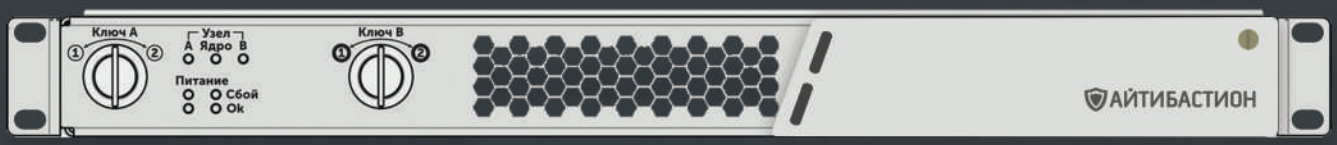
Синоникс

АЙТИБАСТИОН

Шлюз безопасного объединения изолированных сетей

Система позволяет организовать безопасный обмен информацией между узлами одной сети или разными сетями, предотвращая распространение киберугроз и вредоносного взаимодействия между ними.



ПЕРЕДАЧА ДАННЫХ

Передача данных между изначально ИЗОЛИРОВАННЫМИ сетями со встроенной защитой от атак транспортного уровня.

- TCP, UDP, в т.ч. однонаправленная
- Независимые политики для двух контуров
- Физическая блокировка передачи данных
- Скорость до 1 Гб/с

ПЕРЕДАЧА ФАЙЛОВ

Передача файлов между изначально ИЗОЛИРОВАННЫМИ сетями с проверкой этих файлов на соответствие политикам передачи.

- SFTP
- Проверка корректности ЭЦП, размера и маски файлов
- Внешняя валидация по ICAP (DLP, Sandbox, AV и др.)
- Автоматизация процесса доставки файлов

Ключевые возможности

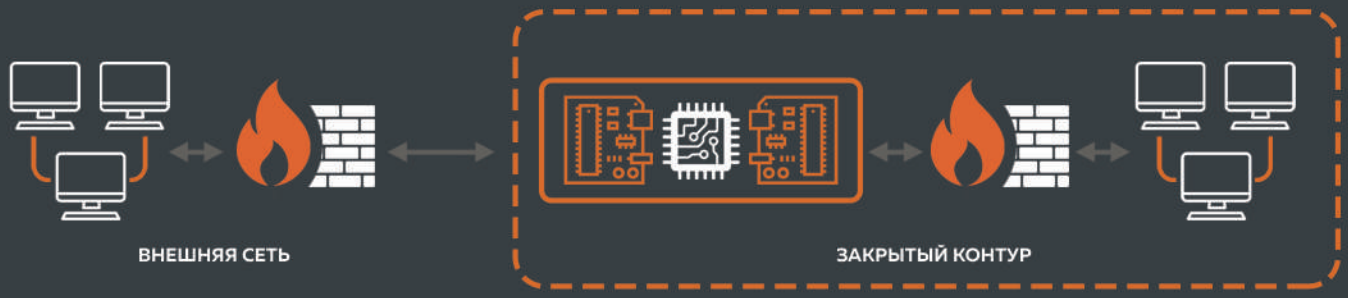
- **Изолирует сети**
  Архитектура и технологии решения обеспечивают контролируемую передачу данных и файлов без прямого объединения сетей. Поэтому две сети, объединенные через Синоникс, становятся невидимыми друг для друга.
- **Разграничивает зоны ответственности**
  Наличие двух встречных наборов правил передачи, а также двух специальных «пусковых» ключей позволяет разграничить зоны ответственности между сотрудниками объединяемых сетей.
- **Нейтрализует сетевые атаки**
  Встроенные технологии изоляции и обработки пакетов обеспечивают нейтрализацию сетевых атак на транспортном уровне и защиту закрытого контура.
- **Противодействует 0-day**
  Скрывает данные об изолированных сетях и информационных системах, а также ограничивает количество систем, которые могут получить доступ за пределами защищаемой сети. Устойчив к полной компрометации и изменению конфигурации.
- **Обеспечивает проверку файлов перед передачей**
  Проверяет наличие корректной ЭЦП, а также маски передаваемых объектов. Имеет встроенные механизмы дополнительной верификации объектов во внешних системах средствами ICAP-протокола.
- **Поддерживает контентную фильтрацию**
  Обеспечивается возможность установки устройства в цепочке сетевого оборудования для повышения качества фильтрации данных, в том числе средствами NGWF.

Принцип работы

Механизм

Синоникс основан на использовании технологии электронной передачи пакетов данных с применением разрешающих правил, установленных в явном виде. Они обеспечивают безопасный обмен данных и файлов в условиях физической изолированности сетей или сегментов одной сети. Правила задаются на каждом из двух Узлов устройства независимо и согласованно для выбранного канала передачи данных и файлов. Если для одного из Узлов правила не заданы, то данные переданы не будут. За конфигурацию Узла и сегмента отвечает отдельный специалист в своей сети, а определение разрешенных каналов передачи данных задаются как IP источника, порт для приема пакетов и IP назначения, порт назначения.

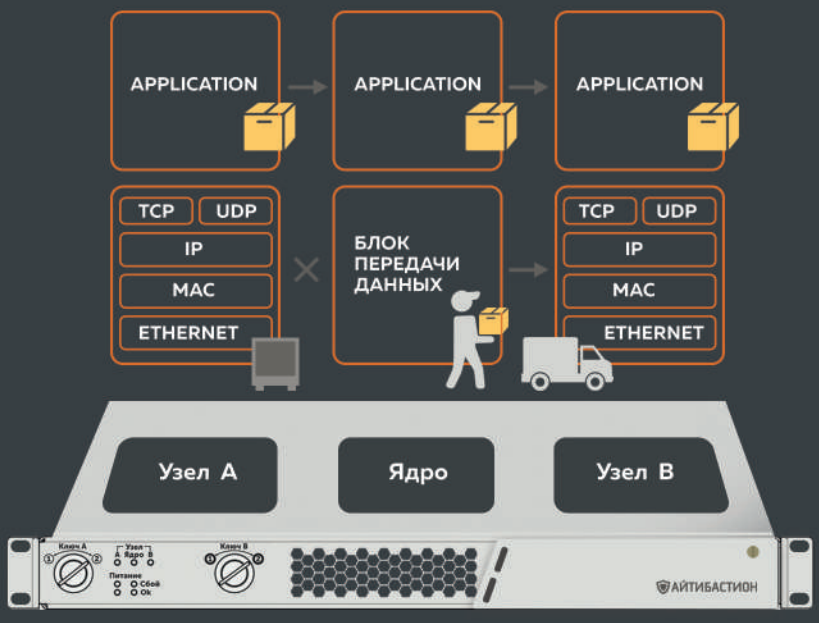
Синоникс может использоваться совместно с межсетевым экраном (МЭ) на физической границе сетей с разным уровнем доверия или сегментов с разным уровнем доступа в рамках одной сети.



Архитектура

Устройство состоит из трёх электронных плат: Узел А, Узел В и Ядро. Синоникс подключается к каждому сегменту сети отдельным сетевым интерфейсом, предназначенным только для передачи данных. Каждый интерфейс связан со своей материнской платой (Узел А и Узел В), которая изолирована от другой через центральную плату – Ядро.

Таким образом исключается прямое соединение между сетями. Если передача разрешена, то на одном из Узлов происходит удаление транспортного уровня, данные на уровне приложений передаются в Ядро. Далее из Ядра происходит передача данных на второй Узел, где транспортный уровень восстанавливается. Таким образом, при передаче информации из одного сегмента в другой система «переупаковывает» информацию по аналогии с тем, как служба доставки запаковывает ваш груз в свою упаковку.



Сценарии применения

Сценарий 1

Цель:
Повышение производительности и непрерывности обмена между изолированными сегментами сети.

Задача:
Организовать непрерывный обмен данными между двумя изолированными сегментами сети и обеспечить безопасность обмена с сохранением их изоляции.

Предпосылки, условия и компромиссы:
Требования по увеличению скорости обмена информацией, получению мгновенной отчетности и параметров из технологического сегмента растут. Для решения этой задачи необходимо объединение ранее изолированных сегментов сети, к примеру, корпоративного и промышленного. При этом риски взлома и компрометации инфраструктуры также возрастают.
И во избежание остановки технологических или бизнес-процессов нужно полностью изолировать такие сегменты друг от друга.

Решение:
Для решения этой задачи используется шлюз безопасного стыка сетей Синоникс в сочетании с классическими решениями информационной безопасности.
Так, NGFW обеспечивает базовую защиту каждой сети, в том числе на уровне контроля приложений. В изолируемом сегменте Синоникс размещается перед NGFW со стороны общей сети или канала связи между сегментами.

В процессе передачи пакетов данных Синоникс полностью перестраивает транспортную составляющую пакета (1-4 уровень модели OSI). Таким образом исключаются атаки на этом уровне и обеспечивается дополнительная защита инфраструктуры и NGFW от атак транспортного уровня.

Синоникс полностью скрывает реальную инфраструктуру защищаемого объекта, предоставляя только заранее определенный канал для обмена информацией.

Сценарий 2

Цель:

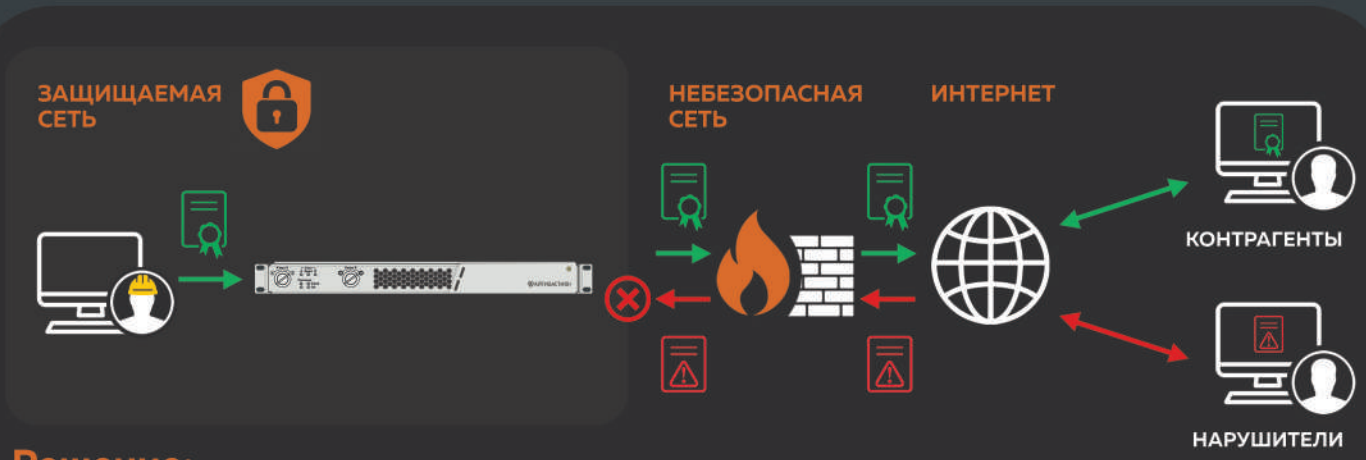
Соответствие требованиям регуляторов и обеспечение связи между собственной инфраструктурой и внешними компаниями (MSSP, SOC и т.п.) путем предоставления доступа к необходимым данным.

Задача:

Обеспечить передачу данных третьей стороне без угрозы безопасности внутренней сети компании.

Предпосылки, условия и компромиссы:

Современная информационная безопасность требует штат квалифицированных специалистов и финансовые вложения на поддержание инфраструктуры. И поэтому активно развивается процесс привлечения сторонних специализированных компаний для решения внутренних задач по ИБ – начиная с аутсорсинга специалистов и MSSP-компаний и заканчивая привлечением сторонних SOC для идентификации, расследования и реагирования на инциденты внутри инфраструктуры. Кроме того, для критически важных объектов существует требование по передаче информации в государственные системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА и FinCERT). Но любое взаимодействие с внешней инфраструктурой должно надежно защищаться и гарантировать передачу данных строго по разрешенному каналу, исключая или минимизируя возможность обратной связи с инфраструктурой.



Решение:

Синоникс используется для передачи важных и необходимых данных для анализа состояния инфраструктуры. Так, формируется безопасный контролируемый туннель до внешней стороны, которым может выступать регулятор и внешние центры обработки данных и реагирования (внешний и коммерческий SOC, ГосСОПКА, FinCERT и др.), а также внешние компании, обеспечивающие работу ИТ и ИБ (подрядчики и MSSP-компании).

Синоникс соединяет конфиденциальную и открытую сети. Информация из защищаемого сегмента ограждена от внешнего воздействия благодаря безопасному контролируемому каналу передачи данных. Передача любых вредоносных объектов через Синоникс в защищаемую сеть с внешней стороны контролируется и предотвращается за счет встроенных средств проверки цифровой подписи файлов, а также дополнительного контроля при помощи интегрируемых средств антивирусной защиты. Благодаря контролируемой передачи и возможности дополнительной интеграции с внешними DLP-системами средствами ICAP-протокола решение минимизирует риски утечки конфиденциальной информации из защищаемой сети. Для реализации полноценной защиты на всех уровнях Синоникс устанавливается совместно с NGFW, расширяя возможности контроля и фильтрации пакетов данных. Система полностью скрывает реальную инфраструктуру защищаемого объекта и предоставляет только заранее определенный канал для обмена информацией.

Сценарий 3

Цель:

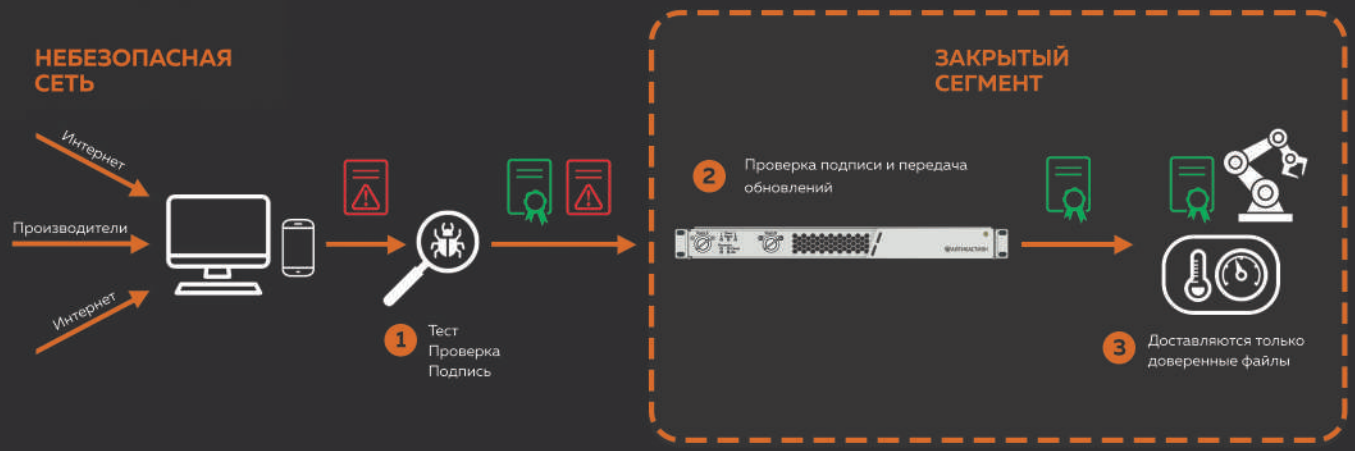
Повышение производительности и надежности процесса обновления промышленных объектов.нных третьей стороне без угрозы безопасности внутренней сети компании.

Задача:

Развернуть надежную и высоко защищенную автоматизированную систему для обмена файлами между двумя изолированными сегментами сети.

Предпосылки, условия и компромиссы:

Процесс обновления оборудования и средств защиты, например, антивирусных баз требует связи и возможности доставки файлов в изолированные контуры. Существующие и наиболее распространенные технологии доставки файлов (перенос файлов на «флешке» или АРМ с двумя сетевыми картами) позволяют реализовать этот процесс, но не могут полностью автоматизировать его. При этом всегда существует «человеческий фактор», который влияет на безопасность изолированных объектов. Следовательно, требуется решение, которое совмещало бы удобство и безопасность и было бы автоматизировано.



Решение:

Пользователь из одной сети подключается по протоколу передачи файлов SFTP к шлюзу Синоникс и получает доступ к изолированному на его стороне файловому SFTP-серверу. Вход осуществляется только при предоставлении корректной УЗ (имени пользователя и пароля) от шлюза Синоникс.

Пользователь размещает файл в каталоге для отправки и ожидает его перемещения на сторону другой сети (промышленной). После полной загрузки в каталог файл автоматически оказывается в очереди на передачу. При этом до фактического перемещения на сторону защищаемой сети он проходит ряд проверок, заданных администратором устройства, а именно:

- проверка размера и маски файла (формата имени);
- проверка цифровой подписи файла;
- проверка через внешние системы по протоколу ICAP.

Если все заданные проверки пройдены, файл получает разрешение на передачу и перемещается устройством на другую сторону в защищаемую сеть. Он может быть размещен в собственном файловом хранилище или передан на целевой сервер по протоколу передачи данных SFTP. Со стороны защищаемой сети другой пользователь так же подключается к Синониксу, используя свои УЗ (имя пользователя и пароль), и может забрать файл из каталога, в котором размещаются переданные файлы. Также шлюз Синоникс может использоваться для двунаправленной передачи файлов между сегментами. Сценарий описывает процесс безопасного объединения двух сетей для передачи файлов. При этом возможна конфигурация, при которой устанавливать другие соединения кроме передачи файлов запрещено и невозможно.

Сценарий 4

Цель:

Обеспечение дополнительной степени защиты при передаче данных в закрытый сегмент и организация безопасного контролируемого доступа в него.

Задача:

Организовать изоляцию сегментов сетей с возможностью передачи части данных из закрытого контура и обеспечить контролируемый доступ к критически важным объектам средствами PAM-системы.

Предпосылки, условия и компромиссы:

Получение актуальных и оперативных данных из закрытых, изолированных сегментов является актуальной, но не единственной задачей в современных реалиях глобальной цифровизации бизнеса. Также важно оперативно обеспечить удаленный доступ к объектам в таких сегментах при условии, что он не только регламентирован, но и надежно защищен и соответствует всем предъявляемым к этим объектам требованиям регуляторов.

Решение:

Для достижения цели используется шлюз безопасного стыка сетей Синоникс в сочетании с PAM-системой СКДПУ НТ.

В рамках организованного безопасного канала между двумя сетями располагается Синоникс. Он предоставляет дополнительный контроль и фильтрацию пакетов на транспортном уровне и обеспечивает связь между заранее определенными системами двух сетей, одной из которой является СКДПУ НТ. NGFW, который размещается после Синоникса, создает базовую защиту изолированной сети.

Далее со стороны закрытого сегмента – СКДПУ НТ, через которую проходит контролируемый безопасный доступ к целевой системе.

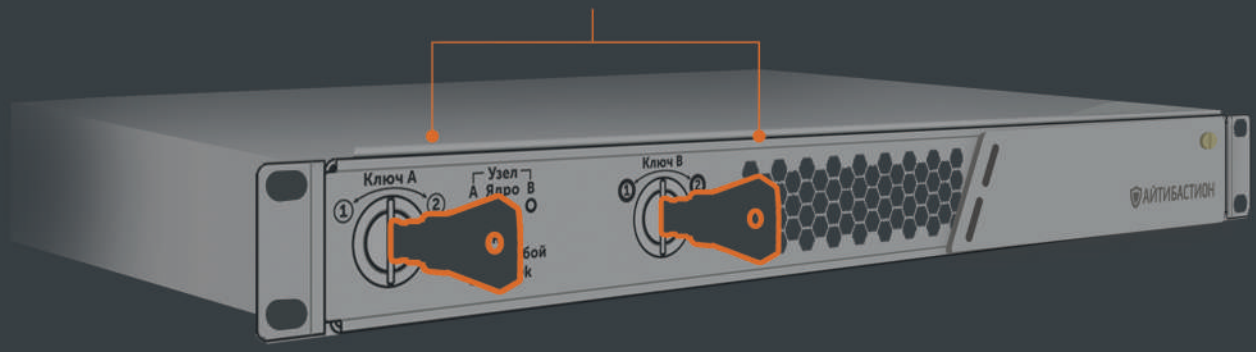
Таким образом обеспечивается не только высокий уровень контроля проходящей между сетями информации, фильтрация и защита от атак на транспортном уровне, но и управление привилегированным доступом внутри закрытого сегмента.

Дополнительный физический контроль

Два встречных набора правил передачи помогают разграничить зоны ответственности между сотрудниками объединяемых сетей. Конфигурация устройства осуществляется через физически изолированные интерфейсы управления соответствующего Узла. Управление может реализовываться как удаленно по сети, так и исключительно локально через интерфейс RS-232.

Изменение конфигурации центральной платы (Ядра) возможно только при наличии физического доступа к ней и вскрытии защитных пломб. А изменение конфигурации одного Узла со стороны другого технологически и конструкционно неосуществимо.

Дополнительный контроль обеспечивается с помощью физических пусковых ключей, разделяемых между сотрудниками, каждый из которых ответственен за свою сеть. Ключи разрешают или блокируют передачу данных через Синоникс путем полного отключения питания Ядра.
При повороте одного из них центральная плата отключается.



Решение позволяет:

- Противодействовать существующим и потенциально неизвестным уязвимостям путем сокрытия данных о стыкуемых сетях и информационных системах, а также путем ограничения доступа к информации о системах внутри закрытого контура.
- Автоматизировать процессы передачи исполняемых файлов и данных с минимизацией передачи между операторами. Такой сценарий позволяет реализовать ряд задач, характерных для процесса безопасной разработки и обновления программного обеспечения в закрытых сегментах, решать задачи передачи данных мониторинга и управления без раскрытия структуры стыкуемых объектов сетевой инфраструктуры.
- Регистрировать события безопасности для последующего просмотра с целью аудита, управления инцидентами, проведения расследований.

Технические характеристики

- **Производство.** На базе отечественного оборудования
- **Оборудование.** Архитектура x86-64 (2 ГГц)
  ОЗУ 8 ГБ. Диск 128 ГБ
- **Форм-фактор.** 19" стойка – 1U
- **ОС.** Астра Линукс 1.7 SE
- **Скорость.** До 1 Гб/с

Интеграции и технологические партнёры

Подтверждена эффективная работа и совместимость с PAM-платформой СКДПУ НТ.

Наши технологические партнеры:

- Антивирусная защита: Kaspersky, Dr.Web
- DLP-системы: Infowatch, Solar, Zecurion
- МЭ и NGFW: Код Безопасности, UserGate, InfoWatch, Infotecs, S-Terra

Соответствие требованиям КИИ

В соответствии с приказом ФСТЭК России №239 от 25 декабря 2017 года Синоникс обеспечивает выполнение следующих мер:

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Комментарии
Обеспечение целостности		
ОЦЛ.2	Контроль целостности информации	Цифровая подпись передаваемых файлов
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	Передача файлов, имена которых соответствуют файловая политика
Защита информационной (автоматизированной) системы и ее компонентов		
ЗИС.2	Защита периметра информационной (автоматизированной) системы	
ЗИС.4	Сегментирование информационной (автоматизированной) системы	
ЗИС.5	Организация демилитаризованной зоны	
ЗИС.6	Управление сетевыми потоками	Настройка направления передачи данных
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию	Настройка IP адресов для предоставления доступа во внешнюю сеть
ЗИС.20	Обеспечение доверенных канала, маршрута	
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	Выход из строя одного канала не влияет на работу устройства в целом
ЗИС.35	Управление сетевыми соединениями	Настройка IP адресов Прерывание сессии FTP (FTPS)
Управление обновлениями программного обеспечения		
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	Настройка IP адресов для получения обновлений из доверенного источника
ОПО.2	Контроль целостности обновлений программного обеспечения	Цифровая подпись файлов обновлений

АЙТИБАСТИОН
Москва.
ул. Старовольнская, 15к1
E-mail: info@it-bastion.com
Тел.: +7 (499) 322 36 67