



Интегрированный файловый и почтовый однаправленный шлюз СТРОМ-ФАЙЛ

Интегрированный файловый и почтовый однаправленный шлюз СТРОМ-ФАЙЛ предназначен для гарантированной однаправленной передачи файлов и почтовых сообщений из сетей, обрабатывающих информацию с меньшим уровнем конфиденциальности (в том числе подключенных к сети Internet), а также файлов с произвольных USB-носителей, в сети, обрабатывающие информацию более высокого уровня конфиденциальности. Помимо этого, через шлюз реализуют соединение двух сегментов сети, у которых отсутствуют требования по обеспечению конфиденциальности, для реализации защиты сети, передающей информацию, от внешнего воздействия. СТРОМ-ФАЙЛ состоит из двух блоков, связанных между собой симплексным многомодовым оптическим кабелем, каждый из которых располагается в соответствующей сети, передающей информацию и назначения.

Выгоды применения

- Реализация гарантированной однаправленной передачи информации на аппаратном уровне, что в зависимости от целей использования позволяет обеспечить конфиденциальность или целостность и доступность одной из соединяемых сетей.
- Простота использования и настройки, требуется минимальное администрирование текстовым файлом специального формата, дальше система работает в автоматическом режиме по заданным правилам, которые при необходимости можно легко изменить.
- По сравнению с традиционной схемой реализации однаправленной передачи информации нет необходимости установки дополнительных прокси-серверов в соединяемых сетях, система обеспечивает решение задачи «под ключ».
- Оперативная поставка.
- Большая наработка на отказ, полное сопровождение в процессе эксплуатации.



Основные характеристики

- Скорость передачи: до 200 Мбит/с.
- Старт: менее 30 секунд.
- Каждый блок представляет собой аппаратную многопроцессорную платформу, размещенную на одной печатной плате, на которой можно выделить сервер с хранилищем, действующий под управлением ОС Linux специальной сборки, и модуль передач (приема) однаправленной сетевой информации, состоящий из FPGA и микроконтроллера.
- Поддержка файловых и почтовых сервисов: SMB, FTP, IMAP, POP3 и SMTP.
- Расстояние между блоками шлюза до 300 метров.
- Интерфейсы:
 - Внешний блок:
 - внешние: RJ-45, медь, витая пара, Ethernet 10/100/1000BASE-TX; SFP, оптика, Ethernet 1000BASE-X; USB 2.0;
 - внутренний: SC, многомодовая оптика, 850 нм.
 - Внутренний блок:
 - внешний: SC, многомодовая оптика, 850 нм;
 - внутренний: RJ-45, медь, витая пара, Ethernet 10/100/1000 BASE-TX; SFP, оптика, Ethernet 1000BASE-X.
- Конфигурирование: текстовый скрипт на SD-карте для каждого блока.
- Поддержка до 100 пользователей.



- Индикация (отображение состояния):
 - Светодиоды.
 - Матричный экран.
- Исполнение внешнего и внутреннего блока по 1U в 19-дюймовую стойку (ВхШхГ 44x483x272).
- Потребление: 30Вт.
- Транспортировка данных осуществляется по IP-протоколу, в соединяемых сетях поддерживается статическая и динамическая адресация.
- Категория подключаемых внутренних сетей до «совершенно секретно» включительно.
- Соккрытие структуры и топологии внутренней сети.
- Минимизация возможности потери информации при передаче, реализуемая дублированием передачи.
- Организация контроля доступа пользователей к передаваемой информации и ее квотирование, задаваемое в конфигурационном файле.
- Пользовательские диски SSD объемом от 64 ГБ до 512 ГБ на внешнем и внутреннем блоке.
- Наличие межсетевого экрана позволяет разрешить или заблокировать прохождение сетевых пакетов, на сетевом интерфейсе разрешен трафик только используемых сервисов.
- Ведение журналов событий на внешнем и внутреннем блоке, с их архивацией и хранением заданное в настройках время, возможность передачи журналов работы на внешние серверы при настройке соответствующих сервисов.
- Каждый блок имеет часы реального времени, реализована возможность задания времени через конфигурационный файл и коррекция времени с использованием сервисов протокола NTP.

Применение

Режим использования интегрированного файлового и почтового однонаправленного шлюза СТРОМ-ФАЙЛ зависит от поставленной задачи.

Передача файлов. Однонаправленный шлюз СТРОМ-ФАЙЛ обеспечивает автоматическую передачу файловой информации из сетей, обрабатывающих информацию с меньшим уровнем конфиденциальности, в сети с более высоким уровнем конфиденциальности. В этом случае на аппаратном уровне гарантируется невозможность утечки информации из категоризированной сети. Помимо этого, через СТРОМ-ФАЙЛ соединяют два сегмента сети, когда есть требования по обеспечению целостности и доступности одного из них. В этом случае однонаправленная передача информации гарантирует отсутствие возможности нежелательного воздействия на сеть, из которой осуществляется передача, со стороны сети, куда передаются данные, в том числе если последняя соединена с сетью Internet. Устройство предоставляет пользователям симметричные сетевые папки, размещенные на внутреннем и внешнем блоках. Папки доступны по протоколам FTP и SMB. К внешнему блоку по данным сервисам доступ пользователей осуществляется с правами на чтение, запись и удаление, а к внутреннему только на чтение и удаление. При копировании пользователем информации в сетевую папку внешнего блока она передается по однонаправленному каналу внутреннему блоку, где помещается в папку пользователя, после чего удаляется из папки внешнего блока. Сервисы передачи и приема файлов через однонаправленный канал работают постоянно, сканируя папки пользователей в режиме карусели, пересылая и сохраняя информацию в соответствующих папках внутреннего блока с сохранением структуры каталогов. В шлюзе реализована возможность автоматической очистки файловых каталогов обоих блоков с задаваемым в конфигурационном файле расписанием. Эта процедура позволяет более эффективно использовать пространство пользовательских дисков.

Передача файлов с внешнего накопителя с разъемом USB. При подключении внешнего накопителя класса Mass Storage Device к USB-разъему внешнего блока однонаправленный шлюз СТРОМ-ФАЙЛ передает всю файловую информацию, записанную на нем, в специальную сетевую папку с зарезервированным именем на внутреннем блоке с сохранением структуры директорий. Для каждого введенного накопителя в специальной папке создается каталог с именем, совпадающим с идентификатором носителя. Доступ к этому каталогу с заданными параметрами учетной записи можно получить по SMB и FTP протоколам.

Передача почтовых сообщений. Внешний блок производит сбор почты со сторонних серверов по протоколам POP3, IMAP, в том числе на основе защищенных соединений с использованием криптографических протоколов TLS и SSL, и передает поступившие сообщения по однонаправленному каналу на внутренний блок. После передачи сообщения оно стирается на сервере внешнего блока. Список учетных записей, паролей, адресов сторонних серверов, портов и ключей шифрования, необходимый для сбора почты задается в конфигурационном файле. Опрос внешних почтовых серверов, указанных в



конфигурационном файле, производится по очереди. Старт нового опроса пула серверов производится циклически с интервалом, указанным при конфигурировании. На микропроцессоре внутреннего блока функционирует почтовый сервер, позволяющий почтовым клиентам пользователей получать электронные письма по протоколам POP3, IMAP. Во внутренней сети криптографические протоколы не используются. Однонаправленный характер передачи информации, реализуемый СТРОМ-ФАЙЛОМ, не позволяет ответить на письмо или послать подтверждение о прочтении из внутренней сети, что гарантирует обеспечение ее конфиденциальности. Для обеспечения эффективного использования пространства пользовательских дисков внешнего и внутреннего блоков реализована возможность автоматической очистки почтовых каталогов обоих блоков с задаваемым в конфигурационном файле расписанием.