solidwall

Intelligent Web
Application
Firewall

КРАТКОЕ РУКОВОДСТВО

пользователя SolidWall

г. Москва

ОГЛАВЛЕНИЕ

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

ВВЕДЕНИЕ

Данное руководство поможет выбрать необходимую конфигурацию интеллектуального межсетевого экрана уровня приложений SolidWall WAF (далее – SolidWall WAF) и познакомит с рекомендуемыми схемами его внедрения.

Интеллектуальный сетевой экран для защиты веб-приложений SolidWall WAF позволяет обеспечить эффективную защиту критичных веб-ресурсов от внешних атак, а также дает возможность осуществлять полный контроль использования приложений в разрешенных сценариях.

SolidWall WAF обеспечивает выполнение ряда следующих функций:

- контроль и фильтрацию трафика защищаемых веб приложений;
- идентификацию и аутентификацию пользователей SolidWall WAF;
- регистрацию событий безопасности (аудит);
- бесперебойное функционирование и восстановление;
- тестирование и контроль целостности;
- управление (администрирование);
- взаимодействие с другими средствами защиты информации.

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

1. ОСНОВНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ

SolidWall WAF может быть установлен как на физические, так и на виртуальные серверы.

Со списком поддерживаемых гипервизоров можно ознакомиться в требованиях на выбранную для установки WAF операционную систему.

В качестве системного программного обеспечения поддерживаются следующие операционные системы (ОС):

- Ubuntu 22.04 Server 64-bit;
- Debian 12 64-bit;
- Astra Linux 1.7 Smolensk.

Актуальная версия SolidWall WAF на момент написания данного руководства — 2.18.

1.1. Минимальные аппаратные требования

- **Объём оперативной памяти (RAM):** не менее 8 ГБ.
- **Процессор (CPU):** 4-ядерный и более с архитектурой x86-64, тактовая частота не ниже 2.4 ГГц.
- **Объём жёсткого диска (HDD):** не менее 500 Гб.
- **Сетевые интерфейсы:** два сетевых интерфейса 1 ГБит/с Ethernet для пассивного режима захвата трафика; один сетевой интерфейс 1 ГБит/с Ethernet для активного режима захвата трафика.

1.2. Разметка диска

В случае, когда установка производится на узел Управления или в режиме stand-alone (все службы располагаются на одном узле) дисковое пространство должно быть размечено в следующих пропорциях: минимум 30 ГБ в «/», минимум 50 ГБ в «/var/log/», минимум 400 ГБ в «/var/lib/postgresql/».

В случае, когда производится установка узла Анализа, дисковое пространство должно быть размечено в следующих пропорциях: минимум 30 ГБ в «/», минимум 50 ГБ в «/var/log/».

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

2. РЕЖИМЫ РАБОТЫ

SolidWall WAF может работать в нескольких режимах захвата трафика.

2.1. Обратный прокси

Режим обратного прокси (активный режим захвата трафика или режим в разрыв) – это основной рекомендуемый режим работы. В данном режиме HTTP(s) трафик терминируется на узлах SolidWall WAF. Это позволяет влиять на пропускаемый трафик и выполнять его фильтрацию от атак и нежелательных HTTP транзакций.

Типовые схемы включения показаны в разделе 3 «Реестр конфигураций SolidWall WAF».

Необходимо отметить, что в данном режиме можно выбирать, влияет ли SolidWall WAF на трафик или нет. По умолчанию в данном режиме работы SolidWall WAF не осуществляет фильтрацию трафика до тех пор, пока оператор не переведёт его в «Режим активных блокировок» для конкретного защищаемого приложения.

2.2. Пассивный захват

Режим пассивного захвата трафика (режим сниффера) – это демонстрационный режим. Он не рекомендован для промышленной эксплуатации.

2.3. Гибридный режим

Данный режим сочетает в себе два предыдущих.

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

3. РЕЕСТР КОНФИГУРАЦИЙ SOLIDWALL WAF

Ниже в таблице перечислены типовые конфигурации SolidWall WAF для режима обратный прокси, а также критерии, которые смогут вам помочь в выборе нужной конфигурации.

Таблица 1. Типовые конфигурации SolidWall WAF

Конфигурация WAF	Максимальная нагрузка, RPS	Отказоустойчивость	Георасределенность	Назначение
Один узел всё-в-одном (см. раздел 4)	2 000	Нет	Нет	Тестовый стенд; защита некритичных ненагруженных веб-приложений
Кластер из двух узлов – актив-пассив (см. раздел 5)	2 000	Да	Возможна	Защита ненагруженных веб-приложений
Распределенная конфигурация с одним узлом Управления и несколькими активными узлами Анализа (см. раздел 6)	100 000	Для узлов Анализа	Возможна для узлов Анализа	Защита нагруженных веб-приложений/большого числа приложений
Распределенная конфигурация с кластером узлов управления (см. раздел 7)	100 000	Да	Возможна	Защита нагруженных веб-приложений/большого числа приложений
Георасределенная конфигурация (см. раздел 8)	100 000	Да	Да	Защита георасределенных нагруженных веб-приложений
Сильно распределенная конфигурация (см. раздел 9)	200 000	Да	Возможна	Защита сильно нагруженных веб-приложений/большого числа приложений

Для нестандартных условий и требований либо для сверхбольших нагрузок конфигурация WAF разрабатывается индивидуально.

В следующем разделе приведена более подробная информация о типовых конфигурациях SolidWall WAF.

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

4. КОНФИГУРАЦИЯ «ОДИН УЗЕЛ»

4.1. Необходимые лицензии

Для конфигурации «Один узел» требуется лицензия PRO от 100 до 2000 RPS на один узел SolidWall WAF. Большие значения RPS с данной конфигурацией не поддерживаются лицензионно.

4.2. Описание конфигураций

На рисунке 1 представлена схема доставки веб-приложения с данной конфигурацией WAF.

Рисунок 1. Схема доставки веб-приложения с конфигурацией «Один узел»

Все модули SolidWall WAF, включая модуль управления с веб-интерфейсом, СУБД, модуль анализа, расположены на одном физическом или виртуальном узле.

При использовании конфигурации «Один узел» рекомендуется дополнить SolidWal WAF следующими инструментами:

1. Рекомендуется использовать AntiDDoS – сервис (как правило на уровне провайдера), осуществляющий очистку трафика до приложения от распределенных атак типа отказ в обслуживании.
2. TLS-server / Балансировщик – опциональные элементы инфраструктуры доставки приложений, терминирующие TLS/SSL-соединения и/или осуществляющие балансировку нагрузки между серверами приложений.

4.3. Сценарии использования

Данную конфигурацию рекомендуется использовать в ситуациях, когда не требуется высокая производительность и отказоустойчивость, а также для целей пилотирования или тестирования SolidWall WAF. При отказе или плановых работах на узле WAF можно реализовать резервный маршрут доставки трафика напрямую к защищаемым приложениям и автоматическое переключение на него, например, при помощи балансировщика. На схеме резервный маршрут обозначен пунктирной стрелкой. Для восстановления узла WAF после сбоя можно использовать функционал снепшотов гипервизора в случае, если WAF установлен на виртуальный сервер. Рекомендуется регулярно делать резервные копии настроек и баз данных WAF. Рекомендуется настроить мониторинг критичных параметров работоспособности узла WAF, а также автоматические уведомления о неисправностях. Если нагрузка на защищаемые приложения вырастет, то масштабирование такой конфигурации может быть только вертикальным. При необходимости можно расширить данную конфигурацию в отказоустойчивую (см. раздел 5) или распределенную (см раздел 6). Подробности об установке и настройке SolidWall WAF изложены в соответствующих руководствах пользователя, которые предоставляются после заключения соглашения о неразглашении.

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

5. КОНФИГУРАЦИЯ «КЛАСТЕР ВЕДУЩИЙ-ВЕДОМЫЙ»

5.1. Необходимые лицензии

Для конфигурации «Кластер ведущий-ведомый» (или активный-пассивный, или master-slave) требуются лицензии PRO от 100 до 2000 RPS на основной и резервный узлы SolidWall WAF.

Большие значения RPS с данной конфигурацией не поддерживаются лицензионно.

5.2. Описание конфигурации

На рисунке 2 представлена схема доставки веб-приложения с данной конфигурацией WAF.

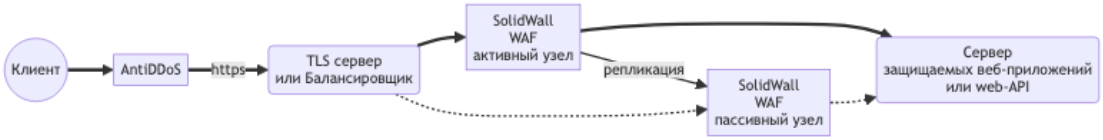

Рисунок 2. Схема доставки веб-приложения с конфигурацией «Кластер ведущий-ведомый»

Все модули SolidWall WAF, включая модуль управления с веб-интерфейсом, СУБД, модуль анализа, расположены на каждом из двух физических или виртуальных узлах.

При использовании конфигурации «Кластер ведущий-ведомый» рекомендуется дополнить SolidWal WAF следующими инструментами:

1. AntiDDoS – сервис (как правило на уровне провайдера), осуществляющий очистку трафика до приложения от распределенных атак типа «отказ в обслуживании». Крайне рекомендуемый элемент защиты приложений.
2. TLS-server / Балансировщик – опциональные элементы инфраструктуры доставки приложений, терминирующие TLS/SSL-соединения и/или осуществляющие балансировку нагрузки между серверами приложений.

5.3. Сценарии использования

Данную конфигурацию рекомендуется использовать в ситуациях, когда не требуется высокая производительность, однако есть высокие требования по обеспечению доступности защищаемых веб-приложений.

Отказоустойчивость WAF обеспечивается режимом работы кластера из двух узлов – ведущего (активный) и ведомого (пассивный). В таком режиме активный узел проксирует через себя HTTP-трафик и непрерывно реплицирует все необходимые данные на пассивный узел WAF. В момент сбоя активного узла пассивный узел становится активным и обеспечивает работоспособность WAF. После восстановления неисправный узел возвращается в строй и становится пассивным узлом.

Рекомендуется регулярно делать резервные копии настроек и баз данных WAF.

Рекомендуется настроить мониторинг критичных параметров работоспособности узла WAF, а также автоматические уведомления о неисправностях.

Если нагрузка на защищаемые приложения вырастет, то масштабирование такой конфигурации может быть только вертикальным. При необходимости можно апгрейдить данную конфигурацию в распределенную (см. раздел 7).

Подробности об установке и настройке SolidWall WAF изложены в соответствующих руководствах по эксплуатации, которые предоставляются после заключения соглашения о неразглашении.

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

6. РАСПРЕДЕЛЕННАЯ КОНФИГУРАЦИЯ С ОДНИМ УЗЛОМ УПРАВЛЕНИЯ

6.1. Необходимые лицензии

Для распределенной конфигурации с одним узлом базы знаний необходима лицензия Enterprise на один узел управления и необходимое количество RPS. Количество узлов Анализа при этом может быть любым.

6.2. Описание конфигурации

На рисунке 3 представлена схема доставки веб-приложения с данной конфигурацией WAF.

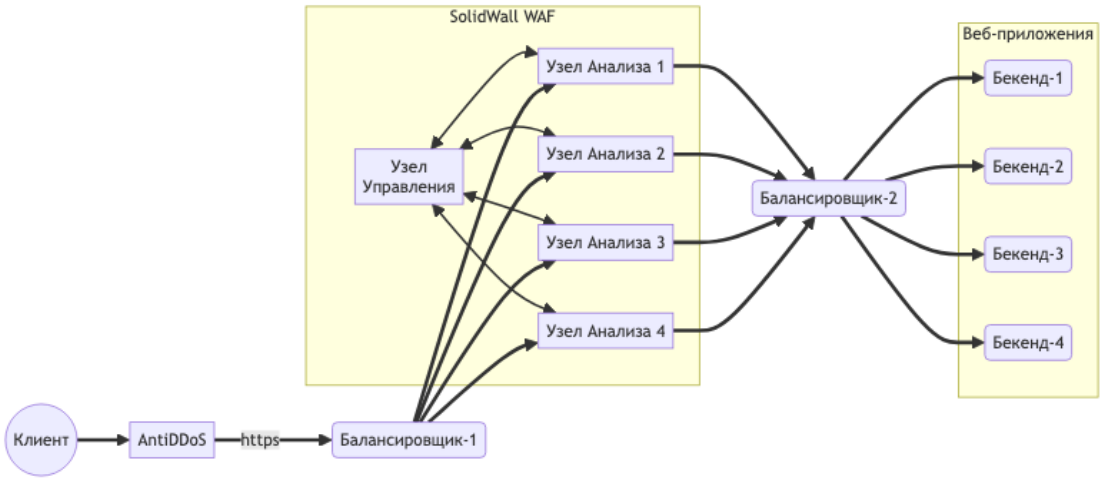

Рисунок 3. Схема доставки веб-приложения с распределенной конфигурацией с одним узлом Управления

WAF устанавливается на виртуальные или физические серверы и включает:

- Узел Управления объединяет в себе СУБД для хранения конфигураций, политик ИБ и данных о транзакциях, модуль управления с веб-интерфейсом и подсистему автоматических задач.
- Узлы Анализа – активные узлы выполняющие проксирование и фильтрацию трафика.

При использовании распределённой конфигурации с одним узлом управления рекомендуется дополнить SolidWal WAF следующими инструментами:

1. AntiDDoS – сервис (как правило, на уровне провайдера), осуществляющий очистку трафика до приложения от распределенных атак типа «отказ в обслуживании». Крайне рекомендуемый элемент защиты приложений.
2. Балансировщики – обязательные элементы инфраструктуры доставки трафика при использовании распределенной конфигурации WAF с несколькими узлами Анализа. Балансировщик-1 балансирует нагрузку по узлам Анализа. Балансировщик-2 балансирует нагрузку по бекендам защищаемых приложений.

6.3. Сценарии использования

Данную конфигурацию рекомендуется использовать в ситуациях, когда требуется высокая производительность и высокая доступность защищаемых веб-приложений. Однако нет жестких требований к

отказоустойчивости узла Управления WAF. Например, допустимо потерять часть информации о трафике за время восстановления узла Управления после сбоя.

При недоступности узла Управления узлы Анализа продолжат выполнять свои функции, кроме возможности сохранять информацию о трафике защищаемых приложений в СУБД. После восстановления связи с узлом Управления информация о трафике продолжит сохраняться в СУБД.

Высокая доступность веб-приложений обеспечивается за счет балансировщиков, которые при помощи специальных проверок должны уметь выявлять неисправные узлы Анализа или бекенды защищаемых приложений и автоматически перенаправлять трафик по оставшимся в строю узлам.

Рекомендуется регулярно делать резервные копии настроек и баз данных WAF.

Рекомендуется настроить мониторинг критичных параметров работоспособности узла WAF, а также автоматические уведомления о неисправностях.

Если нагрузка на защищаемые приложения вырастет, то масштабирование узлов Анализа осуществляется при помощи добавления необходимого числа дополнительных узлов Анализа. Узел Управления масштабируется вертикально. Для больших нагрузок (>50 000 rps) можно вынести отдельные модули узла Управления, например СУБД, на выделенные серверы. Также есть возможность апгрейдить узел Управления до отказоустойчивого кластера узлов Управления (см. раздел 7 «Распределенная конфигурация с кластером узлов Управления»).

Подробности об установке и настройке SolidWall WAF изложены в соответствующих руководствах по эксплуатации, которые предоставляются после заключения соглашения о неразглашении.

7. РАСПРЕДЕЛЕННАЯ КОНФИГУРАЦИЯ С КЛАСТЕРОМ УЗЛОВ УПРАВЛЕНИЯ

7.1. Необходимые лицензии

Для распределенной конфигурации с одним узлом базы знаний необходима лицензия Enterprise на основной и резервный узлы Управления и необходимое количество RPS. Количество узлов Анализа при этом может быть любым.

7.2. Описание конфигурации

На рисунке 4 представлена схема доставки веб-приложения с данной конфигурацией WAF.

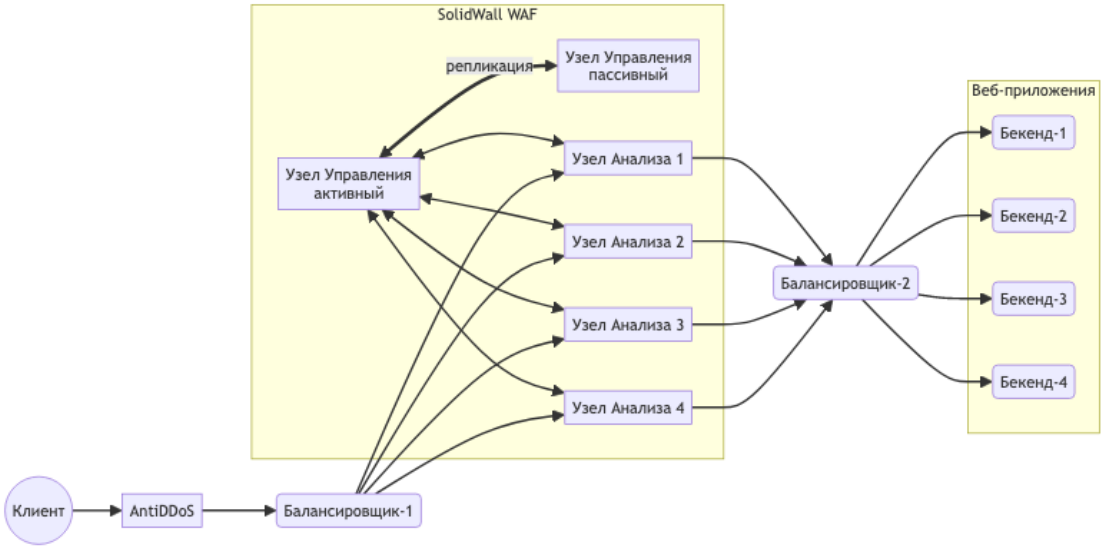

Рисунок 4. Схема доставки веб-приложения с распределенной конфигурацией с кластером узлов Управления

WAF устанавливается на виртуальные или физические серверы и включает в себя:

- Каждый узел Управления объединяет в себе СУБД для хранения конфигураций, политик ИБ и данных о транзакциях, модуль управления с веб-интерфейсом и подсистему автоматических задач.
- Узлы Управления, активный и пассивный, объединены в отказоустойчивый кластер. При падении активного узла его роль на себя берет пассивный.
- Узлы Анализа – активные узлы выполняющие проксирование и фильтрацию трафика.

При использовании распределённой конфигурации с кластером узлов управления рекомендуется дополнить SolidWal WAF следующими инструментами:

1. AntiDDoS – сервис (как правило, на уровне провайдера), осуществляющий очистку трафика до приложения от распределенных атак типа «отказ в обслуживании». Крайне рекомендуемый элемент защиты приложений.
2. Балансировщики – обязательные элементы инфраструктуры доставки трафика при использовании распределенной конфигурации WAF с несколькими узлами Анализа. Балансировщик-1 балансирует нагрузку по узлам анализа. Балансировщик-2 балансирует нагрузку по бекендам защищаемых приложений.

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

7.3. Сценарии использования

Данную конфигурацию рекомендуется использовать в ситуациях, когда требуется высокая производительность и высокая доступность защищаемых веб-приложений, а также необходимо обеспечить отказоустойчивость узлов Управления WAF.

Высокая доступность веб-приложений обеспечивается за счет балансировщиков, которые при помощи специальных проверок должны уметь выявлять неисправные узлы Анализа или бекенды защищаемых приложений и автоматически перенаправлять трафик по оставшимся в строю узлам.

Рекомендуется регулярно делать резервные копии настроек и баз данных WAF.

Рекомендуется настроить мониторинг критичных параметров работоспособности узла WAF, а также автоматические уведомления о неисправностях.

Если нагрузка на защищаемые приложения вырастет, то масштабирование узлов Анализа осуществляется при помощи добавления необходимого числа дополнительных узлов Анализа. Узлы Управления масштабируются вертикально. Также, при необходимости, можно сделать конфигурацию более распределенной (см. раздел 9 «Сильно распределенная конфигурация»), если вынести отдельные модули узла Управления на выделенные серверы.

Подробности об установке и настройке SolidWall WAF изложены в соответствующих руководствах по эксплуатации, которые предоставляются после заключения соглашения о неразглашении.

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

8. ГЕОРАСПРЕДЕЛЕННАЯ КОНФИГУРАЦИЯ С КЛАСТЕРОМ УЗЛОВ УПРАВЛЕНИЯ

8.1. Необходимые лицензии

Для распределенной конфигурации с геокластером узлов базы знаний необходима лицензия Enterprise на основной и 3 резервных узла Управления и необходимое количество RPS. Количество узлов Анализа при этом может быть любым.

8.2. Описание конфигурации

На рисунке 5 представлена схема доставки геораспределенных веб-приложений с данной конфигурацией WAF.

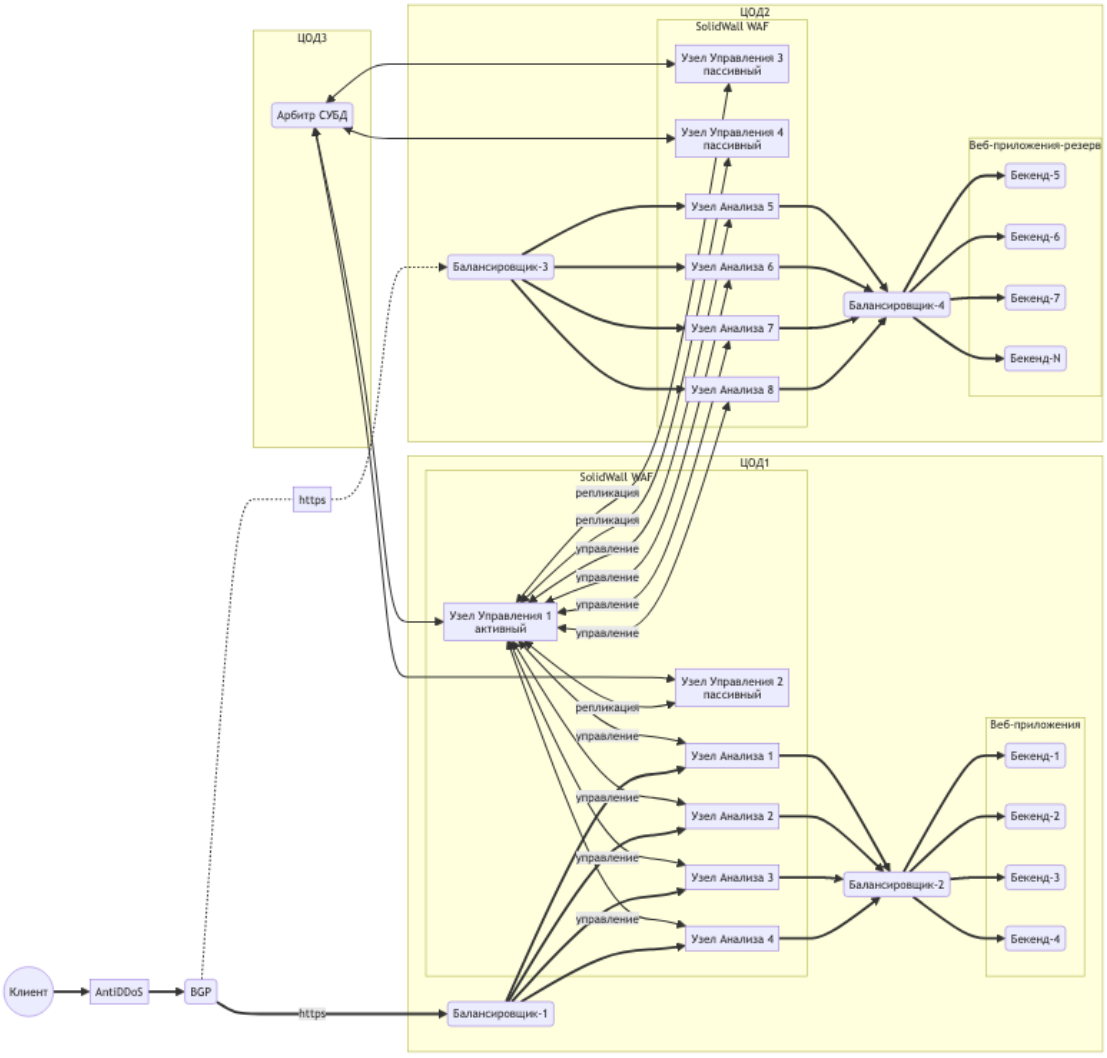

Рисунок 5. Схема доставки геораспределенных веб-приложений с геораспределенной конфигурацией с кластером узлов Управления

Защищаемые приложения расположены в двух ЦОД. При падении одного из двух ЦОД оставшийся ЦОД должен обеспечить доступность и защиту веб-приложений.

WAF устанавливается на виртуальные или физические серверы и включает:

- Каждый узел Управления объединяет в себе СУБД для хранения конфигураций, политик ИБ и данных о транзакциях, модуль управления с веб-интерфейсом и подсистему автоматических задач.
- Узлы Управления, активный и три пассивных, объединены в отказоустойчивый кластер. При падении активного узла его роль на себя берет один из пассивных.
- Узлы Анализа – активные узлы, выполняющие проксирование и фильтрацию трафика.

При использовании георазпределённой конфигурации с кластером узлов управления рекомендуется дополнить SolidWal WAF следующими инструментами:

1. AntiDDoS – сервис (как правило, на уровне провайдера), осуществляющий очистку трафика до приложения от распределенных атак типа «отказ в обслуживании». Крайне рекомендуемый элемент защиты приложений.
2. Распределение нагрузки пользователей веб-приложений между ЦОД обеспечивается за счет BGP-маршрутизации.
3. Балансировщики – обязательные элементы инфраструктуры доставки трафика при использовании распределенной конфигурации WAF с несколькими узлами Анализа. Балансировщик-1 и Балансировщик-3 балансируют нагрузку по узлам Анализа. Балансировщик-2 и Балансировщик-4 балансируют нагрузку по бекендам защищаемых приложений.
4. В третьем ЦОД расположен один узел с ролью Арбитр СУБД, обеспечивающий защиту от аварии типа «split-brain», которая может возникнуть при нарушении связности между ЦОД1 и ЦОД2.

8.3. Сценарии использования

Данную конфигурацию рекомендуется использовать в ситуациях, когда требуется высокая производительность и высокая доступность георазпределеных защищаемых веб-приложений, а также необходимо обеспечить отказоустойчивость узлов Управления WAF, как на уровне каждого ЦОД, так и между ЦОД.

Высокая доступность веб-приложений обеспечивается за счет балансировщиков, которые при помощи специальных проверок должны уметь выявлять неисправные узлы Анализа или бекенды защищаемых приложений и автоматически перенаправлять трафик по оставшимся в строю узлам.

Рекомендуется регулярно делать резервные копии настроек и баз данных WAF.

Рекомендуется настроить мониторинг критичных параметров работоспособности узла WAF, а также автоматические уведомления о неисправностях.

Если нагрузка на защищаемые приложения вырастет, то масштабирование узлов Анализа осуществляется при помощи добавления необходимого числа дополнительных узлов Анализа. Узлы Управления масштабируются вертикально. Также, при необходимости, можно сделать конфигурацию более распределенной (см. раздел 9 «Сильно распределенная конфигурация»), если вынести отдельные модули узла Управления на выделенные серверы.

Подробности об установке и настройке SolidWall WAF изложены в соответствующих руководствах по эксплуатации, которые предоставляются после заключения соглашения о неразглашении.

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57

9. СИЛЬНО РАСПРЕДЕЛЕННАЯ КОНФИГУРАЦИЯ

9.1. Необходимые лицензии

Для распределенной конфигурации с одним узлом базы знаний необходима лицензия Enterprise на основной и резервный узлы Управления и необходимое количество RPS. Количество узлов Анализа при этом может быть любым.

9.2. Описание конфигурации

На рисунке 6 представлена схема доставки веб-приложения с данной конфигурацией WAF.

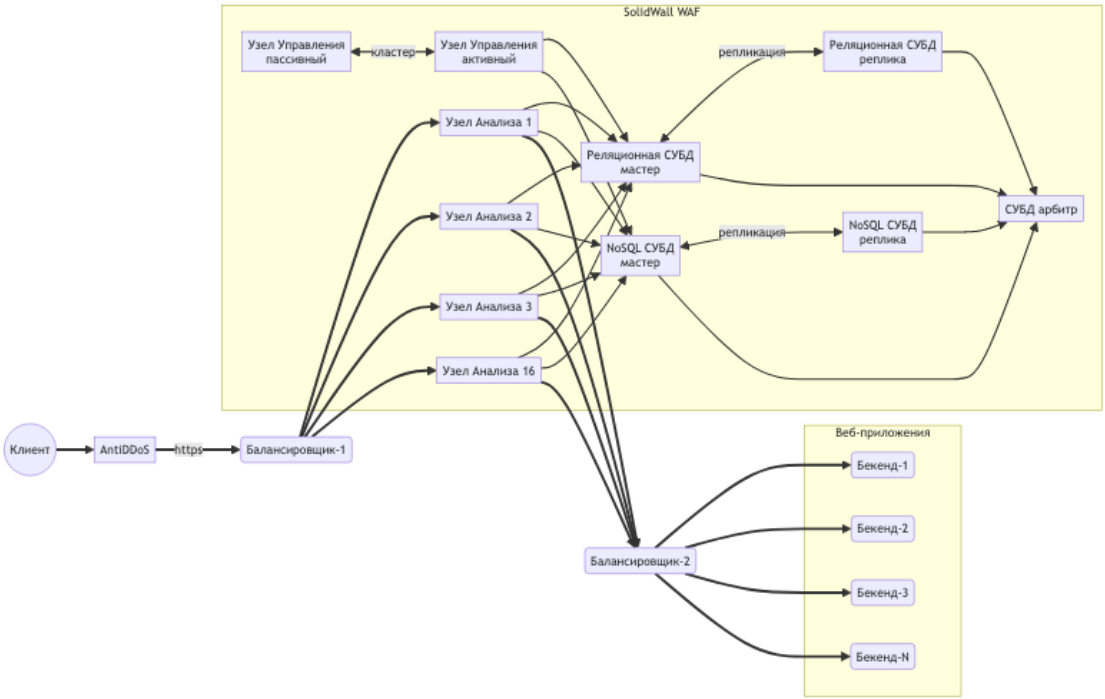

Рисунок 6. Схема доставки веб-приложения с сильно распределенной конфигурацией

Модули WAF устанавливаются на виртуальные или физические серверы и включают:

- Каждый узел Управления объединяет в себе модуль управления с веб-интерфейсом и подсистему автоматических задач с машинным обучением.
- Узлы Управления и узлы СУБД собраны в отказоустойчивые серверы. Данные в СУБД непрерывно реплицируются. При отказе какого-либо из активных узлов резервный автоматически занимает его роль.
- Узлы Анализа – активные узлы выполняющие проксирование и фильтрацию трафика.

При использовании сильно распределённой конфигурации рекомендуется дополнить SolidWal WAF следующими инструментами:

1. AntiDDoS – сервис (как правило, на уровне провайдера), осуществляющий очистку трафика до приложения от распределенных атак типа «отказ в обслуживании». Крайне рекомендуемый элемент защиты приложений.
2. Балансировщики – обязательные элементы инфраструктуры доставки трафика при использовании распределенной конфигурации WAF с несколькими узлами Анализа. Балансировщик-1 балансирует

нагрузку по узлам анализа. Балансировщик-2 балансирует нагрузку по бекендам защищаемых приложений.

9.3. Сценарии использования и рекомендации

Данную конфигурацию рекомендуется использовать в ситуациях, когда требуется очень большая производительность и высокая доступность защищаемых веб-приложений, а также необходимо обеспечить отказоустойчивость подсистем Управления WAF.

Высокая доступность веб-приложений обеспечивается за счет балансировщиков, которые при помощи специальных проверок (check) должны уметь выявлять неисправные узлы Анализа или бекенды защищаемых приложений и автоматически перенаправлять трафик по оставшимся в строю узлам.

Рекомендуется регулярно делать резервные копии настроек и баз данных WAF.

Рекомендуется настроить мониторинг критичных параметров работоспособности узла WAF, а также автоматические уведомления о неисправностях.

Если нагрузка на защищаемые приложения вырастет, то масштабирование узлов Анализа осуществляется при помощи добавления необходимого числа дополнительных узлов Анализа. Узлы Управления и узлы СУБД масштабируются вертикально. При необходимости, можно сделать конфигурацию георазпределенной (см. раздел 8 «Георазпределенная конфигурация с кластером узлов Управления»).

Подробности об установке и настройке SolidWall WAF изложены в соответствующих руководствах по эксплуатации, которые предоставляются после заключения соглашения о неразглашении.

117312, г. Москва, вн. тер. г. муниципальный округ Академический, улица Вавилова, дом 47А, помещение 1/2, solidwall.ru, info@solidwall.ru
+7 (499) 705-76-57