ПРОТЕЙ ТЕХНОЛОГИИ

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

Версия документа
от 04.07.2025

ПРОТЕЙ-SBC. Отвечаем на ваши вопросы о пограничном контроллере сессий

ПРОТЕЙ-SBC (SBC) — это один из передовых пограничных контроллеров сессий в России. Быстро развивающийся программный продукт линейки ПРОТЕЙ востребован во всех сегментах рынка. SBC — это firewall для телефонии. Контроллер является ключевым элементом IP-сети для защиты NGN/IMS-сетей и обладает широким спектром дополнительных функций. Его основные функции — защита сети от несанкционированного трафика и различного рода атак, устранение проблем совместимости оборудования.

SBC повышает надежность и отказоустойчивость сети, анализирует полученную информацию, решает задачи, связанные с управлением вызовами, выполняет транскодирование трафика, процедур коммутации. Кроме того, контроллер упрощает конфигурирование и администрирование, взаимодействие разнородного VoIP-оборудования, обеспечивает безопасность внутренней сети оператора.

Продукт зарегистрирован в реестре отечественного ПО.

ПРОТЕЙ ТЕХНОЛОГИИ

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

Версия документа
от 04.07.2025

Поддерживаются ли в рамках продукта SBC операционные системы РЕД ОС и Astra Linux?

В рамках продукта и решения SBC мы чаще всего взаимодействуем с RPM-based операционными системами. В первую очередь это замена CentOS – OEL 8. При развертывании гипервизора обычно выбираем Ubuntu в качестве хостовой машины, а гостевые ОС - именно на базе RPM (тот же OEL8), из отечественных к нему ближе всего РЕД ОС 7, но сейчас он не применяется нами в коммерческих инсталляциях. В процессе разработки и в поставках мы используем Astra Linux. При выходе новых патчей безопасности ОС мы проводим регрессионное и нагрузочное тестирование на целевых ОС. Поскольку рынок диктует свои правила, у нас также есть инсталляции на ALT Linux в B2G сегменте рынка. Под такие ОС тестирование продукта выполняется по запросу.

Какие протоколы поддерживаются и есть ли WebRTC?

Мы поддерживаем протоколы SIP/SIP-I/T/H323, RTP/SRTP/RTCP, UDP/TCP/TLS транспорт, SSH, SNMP, NTP, HTTP API. STUN, TURN и ICE поддерживаются в рамках WebRTC режима работы. Протокол H323 поддерживается без RAS, то есть нет встроенного гейткипера, и мы взаимодействуем с удаленным оборудованием как с транками H.323. Мы также работаем с MOS/R-Factor для оценки качества речи в вызовах.
В наших планах реализация протокола SIPREC, но существует альтернативный вариант. В случае, если не требуется интегрироваться с системой записи переговоров, наш интерфейс отчетности CDR Viewer позволяет аналогично SIPREC выполнять выборочную запись вызовов в формате pcap для прослушивания их, просмотра сигнализации в Wireshark и других подобных операций.

WebRTC поддерживается. Наш API не очень обширен, но основные функции реализованы, такие как трансфер вызова, ожидание второго вызова и базовые сценарии. Эти функции, в частности, используются у нас в ПРОТЕЙ-Юником (UC) и в видеоконференцсвязи (ВКС).

Можно ли получить протокол тестирования безопасности и какие атаки он позволяет отразить? Проводились ли Virt-тесты?

Мы можем предоставить такой протокол. Существуют стандартные тестировщики на уязвимости и есть RFC 4475, который называется SIP Torture Test Messages.

В соответствии с жизненным циклом продукта, мы достаточно часто выпускаем релизы, в рамках которых мы проводим эти тесты. Существуют различные варианты проверки системы: во-первых, это различные генераторы трафика по типу IXIA, во-вторых, известная операционная система Kali Linux. С Kali Linux мы взаимодействуем: у нас существует отдельная среда с автотестами, с контейнерами этой операционной системы, которые проверяют на уязвимости и различные виды атак.

Virt-тесты да, проводились.

ПРОТЕЙ ТЕХНОЛОГИИ

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

Версия документа
от 04.07.2025

Вопрос по безопасности: есть ли возможность использовать различные сертификаты под разные транки, клиенты, интерфейсы, проверка сертификатов второй стороны, L7-инспекция на основе сигнатур?

В релиз, который вышел в марте, добавляется поддержка разных сертификатов. Это новый функционал, который как раз приходит к нам с TLS 1.3. То есть в Interconnect SBC он уже поддержан, сейчас дорабатывается в Collocated SBC.

Могут быть доступны два режима на одном SBC для стыков и оконечных устройств?

Да, доступны.

Существует ли возможность дешифрования трафика и транскодинг?

Возможность дешифрования трафика и транскодирования существует и может быть выполнена в рамках одной сессии. Есть сценарии применения, когда SBC используется для интеграции оконечных терминалов, например, оборудование Cisco ведет себя иначе, чем Yealink. SBC может предоставлять внешний интерфейс TCP/TLS, чтобы обеспечить хорошую интеграцию с оборудованием Cisco или быструю переключаемость на резервную АТС или другой SBC. Во внутренней сети SBC использует протокол UDP, чтобы обеспечить корректную работу сервисных платформ и АТС.

Вы предоставляете OID или trap, или все вместе в протоколе SNMP?

Мы предоставляем возможность использования OID и trap в рамках протокола SNMP. Мы поддерживаем версии 1, 2 и 3 протокола SNMP, хотя версии 1 и 2 не являются самыми безопасными. Мы также поддерживаем более защищенную версию V3. Обычно мы используем активный опрос OID для получения статистической информации, но также отправляем trap в случае аварийных событий, например, при обнаружении активности транка.

Будет ли front и back как у Cisco? И могут ли подключаться телефоны Cisco с нативной прошивкой через SBC с сохранением автопровижининга и различных функций ДВО?

В наших планах есть подобная реализация. С точки зрения информационной безопасности мы закрываем доступ к операционной системе, чтобы всё управление системой выполнялось через GUI. Соответственно, это позволяет настроить IP-адрес, NTP-сервер для точного времени и выполнить какие-то служебные функции из единого интерфейса.

Если речь идет о SIP-прошивке, то это возможно. В нашей АТС есть функция провижининга Cisco-терминалов. Сейчас мы рассматриваем доработку мигратора, который будет извлекать старые настройки телефона с предыдущей АТС (CUCM) и гибко переносить на нашу новую АТС. Таким образом, можно быстро и бесшовно перенести настройки терминалов Cisco.

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

Версия документа
от 04.07.2025

Полная настройка SBC проводится через веб-интерфейс или какой-то функционал настраивается через командную строку?

Функции, которые относятся непосредственно к самому функционалу SBC, мы реализовали и в CLI, и полностью поддержали в веб-интерфейсе. Это, например, касается SIP-интерфейсов, управления MCU — теми компонентами, которые обрабатывают голосовые потоки и так далее.

Сейчас средствами ПО SBC мы не можем поднимать на сетевых интерфейсах сетевой карты IP-адреса, не можем указать дефолтный шлюз на сервере.

В дальнейшем мы будем переносить в графический интерфейс GUI работу с бэкапами, а также работу с выгрузкой логирования логов. Так, если потребуется журнал логирования системы за период возникновения ошибки или какой-то сложности, это можно будет выполнить в веб-интерфейсе, выгрузить и отправить в техподдержку. Также мы планируем добавить управление сетевыми интерфейсами, чтобы можно было полностью все настроить через GUI.

Лицензии на 25 одновременных сессий — это вызовы или регистрации?

У нас есть профиль трафика, который мы пересчитываем на количество абонентов. Мы используем емкостные лицензии на основании количества сессий: одна сессия — один вызов.

Какое оборудование из ВКС-терминалов тестировалось для подключения извне и существует ли поддержка видеокодеков?

Тестировались широко распространенные Polycom терминалы. Конечно, мы тестировали ПРОТЕЙ-ВКС собственной разработки и сборки. Наши ВКС установлены во многих организациях.

Поддержка видеокодеков существует, но мы не транскодируем видео. Есть возможность маркирования трафика метками QoS/DSCP. При необходимости, на базе медиапрофилей можно менять/заявлять другие кодеки, тем самым выполняя пересогласование параметров медиа. В данном случае мы придерживаемся позиции, что у нас есть свой ВКСС (видеоконференц сервер), который как раз полностью занимается микшированием всех потоков. И в этом плане мы ему не составляем конкуренцию.

Можно ли построить Call Flow (маршрут вызова) между двумя абонентами, обозначенными как плечо A и плечо B?

У нас реализованы хорошие журналы логирования в текстовом виде, для просмотра необходимо зайти в консоль. Есть отдельные компоненты, трассировщики, которые могут построить Call Flow. Например, в CDR Viewer мы можем записывать вызовы по типу SIPREC и выгружать dump.pcap в Wireshark, где есть встроенный функционал Call Flow.

Мы разрабатываем единую платформу веб-интерфейсов для упрощения конфигурирования АТС и

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

SBC без необходимости дополнительных манипуляций в будущем. Учитывая требования к информационной безопасности, в платформе будет предусмотрен централизованный трассировщик, который позволит просматривать Call Flow.

Этот трассировщик будет? Сейчас есть какие-то инструменты онлайн трассировки с визуализацией, помимо логов и CDR?

Есть трассировщики, но они требуют наличия программы Wireshark. Мы пишем записи вызовов - dump-ы в формате Wireshark.

Позволяет ли мигратор использовать парк телефонов Avaya серии J?

В настоящее время у нас отсутствует поддержка провижининга телефонов Avaya серии J. Однако этот функционал включен в дорожную карту развития нашего продукта и запланирован на первое полугодие 2024 года. Мы успешно поддерживаем другие серии телефонов Avaya по мере необходимости.

Для работы SBC требуется наличие отдельной демилитаризованной зоны (DMZ)?

DMZ нужна в зависимости от того, что мы будем подключать и каким образом. Возможно подключать операторов колл-центра через пользовательские VPN без привлечения SBC. Такой подход становится возможным при условии отсутствия сложностей с VPN и обеспечивает надлежащий уровень безопасности инфраструктуры заказчика. Но это не решает вопросы дополнительных мер защиты (от того же DoS), а также усложняет эксплуатацию сети.

Кроме того, при необходимости запрета доступа из области DMZ можно инсталлировать компоненты таким образом, чтобы доступ осуществлялся через публичный адрес SBC. Однако при этом важно учитывать, что, например, при использовании WebRTC, клиенты должны получить STUN-сервер, то есть сами контактные данные SBC для установки WebRTC-сессии, включая передачу сигнального трафика через DTLS протокол. Это также требует соответствующей настройки NAT на сетевом оборудовании, если предпочтительно не открывать прямые сетевые порты или не передавать данные в публичный доступ из соображений безопасности. На SBC реализованы механизмы работы за статическим и динамическим NAT.

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

Версия документа
от 04.07.2025

О компании ПРОТЕЙ Технологии

Компания ПРОТЕЙ Технологии входит в российский IT-холдинг ПРОТЕЙ и занимается реализацией программно-аппаратных продуктов для корпоративного сегмента рынка. ПРОТЕЙ ТЛ предлагает решения для создания и модернизации корпоративной связи на предпри- ятиях из сферы объединённых коммуникаций, телефонии, ВКС-систем и системы управления и мониторинга инфраструктуры предприятий. Решения ПРОТЕЙ разработаны в полном соответствии с международными стандартами и отвеча- ют всем современным требованиям, предъявляемым к объединённым корпоративным коммуни- кациям.