ООО «ИКС ЛАБЗ»
г. Москва, вн.тер.г. муниципальный округ Тверской,
ул. Новослободская, д. 24а, стр. 2, кв. 26

ОГРН 1237700394480
ИНН/КПП 9707001238/770701001

Тел. +7 985 923-09-90, email: info@x-labs.ru

XL Service FW

Техническое описание

Версия 1

11.10.2023

XL Service FW

Оглавление

1.1 Описание системы

1.1.1 XLSFW голосовй Firewall

XL Service Firewall (XLSFW) предоставляет расширенный активный сетевой файервол, способный фильтровать нежелательные типы вызовов из сети клиента. Он использует прямой интерфейс с корпоративной или телефонной сетью общего пользования для получения информации обо всех ожидающих вызовах, а также для применения определенных действий в отношении вызовов, определенных как мошеннические или спам-сообщения. XLSFW обеспечивает защиту в режиме реального времени, основанную на анализе параметров вызова в режиме онлайн и информации, полученной для вызова по сигнальному INVITE или IDP-сообщению.

Обнаружение проблемных вызовов осуществляется на модуле rule engine, который использует сложные алгоритмы для определения правил, которые могут определять для каждого вызова, должен ли он быть разрешен или нет. Правила могут быть сконфигурированы с использованием гибкой логики, позволяющей использовать все параметры вызова, сравнивать со списками номеров или результатами аналитики, которая отслеживает статистическое поведение отдельных вызывающих или вызываемых номеров. Каждое правило определяется одним или несколькими фильтрами, которые выполняются для каждого вызова, и в случае, если этот вызов соответствует условиям фильтрации, к вызову применяется действие, определенное для соответствующего правила. Если вызов не соответствует ни одному из определенных правил, он обрабатывается операцией «continue» без каких-либо изменений в его потоке.

Кроме того, модуль аналитики получает и обрабатывает информацию обо всех инициированных вызовах, а также, при необходимости, информацию о ходе выполнения вызова. Эта информация обрабатывается специализированной аналитической моделью, позволяющей выявлять и блокировать различные сценарии мошенничества.

1.1.2 XLSFW SMS Firewall

Модуль XLSFW SMS Firewall способен оценивать и фильтровать входящий трафик сообщений в режиме реального времени, с последующей блокировкой мошеннических сообщений P2P и A2P в зависимости от типа SMS-трафика (например, национальный, международный, ESME и т. д.). Система также использует офлайн-анализ для обнаружения случаев мошенничества и выявления моделей мошеннического поведения, что может помочь создать эффективные правила мошенничества с SMS, которые затем можно будет применять к сообщениям в режиме реального времени.

Наблюдая за полным потоком вызовов, XLSFW собирает все атрибуты сообщения, полученные из исходящей мобильной части, а также из мобильной завершающей части, а также содержимое SMS-сообщения. Такой широкий спектр собираемых и отслеживаемых атрибутов обеспечивает основу для полной видимости технологического процесса и установления эффективного контроля SMS-трафика.

1.2 Архитектура системы

1.2.1 Основные системные модули

XLSFW — это автономная система предотвращения мошенничества в сфере телекоммуникационных услуг в режиме реального времени, которая управляется с помощью следующих модулей:

- XLSIG: модуль сетевого интерфейса.
- XLSTATE: модуль обработки состояния аналитики в реальном времени.
- XLRTA: приложение для обработки аналитических профилей в режиме реального времени.
- XLAPI: модуль API для carrier interworking.
- XLMON: модуль мониторинга системы.

1.2.2 XLSFW Voice Firewall

Конфигурация ключевых системных модулей для настройки voice firewall представлена на схеме ниже:

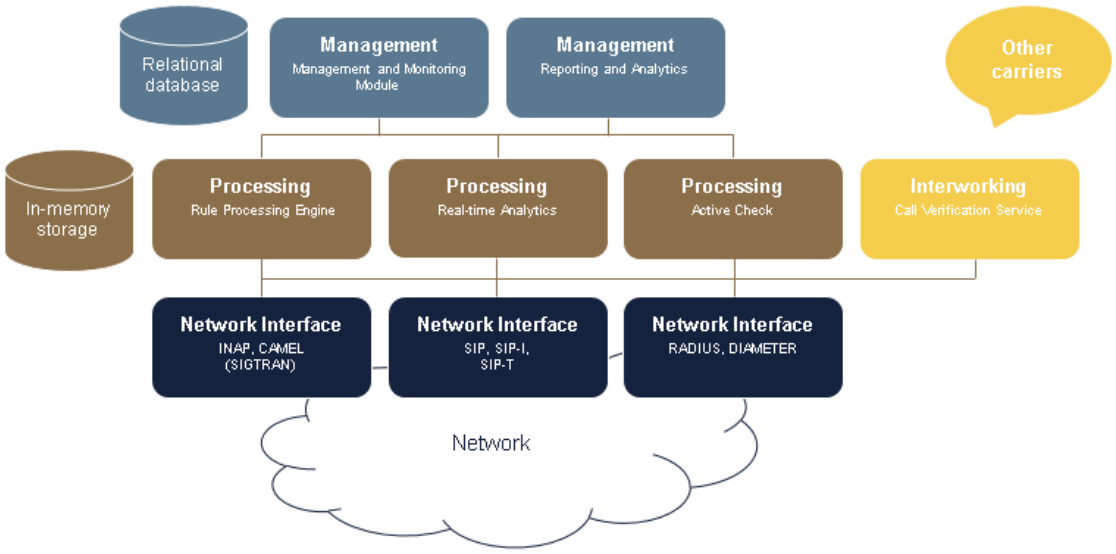

*Рисунок **Ошибка! Текст указанного стиля в документе отсутствует.**.1: Логическая схема XLSFW Voice Firewall*

1.2.3 XLSFW SMS Firewall

Конфигурация ключевых системных модулей для настройки SMS firewall представлена на схеме ниже:

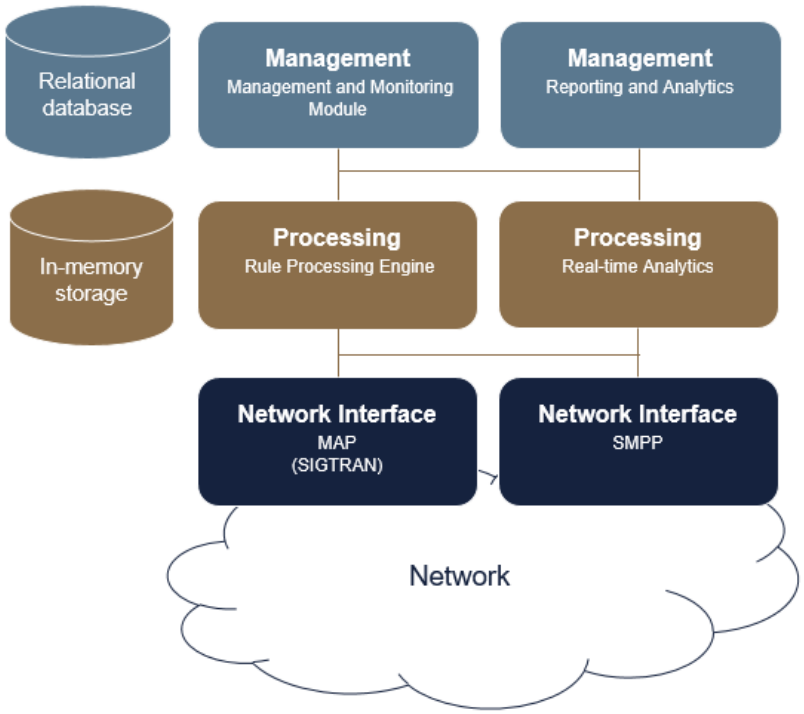

*Рисунок **Ошибка! Текст указанного стиля в документе отсутствует.**.2: Логическая схема XLSFW SMS Firewall*

1.3 Интеграция системы

1.3.1 Интеграция системы XLSFW в телекоммуникационную сеть

Ниже приведена общая схема сетевых интерфейсов и включенных в них систем.

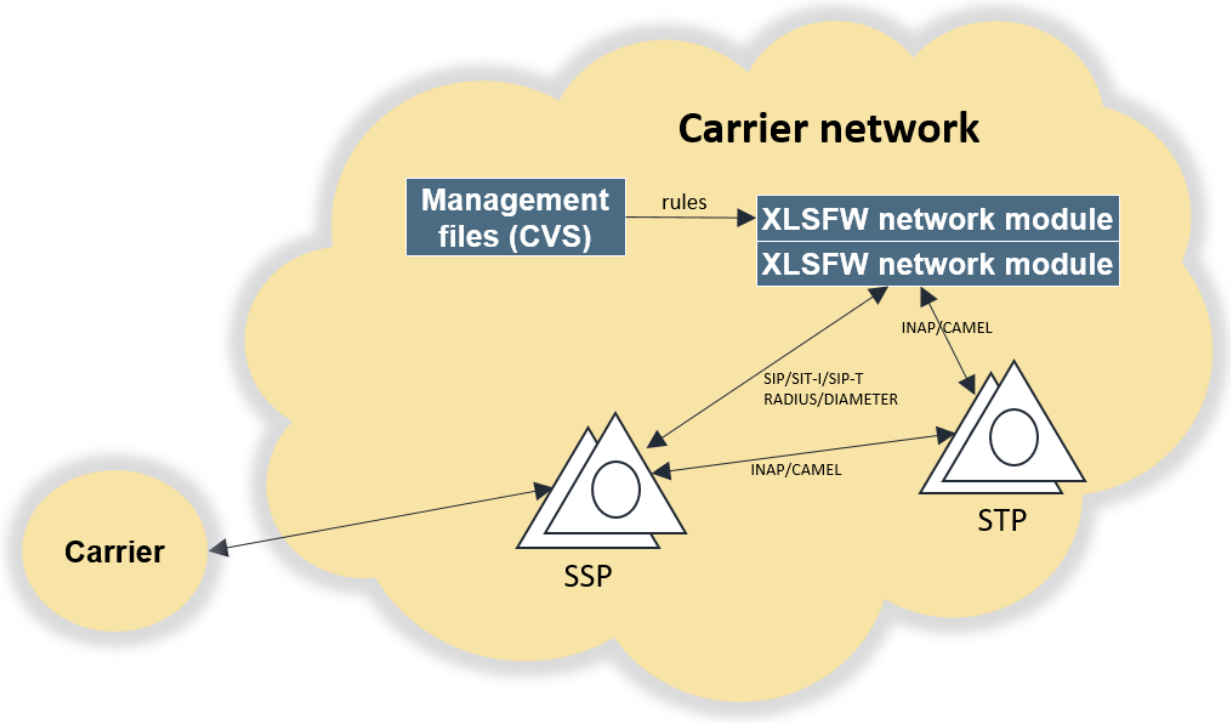

*Рисунок **Ошибка! Текст указанного стиля в документе отсутствует.**.3: Интеграция системы*

XLSFW предоставляет гибкие возможности интеграции::

- SS7 CAMEL/INAP SCP через SIGTRAN
- SS7 MAP/CAMEL/INAP proxy или B2BUA через SIGTRAN
- SIP/SIP-I redirect
- SIP/SIP-I/ISC SIP proxy или B2BUA

XLSFW основан на обработке запросов, полученных по протоколу MAP, INAP или CAMEL, с использованием интерфейса SIGTRAN или SIP/SIP-I/SIP-T. Система анализирует каждый вызов перед его установкой, чтобы определить, следует ли обрабатывать данный вызов иным образом, определенным фрод сценарием (то есть проверяется необходимость применения каких-либо действий/запретов к данному вызову).

В случае интерфейса INAP/CAMEL через SIGTRAN интерфейс как правило устанавливается с помощью STP, чтобы упростить интерфейс с несколькими коммутаторами с дополнительными ассоциациями, тем не менее система также может подключаться к коммутаторам напрямую.

Информация о сети в дополнение к стандартным параметрам MAP/INAP/CAMEL, необходимым для корректного предотвращения интерконнект фрода, также требует информации о входящем операторе. Входящий оператор идентифицируется в системе с помощью service key или других параметров SS7, которые необходимо настроить либо для уникальной идентификации конкретного оператора, или отдельной группы транков, принадлежащей оператору в случае, если сценарии должны различаться между разными группами транков.

В случае интерфейса SIP/SIP-I/SIP система может быть сконфигурирована для работы либо как SIP-переадресация, либо как SIP-прокси-сервер. В обоих случаях информация об операторе является оценкой параметров SIP.

Используя указанный интерфейс, XLSFW обрабатывал следующие основные типы потоков вызовов:

- CAMEL/INAP позволяющий обрабатывать операции IDP
- Интерфейс MAP, обеспечивающий доступ к отчетам SRI4SM, FSM и о доставке SMS.
- SIP-интерфейс, позволяющий обрабатывать поток голосовых вызовов и поток SMS-сообщений через IP.

1.3.2 Интеграция с внешними системами

Система обеспечивает простую интеграцию с другими ИТ-системами через открытую базу данных, веб-службу SOAP и FTP-интерфейсы передачи файлов.

Интерфейсы позволяют в первую очередь:

- Импорт данных списка номеров из внешних источников.
- Интерфейс автоматического включения номеров, включенных в списки номеров.
- Доступ к данным событий и сеансов из/к внешней системы.
- Интерфейс с корпоративной системой мониторинга через SNMP для мониторинга состояния системы.

1.4 Описание возможностей обработки XLSFW

XL Service Firewall (XLSFW) обеспечивает предотвращение несанкционированного трафика в реальном времени, предоставляя интерфейсы управления вызовами в реальном времени в базовой сети. Логика обнаружения мошенничества основана на использовании правил. Каждое правило включает набор фильтров и определяет действие. Каждый фильтр предоставляет набор условий для сопоставления с входящим вызовом. Если для анализируемого звонка выполняются условия фильтра, система выполняет действие, определенное в соответствующем правиле. Полная обработка в реальном времени выполняется на этапе установления вызова.

1.4.1 Логика обработки в реальном времени

Такая конфигурация, тесно связана с логикой обработки в реальном времени:

В сеть поступает новый звонок или новое SMS-сообщение. В случае голосового вызова первый входящий оператор определяется на основе номера. На основе входящего оператора определяется уникальный service key для конкретного оператора. На основе service key система определяет категорию оператора. На основе категории оператора определяется раздел правил (группа правил, связанных с категорией оператора); в случае, если категория оператора связана с несколькими разделами правил, они обрабатываются один за другим в том же порядке, который указан в файле конфигурации.

Аналогично, в случае SMS раздел правил определяется на основе определения источника направления (global title) SMS-сообщений, используемых для определения типа SMS-трафика (например, национальные/международные MNOS, организации ESME, учетные записи LA и т.д.).

Кроме того, каждый раздел правил обычно включает в себя набор из нескольких правил, и каждое правило обычно включает в себя набор фильтров. Оба фильтра и правила обрабатываются один за другим в том же порядке, который указан в файле конфигурации (rules.csv). В рамках правила система обрабатывает все определенные фильтры от первого до последнего, за одним исключением: в случае, если набор фильтров включает фильтр типа “ check point”, система прекращает обработку фильтров для соответствующего правила в этой точке и продолжает обработку следующего правила.

Таким образом, когда раздел правил определен для входящего вызова, система сначала анализирует первый фильтр, который определен для первого правила. Этот анализ выполняется путем сравнения параметров вызова с условиями фильтрации. Как правило, первый фильтр всегда имеет тип “include”. Если параметры вызова соответствуют первому фильтру (“include”), это условие включает вызов приложения rule. С другой стороны, если параметры вызова не соответствуют первому фильтру (“include”), это условие не включает вызов приложения rule. В любом случае система продолжает анализ второго фильтра. Если фильтр имеет тип “include” и параметры вызова соответствуют второму фильтру, это условие включает вызов приложения rule. Если фильтр имеет тип “исключить” и параметры вызова соответствуют второму фильтру, это условие исключает вызов из применения правила. Если

параметры вызова не соответствуют второму фильтру (типа “include” или “exclude”), это условие не включает вызов приложения rule. Таким образом, система продолжает анализ всех фильтров, определенных для правила, от первого до последнего* в том же порядке, который указан в файле конфигурации (rules.csv), который, наконец, выдает ответ, соответствует ли вызов соответствующему правилу или нет. Если да, то к вызову применяется действие правила. Если нет, то обработка продолжается с анализом следующего правила. Если ни одно из правил не соответствует вызову, то вызов обрабатывается без какого-либо вмешательства системы.

*Примечание: Однако есть одно исключение из этой логики, и это случай, когда в набор фильтров, определенных для правила, включен фильтр типа “check point”. В таком случае система прекращает анализ фильтров на этом этапе, решение о том, соответствует ли вызов соответствующему правилу или нет, зависит от анализа фильтров перед фильтром “check point”, и система переходит к анализу следующего правила в строке.

1.4.2 Проверка

Правила могут включать метод активной проверки, при котором запрашиваются внешние ресурсы для получения дополнительной информации о процессе вызова или абоненте, включенном в вызов. Затем на основе результата запроса определяется необходимое действие.

Для активной проверки вызовов перед настройкой вызова поддерживаются следующие методы:

- HLR Check: определение текущего зарегистрированного местоположения абонента, статуса роуминга, местоположения и т.д.;
- Call back: предотвращение спам-атак, генерируемых машиной, путем идентификации и подтверждения того, что вызывающий абонент не является машиной (на основе использования меню IVR);
- IVR: предотвращение спам-атак, генерируемых машиной, путем идентификации и подтверждения того, что вызывающий абонент не является машиной (на основе использования меню IVR);
- State server: определение статуса обработанного вызова во внешней справочной системе (сервер состояний), которая собирает и агрегирует связанные с вызовом данные о выбранных недавних событиях за определенный пользователем период.

В алгоритме обработки есть специфика на случай правил, требующих активной проверки. В таком случае обработка правил продолжается от первого правила до последнего, определенного для соответствующего раздела правил, однако никакие действия не применяются до получения результатов активной проверки. Это значительно сокращает время обработки.

Затем, основываясь на результатах активной проверки, система определяет первое правило, соответствующее вызову, и применяет к правилу соответствующее действие. Если по результатам активной проверки система определяет, что ни одно из правил не соответствует вызову, то вызов обрабатывается без какого-либо вмешательства системы.

XL Service FW

1.5 Последовательность логики обработки в реальном времени

XLSFW анализирует вызовы в режиме реального времени, чтобы определить адекватный ответ системы и обработать вызов или сообщение в соответствии с настроенными правилами. Реакция может быть определена на основе результатов, полученных в результате следующих типов обработки в режиме реального времени:

- Немедленный ответ на основе настроенных правил: вызов или сообщение отслеживаются в режиме реального времени, и системное действие определяется на основе:
  - Оценка всех параметров вызова
  - Поиск списков номеров, в справочнике ФАС и справочнике данных о портированных номерах
  - Оценка настроенных правил для определения того, следует ли применять действие

- Использование методов активной проверки для определения ответа: конкретные данные, относящиеся к вызовам и сообщениям, собираются на сервере состояния и запоминаются на короткое время, а затем определяется ответ системы на основе сравнения фактических данных вызова / сообщения с совокупностью данных:
  - Запросить внешние ресурсы (State server) для получения дополнительной информации о вызове процесса или абоненте, включенном в вызов
  - Используйте результат запроса для определения необходимого действия

- Ответ, основанный на результатах аналитики в режиме реального времени: конкретные данные о вызове проверяются непосредственно в сети, и системное действие определяется после сравнения фактических значений с предопределенными целевыми значениями:
  - В соответствии с определенными сценариями аналитические параметры рассчитываются по необходимым категориям в режиме реального времени (обновляются при каждом звонке/сообщении).
  - Система сверяет аналитические значения с заданными целевыми значениями и определяет необходимые действия на основе этого результата

- Проверка вызова с помощью carrier interworking:
  - Использование проверки происхождения для проверки того, действительно ли вызов с полученным вызывающим номером был зарегистрирован в домашней сети.
  - Использование проверки завершения звонка для защиты вызова путем использования выделенного временного номера маршрутизации при его передаче.

