HTTPS, автоматически заполняется шлюзом автоматизации HTTPS, подключенным к облачной системе SSL ZoTrus, для подачи заявки на сертификат с двойным SSL, проверки доменного имени, получения выданного сертификата SSL, установки SSL. сертификат и включите сертификат SSL. Автоматически настроенный SSL-сертификат ECC пользуется глобальным доверием и поддерживает прозрачность сертификата. Он выдается промежуточным корневым сертификатом бренда ZoTrus — ZoTrus ECC DV SSL CA, его корневым сертификатом CA является старейший в мире корневой сертификат CA алгоритма ECC — Sectigo ECC, а также Вся цепочка использует алгоритм ECC, скорость шифрования в 18 раз выше, чем у SSL-сертификата алгоритма RSA, для быстрого доступа к веб-сайту конечными пользователями. Автоматически настроенный SSL-сертификат SM2 OV соответствует Закону о криптографии и ему доверяют все браузеры SM2. В настоящее время это единственный SSL-сертификат 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, который Guizhou CA имеет лицензию CA, выданную MIIT и SCA, вся цепочка использует алгоритм SM2, скорость шифрования - 20 раз. быстрее, чем алгоритм RSA, для быстрого доступа к веб-сайту конечным пользователям.

Срок действия двойных сертификатов SSL, автоматически настроенных шлюзом автоматизации HTTPS ZoTrus, составляет 90 дней, что заранее соответствует предстоящей политике 90-дневного сертификата. На следующем рисунке слева показан 90-дневный SSL-сертификат SM2 OV, настроенный шлюзом по умолчанию, а также SSL-сертификат ECC DV с 90-дневным сроком действия, настроенный шлюзом справа, а также автоматическое развертывание 90-дневного сертификата SSL. Сертификат -day значительно повысит безопасность и гибкость службы шифрования HTTPS. Двойные сертификаты SSL основаны на алгоритме эллиптической кривой, файл цепочки сертификатов является самым маленьким, что экономит трафик IDC и трафик мобильного телефона пользователя, экономит энергопотребление IDC и мощность мобильного телефона пользователя. , это более экологично.

Field	Value
Signature algorithm	SM3WithSM2
Signature hash algorithm	SM3
Issuer	SM2 SSL Pro CA, CN
Valid from	Monday, July 8, 2024 8:06:52 AM
Valid to	Monday, October 7, 2024 8:06:52 AM
Subject	cersign.cn,CerSign Technolog...
Public key	ECC (256 Bits)
Public key parameters	SM2

CN = cersign.cn
 O = CerSign Technology Limited
 L = Shenzhen
 S = Guangdong
 C = CN

Field	Value
Signature algorithm	sha256ECDSA
Signature hash algorithm	sha256
Issuer	ZoTrus ECC DV SSL CA, ZoTrus Tec...
Valid from	Monday, July 8, 2024 8:00:00 AM
Valid to	Monday, October 7, 2024 7:59:59 AM
Subject	cersign.cn
Public key	ECC (256 Bits)
Public key parameters	ECDSA P256

CN = cersign.cn

Шлюз автоматизации HTTPS ZoTrus по умолчанию имеет встроенный модуль WAF. Этот модуль разработан на основе системы ModSecurity с открытым исходным кодом, которая поддерживает часто используемые функции брандмауэра веб-приложений, такие как: предотвращение SQL-инъекций, предотвращение атак с использованием межсайтовых сценариев (XSS), предотвращение атак с использованием локальных файлов, содержащих уязвимости, и предотвращение использования удаленных файловых (включая уязвимости) атак, предотвращение атак с использованием уязвимостей удаленного выполнения команд, предотвращение внедрения PHP-кода, предотвращение злонамеренного доступа, нарушающего протокол HTTP, предотвращение атак с использованием удаленного выполнения команд. Уязвимости с тем же идентификатором можно использовать для атак, предотвращения вредоносного сканирования веб-сайтов, предотвращения утечки исходного кода или информации об ошибках, внесения в черный список проектов-приманок и блокировки IP-адресов на основе оценки присвоения IP-адреса и т. д. Если клиент уже приобрел устройство WAF, необходимо только развернуть шлюз автоматизации HTTPS SM2 перед устройством WAF. Устройство WAF должно отвечать только за анализ HTTP-контента в открытом виде для обеспечения соответствующей защиты, и нет необходимости подавать заявку на сертификат SSL от центра сертификации для развертывания на устройстве WAF.

Шлюз автоматизации HTTPS ZoTrus также является шлюзом аутентификации безопасности, который поддерживает сертификат USB-ключа SM2, выданный центром сертификации Китая для использования двусторонней аутентификации (стандарт SKF), с функцией поддержки двусторонней аутентификации браузера ZT, пользователям не требуется Любая дополнительная разработка, просто включите двустороннюю аутентификацию при настройке службы автоматизации SM2 HTTPS на шлюзе, пользователи могут установить несколько центров сертификации для выдачи клиентских сертификатов, а сертификат корневого центра сертификации China Public SM2 установлен по умолчанию. Он поддерживает двустороннюю аутентификацию мягкого сертификата алгоритма RSA и жесткого сертификата USB-ключа.

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

01

Нулевая реконструкция для шифрования https

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

02

Автоматическая настройка SSL-сертификатов

По умолчанию двойные сертификаты SSL (ECC/SM2) автоматически настраиваются для доменного имени веб-сайта, бесплатно установленного пользователем. Пользователям не нужно подавать заявку на получение SSL-сертификата в центре сертификации, а также не нужно устанавливать и настраивать SSL-сертификат.

03

Высокопроизводительная https-разгрузка

Полностью возьмите на себя функцию SSL-шифрования исходного сервера, что значительно снизит нагрузку на производительность исходного сервера, позволит выделить исходный сервер для бизнес-системы и значительно улучшит скорость ответа клиента.

04

Мультиплексирование клиентских соединений

Внедрить технологию динамического пула соединений и технологию мультиплексирования для объединения большого количества запросов на подключение клиентов, сохранить большинство TCP-соединений сервера и поддерживать их непрерывно, значительно сократить количество клиентских подключений, которые необходимо обрабатывать исходному серверу (до 90%), и ускорить скорость обработки соединения и улучшить возможности бизнес-обработки исходного сервера.

05

Сжатие передачи веб-данных

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

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

ZOTRUS

06

Обратный прокси-кеш

Используйте кеш-память и структуру хранения пакетов для кэширования содержимого веб-сайта на короткое время, уменьшите нагрузку на исходный сервер из-за доступа пользователя, а также улучшите вычислительную мощность исходного сервера и удобство доступа пользователя.

07

Механизм сохранения сеанса

Механизм сохранения сеанса, основанный на файлах cookie и IP-адресе источника, может выбирать конкретный сервер, к которому подключился пользователь, и обеспечивает плавную обработку пользовательских запросов. Можно сократить количество новых подключений и эффективно снизить нагрузку на систему связанных устройств и серверов.

08

Многоалгоритмная балансировка нагрузки

Поддержка семиуровневых и четырехуровневых протоколов для распределения 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.

09

Модуль брандмауэра веб-приложений (ZoTrus Gateway WAF)

Основанный на ведущей в отрасли разработке системы ModSecurity с открытым исходным кодом и глубокой оптимизации, он поддерживает часто используемую функцию брандмауэра веб-приложений, обеспечивает защиту от очистки веб-трафика после выгрузки зашифрованного трафика https и перенаправляет только обычный и безопасный трафик на внутренний веб-сервер позади.

10

Аутентификация безопасности

Встроенная функция аутентификации безопасности, поддержка использования двусторонней аутентификации (стандарт SKF) для сертификатов USB-ключа SM2, выданных китайскими центрами сертификации, беспрепятственная поддержка функции двусторонней аутентификации браузера ZT и поддержка программного сертификата клиента алгоритма SM2/RSA для обеспечения безопасности аутентификация.



Показатели эффективности

ZOTRUS

Шлюз автоматизации HTTPS ZoTrus обеспечивает эффективное, безопасное, прозрачное, простое в развертывании, полностью автоматическое инновационное решение без реконструкции для реализации шифрования https и защиты WAF, которое может эффективно расширить пропускную способность сетевых устройств и серверов, увеличить пропускную способность, и расширить возможности обработки сетевых данных, повысить гибкость и удобство использования сети, а также улучшить взаимодействие с пользователями, посещающими веб-сайт.

ZoTrus HTTPS Automation Gateway предоставляет полностью независимые и управляемые программные и аппаратные интеграционные продукты, включая 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 независимую сетевую карту и т. д. Полностью автономный и управляемый программный и аппаратный интегрированный SM2 HTTPS Automation Gateway может удовлетворить требования приложений этих отраслей, которые предъявляют чрезвычайно высокие требования к контролю информационной безопасности.

Каждый шлюз автоматизации HTTPS ZoTrus 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). до 255 доменных имен веб-сайтов для достижения адаптивного шифрования https с двойным алгоритмом. Количество веб-сайтов, поддерживающих шифрование https, ограничено количеством новых подключений, пропускной способностью и параллелизмом, поддерживаемыми оборудованием шлюза.

Каждый шлюз автоматизации HTTPS ZoTrus имеет гарантийный срок 5 лет и автоматически настраивает глобально доверенный SSL-сертификат ECC DV и SSL-сертификат соответствия криптографии SM2 OV не более чем для 255 доменных имен веб-сайтов в течение 5 лет. Рассчитанная на основе стоимости сертификата SSL CerSign OV SSL Lite (4888 юаней в год), стоимость автоматически настраиваемых сертификатов SSL достигает 6,23 миллиона юаней ($= 5 * 255 * 4888$, что соответствует 865 тысячам долларов США). и эксклюзивное в мире суперэффективное решение для автоматизации шифрования https!

ZoTrus HTTPS 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 https-шифрования, особенно требований приложений нулевой реконструкции для реализации https-шифрования SM2. 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.

ZOTRUS



Модель	MG-1-6	MG-1-7	MG-1-8	MG-1-9
Процессор	Intel (два процессора)	Хайгон (Один процессор)	Intel (два процессора)	Хайгон (Один процессор)
Включая количество ECC SSL	100	100	255	255
Включая SM2 SSL Кол-во	100	100	255	255
Двойная автоматическая выдача SSL	5 лет	5 лет	5 лет	5 лет
Тип SSL ECC	DV SSL	DV SSL	DV SSL	DV SSL
Тип SM2 SSL	OV SSL	OV SSL	OV SSL	OV SSL
Тип ВТИВ	EV	EV	EV	EV
SM2 https пропускная способность	9 Gbps	9 Gbps	9 Gbps	9 Gbps
Пропускная способность ECC https	9 Gbps	9 Gbps	9 Gbps	9 Gbps
SM2 SSL-запрос	90 K/s	60 K/s	90 K/s	60 K/s
ECC SSL-запрос	120 K/s	90 K/s	120 K/s	90 K/s
Макс. одновременно	1.8M	1.3M	1.8M	1.3M
Функция WAF	Встроенный	Встроенный	Встроенный	Встроенный
Настройка правил WAF	Да	Да	Да	Да
Правило регулярного обновления	Да	Да	Да	Да
Сетевой интерфейс	6xG + 4x10G	6xG + 4x10G	6xG + 4x10G	6xG + 4x10G
Размер шасси	2U	2U	2U	2U
Власть	2.44M RMB	2.44M RMB	6.23M RMB	6.23M RMB
Срок действия сертификата (5 лет)	600K RMB	600K RMB	1.5M RMB	1.5M RMB
Сохранить значение ЧСС (5 лет)	600 тысяч юаней	600 тысяч юаней	1,5 млн юаней	1,5 млн юаней
Подходящая область применения	Финансовые колледжи и университеты МСП	Крупные предприятия Правительственный / Финансовый сектор	Публичное облако крупного предприятия Облако электронного правительства	Облако электронного правительства для крупных предприятий и финансовых учреждений

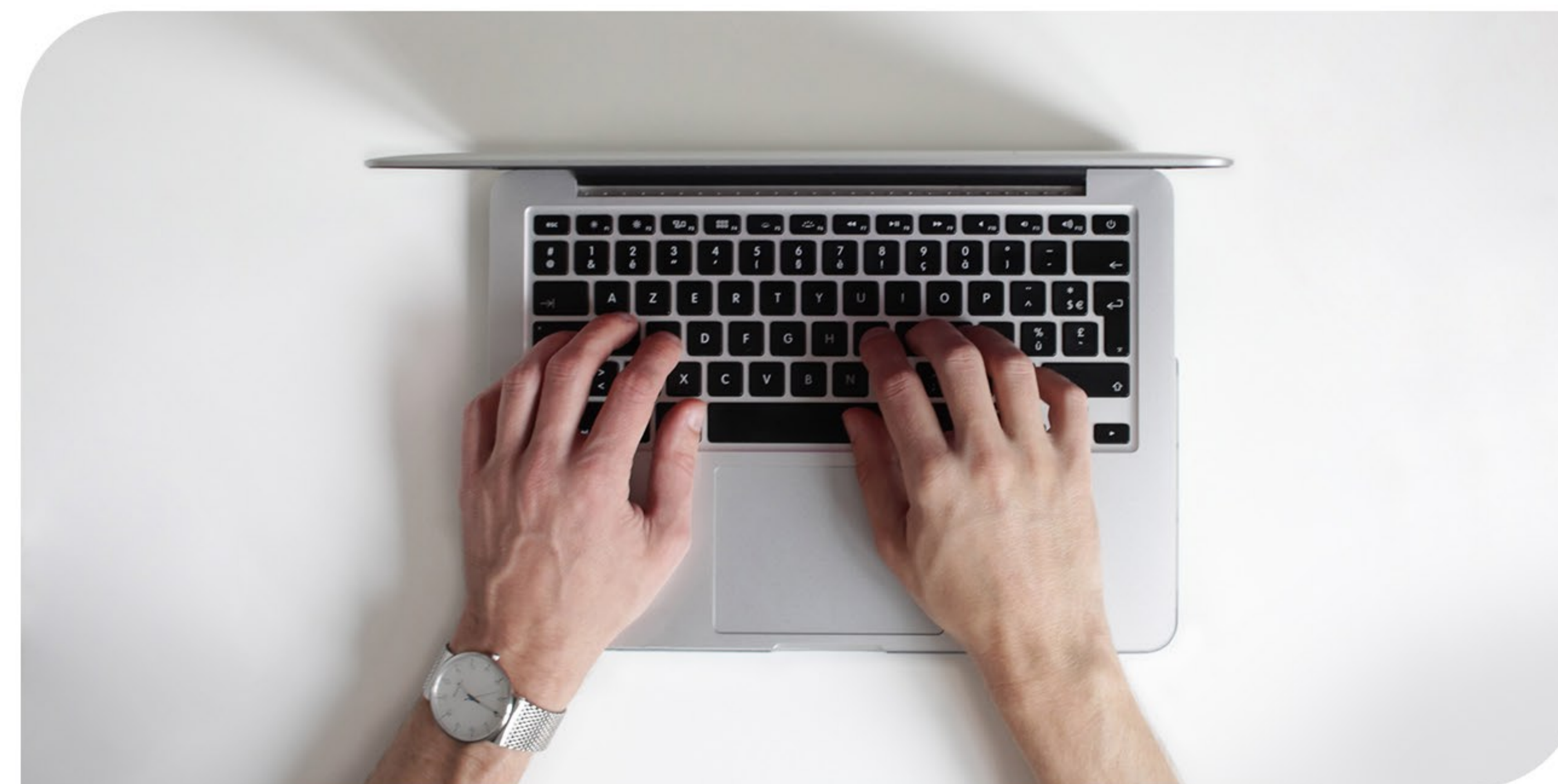
ZOTRUS

4

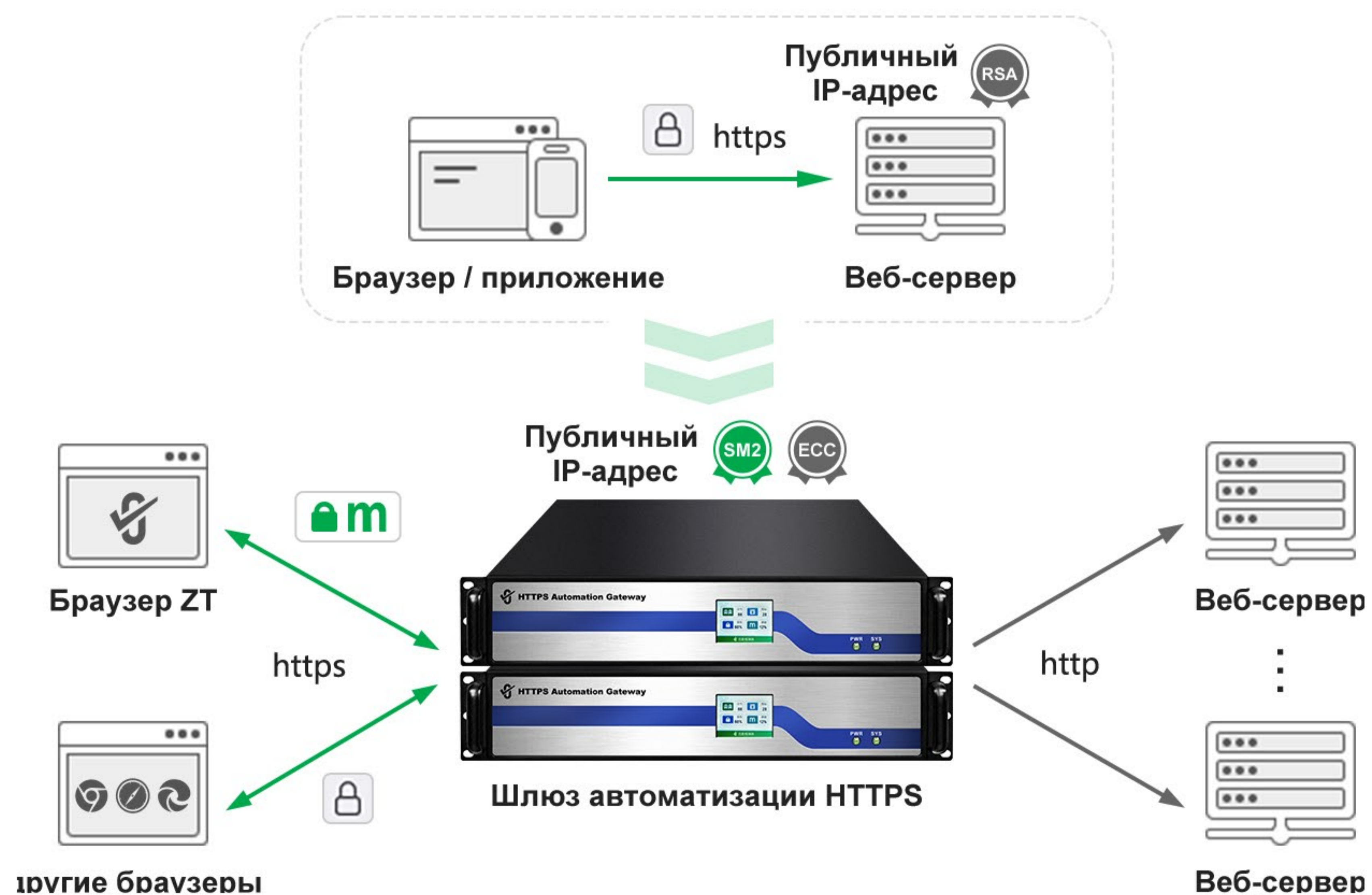
Решения по
развертыванию

<https://www.zotrus.com>

Шлюз автоматизации HTTPS ZoTrus поддерживает несколько режимов развертывания и применения, а также кластерное развертывание нескольких устройств. Чтобы обеспечить высокую доступность шлюза, настоятельно рекомендуется развернуть два шлюза, чтобы обеспечить 24*365 дней непрерывного автоматического предоставления службы шифрования HTTPS и службы защиты WAF.



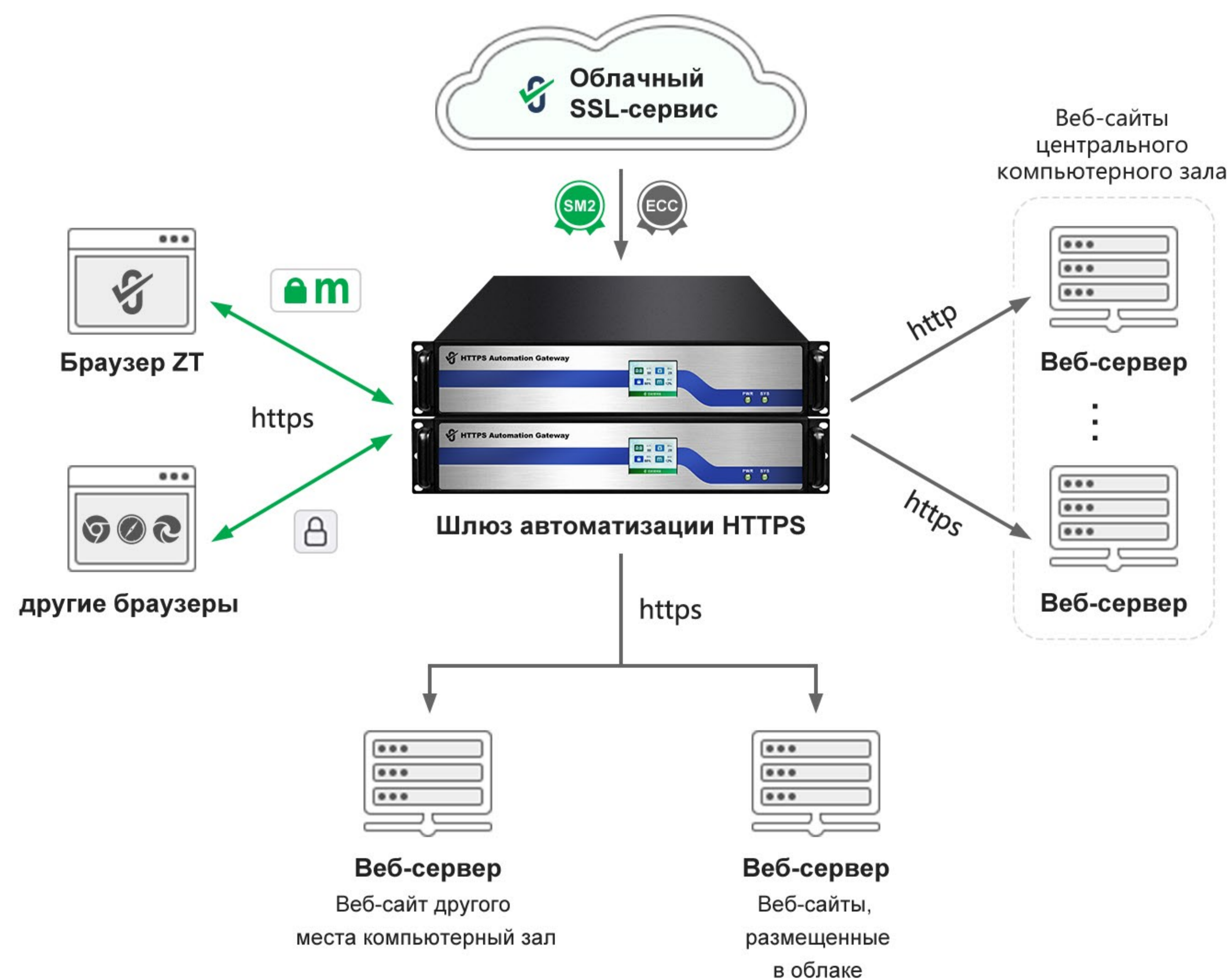
1. Предоставление услуги автоматизации шифрования HTTPS для локальных веб-серверов (веб-сайтов).



Традиционная реализация шифрования HTTPS заключается в том, что пользователь подает заявку на сертификат SSL в ЦС и вручную разворачивает его на веб-сервере для реализации шифрования HTTPS, что является очень трудоемкой и трудоемкой задачей для пользователей, которым необходимо развернуть сертификаты SSL для нескольких веб-сайтов. Если пользователь приобретет шлюз автоматизации HTTPS ZoTrus и развернет его перед веб-сервером, ему не нужно подавать заявку на сертификат SSL от центра сертификации, и шлюз ZoTrus автоматически подключится к системе обслуживания SSL ZoTrus Cloud для автоматической настройки двойного SSL-сертификаты для веб-сайта, а также автоматически реализуют шифрование HTTPS и защиту WAF.

Один сетевой порт шлюза автоматизации HTTPS ZoTrus подключен к исходному общедоступному сетевому интерфейсу, настроен общедоступный IP-адрес исходного веб-сервера, исходный веб-сервер подключен к другим портам и максимум 8 веб-серверов. могут быть подключены по умолчанию, и вместо этого эти веб-серверы настраиваются с использованием частных IP-адресов. Весь сетевой трафик данных ускоряется, разгружается и передается через шлюз, а пакеты данных, соответствующие протоколу приложения безопасности, будут пересылаться на соответствующий внутренний веб-сервер в соответствии с политикой балансировки нагрузки, поддерживающей пересылку открытого текста HTTP и зашифрованную пересылку HTTPS. Клиентам не нужно подавать заявку на сертификат SSL в ЦС и не нужно разворачивать сертификат SSL, а шлюз автоматически подключается к системе обслуживания SSL ZoTrus Cloud для автоматической подачи заявки на сертификат SSL с двойным алгоритмом и автоматического развертывания сертификатов SSL. и автоматически внедрить службу шифрования HTTPS с адаптивными алгоритмами шифрования, отвечающую требованиям приложений по соответствию криптографии и глобальному доверию. Гарантия на шлюз составляет 5 лет, шлюз будет заменен бесплатно для обеспечения бесперебойной работы службы автоматизации шифрования HTTPS и службы защиты WAF в течение 5 лет.

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



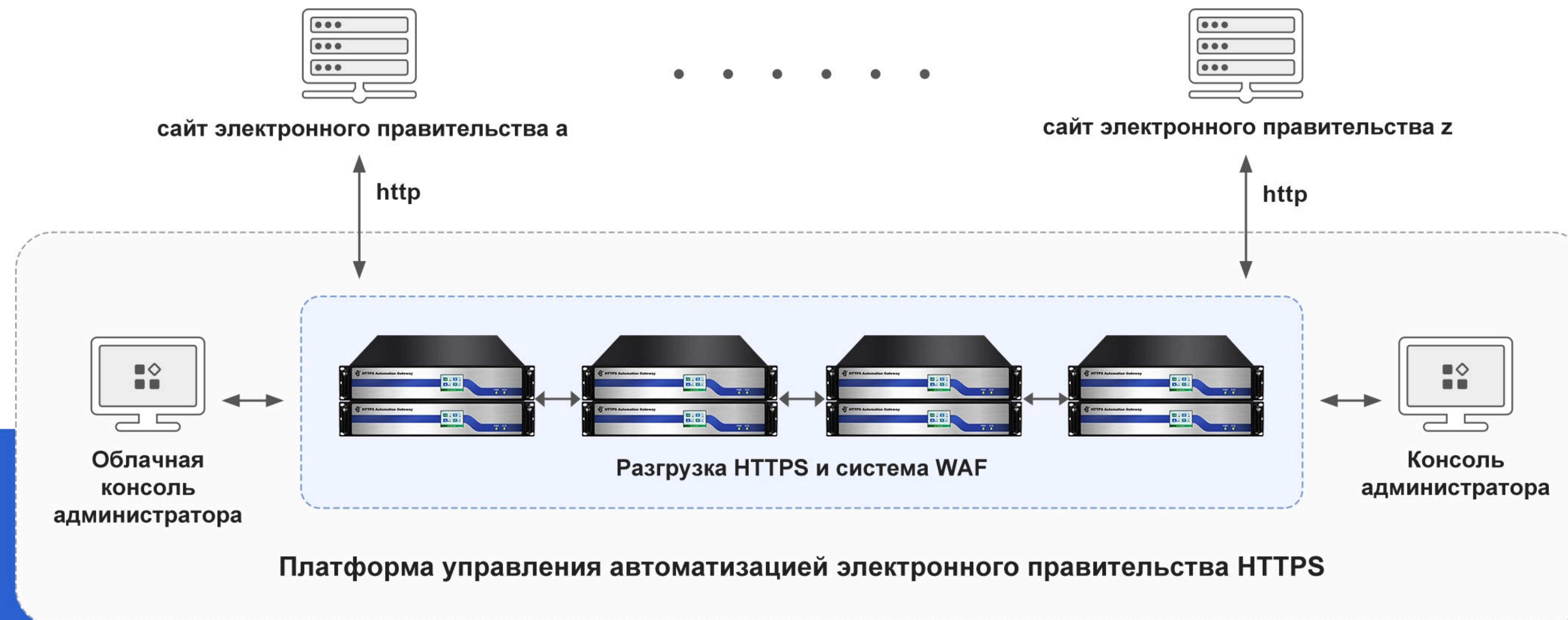
Для пользователей, которым необходимо не только внедрить службы автоматизации шифрования HTTPS на локальных серверах, но также иметь веб-серверы в филиалах или несколько веб-сайтов, развернутых в облаке, которым также требуется служба автоматизации HTTPS, ZoTrus Gateway поддерживает как режим локальной пересылки, так и режим удаленной обратной связи. Исходный режим. Независимо от того, находится ли веб-сервер (веб-сайт) в чужом компьютерном зале или на облачном хосте, если шлюз может получить к нему доступ через общедоступную сеть или интранет, эти веб-сайты являются исходными серверами с возвратом к исходному состоянию, похожими на службы CDN. и шлюз может предоставить им всем службу автоматизации шифрования HTTPS и службу защиты WAF. Двойные шлюзы предоставляют службу автоматизации шифрования HTTPS и службу защиты WAF для до 255 веб-сайтов, и большему числу веб-сайтов необходимо приобрести больше шлюзов.

Чтобы обеспечить безопасность данных системы веб-сайта, которая не расположена в центральном компьютерном зале, обратное соединение от шлюза к другому серверу местоположения должно быть зашифровано с помощью HTTPS для достижения полноканального шифрования. ZoTrus Technology бесплатно предоставляет самозаверяющий SSL-сертификат возврата к источнику со сроком действия 5 лет для веб-сайтов возврата к источнику, при этом исходный веб-сайт не требует развертывания глобально доверенного SSL-сертификата со сроком действия 5 лет. всего один год.

Этот метод развертывания также подходит для поставщиков услуг, которые обеспечивают дизайн веб-сайтов, веб-хостинг и продажу сертификатов SSL, а также развертывают несколько шлюзов для предоставления службы автоматизации шифрования HTTPS и службы защиты WAF для своих собственных бизнес-систем, а также службы автоматизации шифрования HTTPS и Служба защиты WAF для своих клиентов, независимо от того, где размещен веб-сайт клиента, достаточно, чтобы он был доступен только по HTTP или HTTPS.

3. Решение для автоматического развертывания кластера с шифрованием HTTPS на облачной платформе.

Для различных облачных платформ, таких как облачные платформы электронного правительства и общедоступные облачные платформы, существуют десятки тысяч или даже миллионы веб-сайтов, которым требуется шифрование HTTPS, и единственное решение может быть найдено только путем автоматизации. Необходимо развернуть несколько шлюзов автоматизации шифрования HTTPS для формирования кластерного массива — разгрузки HTTPS и системы WAF, а несколько шлюзов автоматизации шифрования HTTPS работают вместе, чтобы разделять бизнес-трафик и служить шлюзами горячего резерва друг для друга. В случае сбоя шлюза работающие на нем службы будут переданы другим шлюзам, чтобы обеспечить адекватное и своевременное реагирование на планирование обслуживания. Режим кластера подходит для развертывания резервных сетевых сред с упором на чрезвычайно высокую производительность.



4. Опционально: система автоматизации HTTPS ZoTrus SM2.

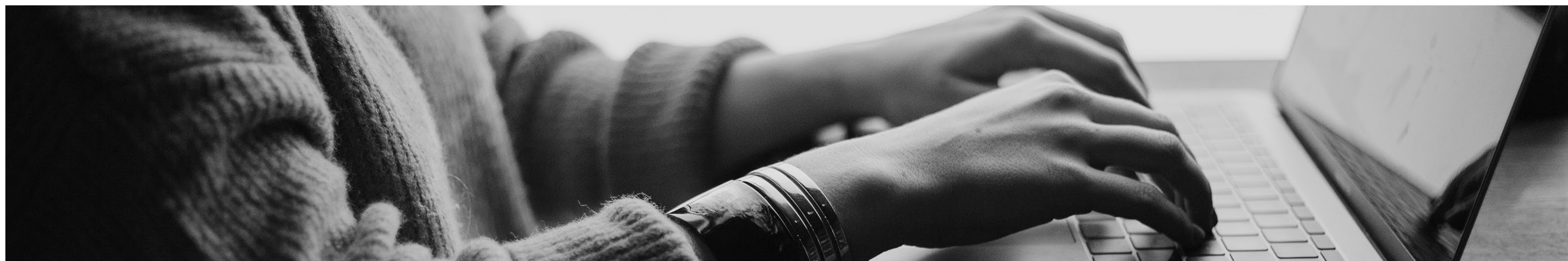


Если у вас есть простаивающий сервер или вам неудобно разворачивать аппаратное устройство шлюза автоматизации HTTPS ZoTrus, вы можете приобрести систему автоматизации HTTPS ZoTrus SM2 и развернуть систему шлюза на своем собственном сервере с голым железом, чтобы добиться тех же превосходных функций, что и ZoTrus. Шлюз автоматизации HTTPS.

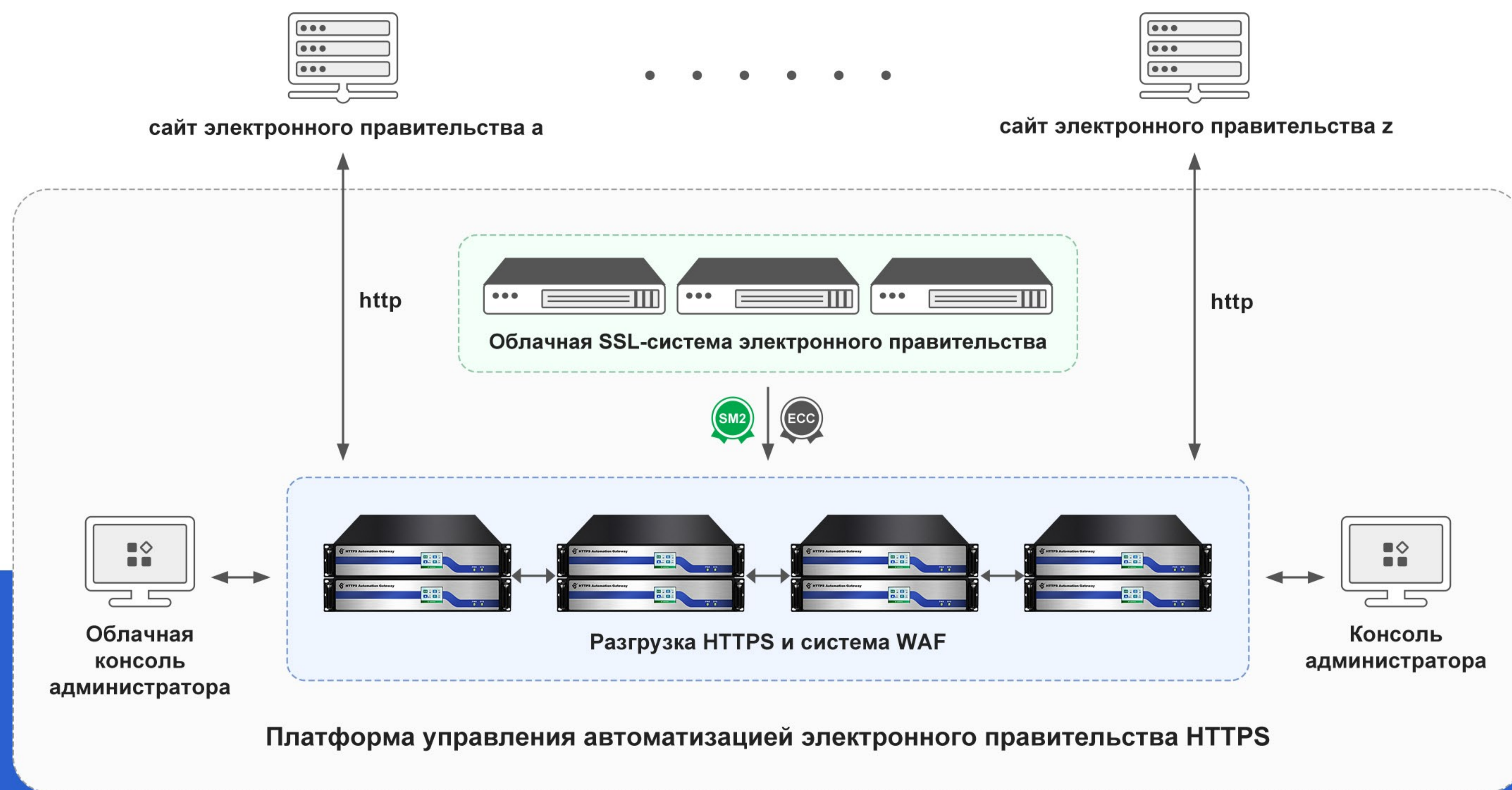
Система автоматизации ZoTrus SM2 HTTPS — это система, объединяющая операционную систему Linux (Ubuntu, Kylin OS и UOS дополнительно), веб-сервер Tengine, Tongsuo SSL, базовую систему ZoTrus HTTPS Automation Gateway, которую можно установить непосредственно на «голое железо» сервера. и посвящен реализации автоматизации SM2 HTTPS. После установки системы пользователю нужно только войти в интерфейс веб-управления, настроить доменное имя веб-сайта для реализации автоматического применения и развертывания SSL-сертификата с двойным алгоритмом, а также для поддержки автоматического развертывания SSL с двойным алгоритмом. сертификат на 5 лет бесперебойного обслуживания 255 веб-сайтов по умолчанию и автоматически реализует шифрование HTTPS адаптивного алгоритма, а браузеры, поддерживающие алгоритм SM2, такие как ZT Browser, преимущественно используют алгоритм SM2 для достижения шифрования SM2 HTTPS, а браузеры которые не поддерживают алгоритм SM2, используют алгоритм ECC для шифрования HTTPS.

Система автоматизации HTTPS ZoTrus SM2 обладает всеми функциями шлюза автоматизации HTTPS ZoTrus, связывает физический сервер и учетную запись пользователя и очень подходит для клиентов с собственным серверным оборудованием, таким как облачная платформа электронного правительства, коммерческая общедоступная облачная платформа, корпоративную частную облачную платформу и т. д., а также в полной мере использует существующие простаивающие серверы для предоставления службы автоматизации HTTPS и службы защиты WAF для различных веб-систем.

5. Необязательно: локальное развертывание облачной системы SSL.



По умолчанию шлюз автоматизации HTTPS автоматически подключается к облачной системе SSL ZoTrus, чтобы включить шифрование https после получения двойных сертификатов SSL. Клиенты облачной платформы, которые хотят самостоятельно выдавать двойные сертификаты SSL собственной марки, которые автоматически развертываются на шлюзе, могут развернуть облачную систему SSL ZoTrus локально, чтобы реализовать автоматическую выдачу двойных сертификатов SSL с помощью выделенного промежуточного звена SSL с собственной торговой маркой. корневой сертификат. Локально развернутая система называется облачной системой SSL электронного правительства или системой SSL публичного облака.



Облачная SSL-система электронного правительства — это локально развернутая система CA для выдачи SSL-сертификатов, соответствующих криптографии и поддерживающих прозрачность сертификатов SM2. Развертывание всей системы призвано реализовать полностью независимую и контролируруемую выдачу и управление SSL-сертификатами SM2 для веб-сайта электронного правительства, а также относительно независимую выдачу SSL-сертификатов ECC. Чтобы добиться независимой и контролируемой выдачи SSL-сертификатов электронного правительства, прежде всего, должен существовать промежуточный корневой сертификат для выдачи SSL-сертификатов, чтобы все системы электронного правительства могли надежно осознавать, что все системы электронного правительства доверяют только выданным SSL-сертификатам. с помощью своих собственных промежуточных корневых сертификатов, эффективно предотвращая различные SSL-атаки «посредника» на веб-сайты электронного правительства и другие фальшивые атаки на веб-сайты электронного правительства.



Резюме



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

Эксклюзивная глобальная инновация ZoTrus HTTPS Automation Gateway, обеспечивающая нулевое изменение исходного веб-сервера для реализации автоматического шифрования https, службы защиты WAF, двухалгоритмного адаптивного шифрования https SM2/ECC, просто настройте доменное имя веб-сайта и IP-адрес при запуске, немедленно включите Служба шифрования и ускорения https, защита WAF, безопасная доставка TCP/DTLS, автоматическая подготовка двойных сертификатов SSL, соответствие глобальному доверию и криптографии, высокоскоростное динамическое кэширование и сжатие, мультиплексирование соединений, сохранение сеансов и балансировка нагрузки и т. д. При обеспечении высокой производительности, он обеспечивает самое высокое в отрасли соотношение производительности и цены.

Шлюз автоматизации HTTPS ZoTrus работает по принципу «подключи и работай», развертывается на передней части сервера веб-сайта. Исходный сервер веб-сайта может быть легко обновлен с http до https без каких-либо изменений, а шифрование HTTPS SM2 соответствует криптографии. соответствие требованиям и шифрование ECC https для совместимости со всеми браузерами, не поддерживающими алгоритм SM2. Его мощная функция ускорения, разгрузки и пересылки https обеспечивает дополнительную поддержку повышения производительности сервера веб-сайта, не только не увеличивает нагрузку на шифрование и дешифрование https, но также расширяет возможности внешнего ответа и способность обрабатывать запросы пользователей. Бесшовное переключение шлюза автоматизации HTTPS ZoTrus с нулевой реконструкцией, отсутствием обслуживания и нулевым воздействием является первым выбором и обязательным для шифрования SM2 https, защиты WAF и обновления безопасности системы с http на https.