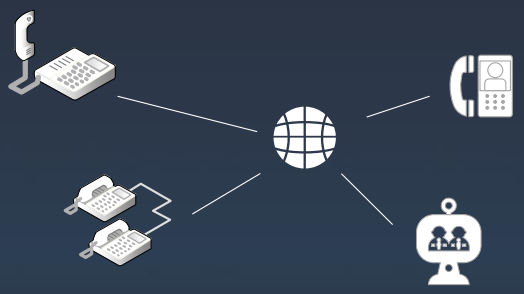
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



Применение InfoDiode для организации передачи трафика IP-телефонии

Применение однонаправленных каналов передачи данных позволяет существенно повысить безопасность защищаемого сегмента сети, делая принципиально невозможным проведение большинства типов удалённых атак на ИТ-инфраструктуру. Однако некоторые взаимодействия, например, с применением протокола телефонной сигнализации SIP, принципиально работают только при передаче данных в обоих направлениях. Наличие двунаправленного обмена повышает риски компрометации данных, нарушения целостности данных, а также риски информационной безопасности в целом. Несмотря на сохранение рисков организации эффективных векторов атак на базе двунаправленного взаимодействия между сегментами сети, применение двух однонаправленных каналов в ряде случаев считается компромиссным как с точки зрения удобства обмена информацией, так и с точки зрения построения комплексной эффективной системы противодействия кибератакам.

С целью минимизации рисков эксплуатации злоумышленником двунаправленных каналов связи между доверенным и недоверенным сегментами и рисков обхода соответствующих программных средств защиты целесообразно рассматривать использование аппаратных средств защиты, передающих физический сигнал и информацию только в одном направлении, и гарантирующие изоляцию защищаемого сегмента на физическом уровне.

АМТ-ГРУП предлагает своим заказчикам продукты **InfoDiode**, построенные на принципах однонаправленной передачи данных, и позволяющие эффективно решать задачи обмена данными между сегментами сети с разным уровнем доверия. В частности, применение решений InfoDiode позволяет устанавливать мультимедийные сессии обмена данными (голосовая и видео связь), выполнять обмен документами и медиафайлами между защищаемым и менее доверенным сегментом или сетью. Такая схема обмена реализуется применением двух комплектов **InfoDiode** через которые настраивается передача протоколпротоколов телефонного взаимодействия. Решение позволяет организовать двустороннюю аудио- видео- связь, существенно повысив уровень защиты периметра сети.

115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.amt.ru
www.infodiode.ru

19.10.2023

Пример сценария применения InfoDiode при организации IP-телефонного взаимодействия

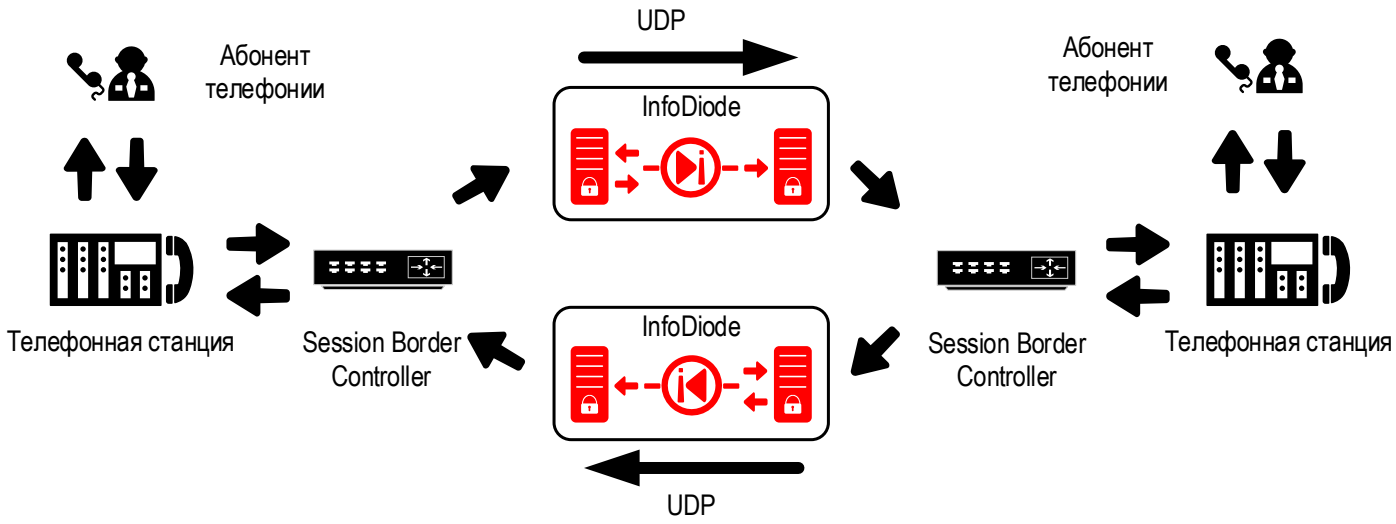
Установление аудио–, видео– телефонных соединений требует организации передачи данных как из защищаемого сегмента в менее доверенный, так и в обратном направлении. Для этого используются два комплекта **АПК InfoDiode PRO**, устанавливаемые разнонаправленно, в которых настроено туннелирование протокола UDP, который, в свою очередь, является транспортным протоколом для телефонного трафика.

В описываемом сценарии рекомендуется также использование специализированных устройств – контроллеров пограничных сессий (SBC, Session Border Controller), в задачи которых входит, в том числе, сокрытие топологии сети доверенного сегмента, что дополнительно повышает безопасность последнего и защищает от попыток изменить настройки оборудования.

В данном сценарии взаимодействие организовано между телефонной системой на базе CUCM (Cisco Unified Communications Manager) и системой управляемых совещаний IP FORUM собственной разработки АМТ-ГРУП. В роли каждой из них может выступать любая современная IP-телефонная станция, поддерживающая взаимодействие по протоколу SIP.

Для передачи телефонного трафика с помощью АПК InfoDiode PRO необходимо реализовать двунаправленную схему, в которой один базовый комплект АПК InfoDiode PRO будет отвечать за передачу UDP-трафика из защищённого сегмента наружу, а второй - за получение UDP-трафика из менее доверенного сегмента. При настройке правил UDP-туннелирования, в случае необходимости, можно ограничить передачу данных определенными сетевыми портами в соответствии с требованиями протокола SIP.

Следует учесть, что для обеспечения корректной работы протокола SIP необходимо на внешних интерфейсах АПК InfoDiode PRO сохранять в заголовках пакетов реальные IP-адреса телефонных устройств, исключая их подмену с помощью механизма трансляции (NAT, Network Address Translation). Это связано с тем, что содержимое SIP-пакетов также несет в себе информацию об адресах этих устройств. Сокрытие адресов выполняется средствами упоминаемых выше контроллеров пограничных сессий.



115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.amt.ru
www.infodiode.ru