



ESBC-31

Пограничный контроллер сессий ESBC-31



Описание

Пограничный контроллер сессий ESBC-31 — компонент VoIP-сети, участвующий в процессе обслуживания вызова в качестве пограничного контроллера сессий. Устройство обеспечивает нормализацию сигнального протокола, защиту сети оператора от несанкционированного доступа и различных атак. Используется на границах IP-сетей:

- между сетями операторов связи;
- между сетью оператора и корпоративной сетью клиента;
- между сетью оператора и публичной сетью.

ESBC обеспечивает защиту сети оператора от несанкционированного доступа. Инструментами для обеспечения безопасности служат интеллектуальное управление доступом и скрытие топологии сети. Использование ESBC позволяет предоставить доступ в операторскую или корпоративную сеть из внешней недоверенной сети, обеспечивая защиту коммерческих интересов компании. Пограничный контроллер сессий ESBC-31 от Eltex могут использоваться для импортозамещения брендов Cisco, Avaya, Yealink, Grandstream, Fanvil, Polycom в области телекоммуникационного оборудования, где отсутствует техническая поддержка на русском языке и лицензирование. Пограничный контроллер сессий ESBC-31 вы можете купить, обратившись к нашим менеджерам. Также, вы можете получить консультацию наших квалифицированных сетевых инженеров, специалистов по серверному оборудованию и других специалистов технического отдела. Мы работаем по всей территории России. Если вам необходимо купить пограничный контроллер сессий ESBC-31 в Москве, Санкт-Петербурге, Новосибирске, Екатеринбурге, Казани, Владивостоке, Краснодаре, Самаре, Омске и других городах, мы будем рады помочь вам в этом. Другие пограничные контроллеры сессий Eltex:

- Программный пограничный контроллер сессий vESBC
- SBC-1000
- SBC-3000
- ESBC-3200
- ESBC-3350

Характеристики

Интерфейсы

Ethernet 101001000BASE-T (RJ-45)	8
Ethernet 1000BASE-X (SFP)	6
10GBASE-R (SFP+)1000BASE-X (SFP)	2
Последовательный порт RS-232	3
Консольный порт RS-232 (RJ-45)	1
USB 2.0	1
USB 3.0	1
Слот для microSD-карт	1
Нагрузка	До 800 одновременных вызовов
CPU	4
RAM	4 ГБ DDR4
Flash-память	8 ГБ eMMC
Максимальная потребляемая мощность	44 Вт
Питание	100–240 В AC, 50–60 Гц; 36–72 В DC До двух источников питания с возможностью горячей замены
Интервал рабочих температур	От -10 до +45 °C
Интервал температуры хранения	От -40 до +70 °C
Относительная влажность при эксплуатации	Не более 80 %
Относительная влажность при хранении	От 10 до 95%
Габариты (Ш ? В ? Г)	430 ? 44 ? 275 мм
Масса	3,425 кг
Срок службы	Не менее 15 лет

Функциональные возможности

- Обеспечение безопасности сети оператора связи
- Трансляция публичных IP-адресов
- Гибкое распределение резервных маршрутов
- Поддержка SIP-абонентов
- Анализ и верификация SDP
- Гибкое распределение вызовов на основе правил
- Модификация SIP-заголовков с помощью регулярных выражений PCRE
- Поддержка гибкой маршрутизации вызовов
- Маршрутизация на группу направлений с поддержкой логики балансировки (RR и WRR)
- Поддержка динамического режима работы транков через DNS, RADIUS
- Поддержка перемаршрутизации при неудачном вызове (контроль по кодам ответов SIP)
- Поддержка обработки ответов 3XX для управления перенаправлением вызовов
- Контроль доступности направлений по OPTIONS
- Контроль установленных сессий:
- по наличию RTP/RTCP
- с использованием таймеров сессии (RFC4028)
- Хранение и восстановление записей о зарегистрированных абонентах в БД
- Транскодирование/проксирование медиа (аудио и видео)
- Поддержка WebRTC+ICE для браузерных приложений
- Поддержка QoS (назначение Diffserv) для SIP и RTP
- Запись биллинговой информации в CDR-файл, параллельная запись CDR-файла на локальный носитель и удаленный сервер (FTP, SFTP, SCP)
- Поддержка аутентификации:
- аутентификация регистраций абонентов через RADIUS
- локальное хранение данных аутентификации
- регистрация транков в режиме клиента на вышестоящей IP ATC
- Поддержка транзита ISUP (SIP-I/SIP-T)
- Поддержка туннелирования PPTP и L2TP over IPsec для передачи SIP и медиатрафика
- Поддержка функции ротации номеров (Cg/CdPN) при осуществлении исходящих вызовов
- Использование тегов сессии для повышения гибкости при маршрутизации/модификации SIP-сообщений
- Управление параметром Expires для контроля абонентов и защиты от перегрузок
- Поддержка механизмов управления регистрациями абонентов:
- принудительная разрегистрация;
- принудительная перерегистрация.

Обход NAT

Функция, необходимая для обеспечения прозрачности IP-сетей для голосового и видеотрафика.

- поддержка режима nat-comedia
- поддержка Public-IP
- поддержка работы через удаленный STUN-сервер
- локальный STUN-сервер
- поддержка "sip.instance" и "reg-id" (RFC5626)

Безопасность

ESBC обеспечивает защиту сети оператора от несанкционированного доступа. Инструментами для обеспечения безопасности служат интеллектуальное управление доступом и скрывание топологии сети. Использование шифрования сигнализации SIP и медиапоток обеспечивает конфиденциальность и безопасность передаваемых данных.

- динамический брандмауэр
- защита от SIP-флуда
- защита от SIP-spoofing атак
- блокировка по AOR, User-Agent
- блокировка по содержимому SIP-сообщения
- поддержка шифрования сигнализации (TLS) и медиапоток (SRTP SDES, DTLS-SRTP)
- реализован функционал выгрузки событий информационной безопасности в сторонние SIEM-системы в режиме реального времени

Контроль трафика

ESBC позволяет управлять количеством входящих и исходящих SIP-запросов в зависимости от направления:

- управление количеством установленных сессий, ограничение входящих/исходящих CPS, RPS
- поддержка дополнительных ограничений (rps, regps, session pps и др.)

Сокрывание топологии сети

ESBC используется для предоставления доступа в операторскую или корпоративную сеть из внешней недоверенной сети, обеспечивая защиту коммерческих интересов компании.

Поддерживаются следующие механизмы:

- интеллектуальная трансляция IP-адресов для сигнального и медиатрафика
- полноценный B2BUA для обеспечения требуемого уровня изоляции сетей

Мониторинг

- Мониторинг устройства по SNMP, отправка SNMP-трапов при авариях
- Просмотр информации о зарегистрированных абонентах
- Мониторинг состояния транков
- Построение SIP Call Flow Diagram
- Просмотр и управление установленными соединениями
- Просмотр и управление белым/черным списками
- Статистика CPS, RPS
- Статистика SIP-сообщений
- Утилита Sngrep
- Мониторинг параметров трафика (KPI):
 - активные вызовы
 - средняя длительность вызова (ACD)
 - входящие/исходящие попытки вызова
 - количество зарегистрированных абонентов/контактов

Протоколы сигнализации

- SIP

Функциональность протокола SIP

- RFC-3261
- RFC-3264 (Offer/Answer)
- RFC-3311 (Update Method)
- RFC-4566 (SDP)
- RFC-1889 (RTP)
- RFC-2833 (Telephone Event)
- RFC-3515 (Refer Method)
- RFC-3265 (Subscribe)
- RFC-6086 (INFO Method)
- RFC 7118 (WebSocket)

- RFC 8445 (ICE) кроме STUN/TURN
- RFC 5768 (ICE SIP)
- RFC 8839 (SDP ICE)
- B2BUA peering
- RFC 4028
- RFC 5168
- RFC 3489 (Classic STUN)
- RFC 8489 (STUN)
- RFC 5626

Медиапротоколы

- RTP
- RTCP
- SRTP (SDES, DTLS)

Транспортные протоколы

- TCP
- UDP
- TCP/UDP interworking
- TLS
- WS/WSS

Сетевые протоколы

- IPv4
- IPv6

Поддерживаемые видеокодеки (в режиме транскодирования)

- H.263-1998
- H.264
- VP8
- VP9

Резервирование

Применение схемы кластерного резервирования и дублированных источников электропитания обеспечивает полноценное резервирование:

- отказоустойчивый кластер в режиме облегченного резерва по схеме 1+1
- простота администрирования и интеграции: синхронизация конфигураций, времени, версий; Zero Touch Provisioning (ZTP)

Безопасность

- Защита от DoS
- Защита от VoIP-атак

Передача факса

- T.38
- G.711

Поддерживаемые аудиокодеки (в режиме транскодирования)

- G.711 (a-law, µ-law), G.729, G.722, G.726, iLBC, opus, speex, AMR, GSM, L16-mono

Управление

- MML-консоль (SSH/Telnet)
- Web-интерфейс2
- Консольный порт RS-232 (RJ-45)