Устройство однонаправленной передачи данных
аппаратно-программный комплекс AMT InfoDiode PRO

(наименование и индекс изделия)

РУКОВОДСТВО ПО ПОДГОТОВКЕ К ЭКСПЛУАТАЦИИ

AMTID-IDK-1000, AMTID-IDK-2000

(обозначение)

2024 г.

Содержание

1. Введение 3
2. Технические характеристики АПК InfoDiode PRO базовая комплектация 4
2.1 Габариты....4
2.2 Эл. питание, мощность и тепловыделение 4
2.3 Физические характеристики....5
2.4 Интерфейсы 5
3. Технические характеристики АПК InfoDiode PRO кластерная комплектация 6
3.1 Габариты....6
3.2 Эл. питание, мощность и тепловыделение 6
3.3 Физические характеристики....7
3.4 Интерфейсы 7
4. Базовая комплектация....8
4.1 Подготовка к настройке....10
4.2 Подключение АПК InfoDiode PRO к корпоративной сети 12
4.2.1 Подключение к электросети, включение эл.питания АПК InfoDiode PRO 12
4.2.2 Подключение серверов In-Proxy и Out-Proxy к корпоративной сети....12
4.2.3 Подключение серверов к аппаратной компоненте InfoDiode RACK single: 12
4.2.4 Проверка и изменение конфигурации прокси-серверов....12
5. Кластерная комплектация 15
5.1 Подготовка к настройке....17
5.2 Подключение кластера АПК InfoDiode PRO к корпоративной сети....20
5.2.1 Подключение к электросети, включение эл.питания АПК InfoDiode PRO 20
5.2.2 Подключение серверов In-Proxy и Out-Proxy к корпоративной сети....20
5.2.3 Подключение серверов к аппаратным компонентам InfoDiode RACK double...20
5.2.4 Проверка и изменение конфигурации прокси-серверов....21
6. Настройка АПК InfoDiode PRO....24
6.1 Настройка передачи файлов по FTP....24
6.2 Настройка потоковой передачи трафика по UDP 25
6.2.1 Пример настройки передачи.....26
6.3 Настройка передачи электронной почты 26

1. Введение

Настоящее руководство содержит инструкцию по подготовке к эксплуатации оборудования АПК InfoDiode PRO и его первоначальной настройке.

Монтаж оборудования должен производиться с учетом соблюдения всех технических требований и характеристик АПК InfoDiode PRO.

2. Технические характеристики АПК InfoDiode PRO базовая комплектация

2.1 Габариты

Базовый АПК InfoDiode PRO base состоит из 3-х компонент и занимает 3 rack unit: два сервера и одна аппаратная компонента однонаправленной передачи данных.

В Таблица 1 приведены габаритные характеристики всех компонент базового АПК InfoDiode PRO base.

Таблица 1. Габаритные характеристики компонент АПК InfoDiode PRO base

	Ширина (мм)	Глубина (мм)	Высота (мм)	Вес (кг)
Сервер	483	497	44	10
Аппаратная компонента	483	250	44,5	5,1
АПК InfoDiode PRO base в комплекте	483	497	133	25,1

2.2 Эл. питание, мощность и тепловыделение

- Эл. питание - 230 В (AC);
- Частота - 50-60 Гц (однофазный).

На каждом сервере по 2 блока эл. питания (для обеспечения отказоустойчивости).

На аппаратной компоненте 2 блока эл. питания (для обеспечения защиты и разделения принимающей и передающей сторон в части электроснабжения).

В Таблица 2 приведены расчетные и максимальные показатели мощности и тепловыделения базового АПК InfoDiode PRO base.

Таблица 2. Показатели мощности и тепловыделения АПК InfoDiode PRO base

Показатель	InProxy	OutProxy	АК InfoDiode RACK single	АПК InfoDiode PRO base в комплекте
Мощность, Вт: расчетная	277,8	277,8	15	570,6
Мощность, Вт: максимальная	450	450	30	930
Тепловыделение, BTU/hr: Расчетное	947,3	947,3	51,2	1945,8
Тепловыделение, BTU/hr: Максимальное	1535	1535	102	3172

2.3 Физические характеристики

Температура: рабочая от +10 до +35°C, хранение от –40 до +70°C;

Влажность: от 5 до 90 %, без конденсации влаги.

2.4 Интерфейсы

Data&Management на каждом сервере: 4x1000Base-T (RJ-45), 2xSFP модуль 1000Base-SX (LC), 1x Mgmt LAN (RJ-45)..

Пропускная способность:

- потоковый трафик (UDP) – до 900 Mbps;
- прокси передача (FTP/CIFS/SMTP) – до 300 Mbps.

Поддержка статических маршрутов.

3. Технические характеристики АПК InfoDiode PRO кластерная комплектация

3.1 Габариты

Кластерная версия АПК InfoDiode PRO cluster состоит из 6-ти компонент и занимает 6 rack unit: четыре сервера и две двойные аппаратные компоненты однонаправленной передачи данных.

В Таблица 3 приведены габаритные характеристики всех компонент кластерной версии АПК InfoDiode PRO cluster.

Таблица 3. Габаритные характеристики компонент АПК InfoDiode PRO cluster

	Ширина (мм)	Глубина (мм)	Высота (мм)	Вес (кг)
Сервер	483	497	44	10
Двойная аппаратная компонента	483	250	44,5	5,3
АПК InfoDiode PRO cluster в комплекте	483	497	266	50,6

3.2 Эл. питание, мощность и тепловыделение

- Эл. питание - 230 В (AC);
- Частота - 50-60 Гц (однофазный).

На каждом сервере по 2 блока эл. питания (для обеспечения отказоустойчивости).

На каждой двойной аппаратной компоненте 2 двойных блока эл. питания (для обеспечения защиты и разделения принимающей и передающей сторон в части электроснабжения).

В Таблица 4 приведены расчетные и максимальные показатели мощности и тепловыделения кластерной версии АПК InfoDiode PRO cluster.

Таблица 4. Показатели мощности и тепловыделения АПК InfoDiode PRO cluster

Показатель	InProxy	OutProxy	АК InfoDiode RACK double	АПК InfoDiode PRO cluster в комплекте
Мощность, Вт: расчетная	277,8	277,8	15	1142,2
Мощность, Вт: максимальная	450	450	30	1860
Тепловыделение, BTU/hr: Расчетное	947,3	947,3	51,2	3891,6
Тепловыделение, BTU/hr: Максимальное	1535	1535	102	6344

3.3 Физические характеристики

Температура: рабочая от +10 до +35°C, хранение от –40 до +70°C;

Влажность: от 5 до 90 %, без конденсации влаги.

3.4 Интерфейсы

Data&Management на каждом сервере: 4x1000Base-T (RJ-45), 2xSFP модуль 1000Base-SX (LC), 1x Mgmt LAN (RJ-45).

Пропускная способность:

- потоковый трафик (UDP) – до 900 Mbps;
- прокси передача (FTP/CIFS/SMTP) – до 300 Mbps.

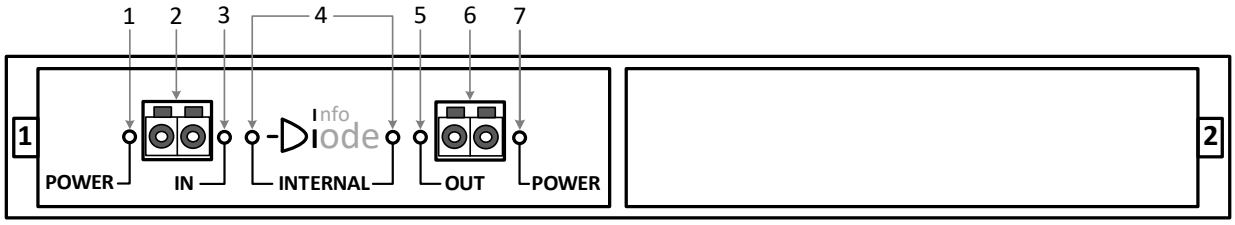
Поддержка статических маршрутов.

4. Базовая комплектация

В базовую комплектацию АПК InfoDiode PRO base входит:

- Аппаратное устройство однонаправленной передачи данных АК InfoDiode RACK single;
- Два Сервера Kraftway (In-Proxy и Out-Proxy) с предустановленным ПО InfoDiode;
- Два патч-корда Multi-mode с коннекторами LC-LC.

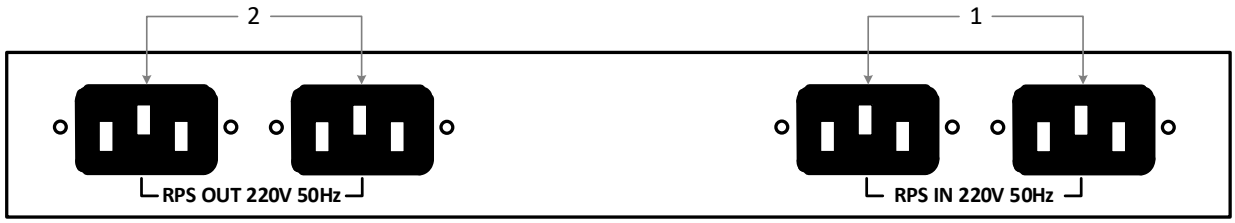
На Рисунок 1 изображена передняя панель аппаратного устройства однонаправленной передачи данных АПК InfoDiode RACK single:



1 – Индикатор эл.питания порта IN
2 – Разъем LC-LC для подключения InProxy сервера
3 – Индикатор статуса соединения порта IN
4 – Индикатор статуса однонаправленного соединения
5 – Индикатор статуса соединения порта OUT
6 – Разъем LC-LC для подключения OutProxy сервера
7 – Индикатор эл.питания порта OUT

Рисунок 1. Передняя панель аппаратного устройства однонаправленной передачи данных АК InfoDiode RACK single

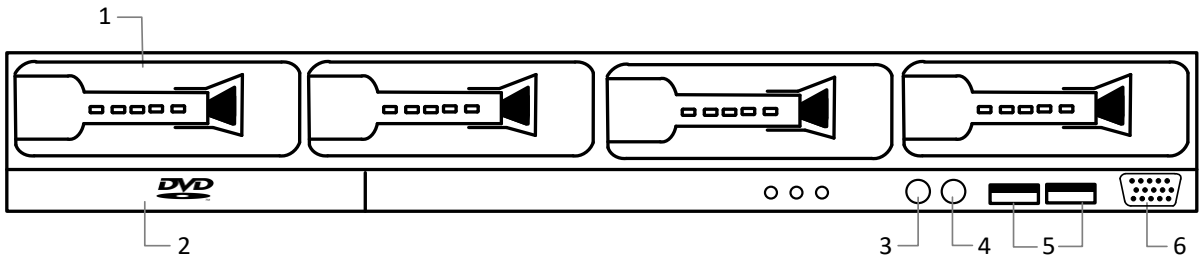
На Рисунок 2 изображена задняя панель аппаратного устройства однонаправленной передачи данных АК InfoDiode RACK single:



1 – Разъемы для подключения резервированного эл.питания IEC порта IN
2 – Разъемы для подключения резервированного эл.питания IEC порта OUT

Рисунок 2. Задняя панель аппаратного устройства однонаправленной передачи данных АК InfoDiode RACK single

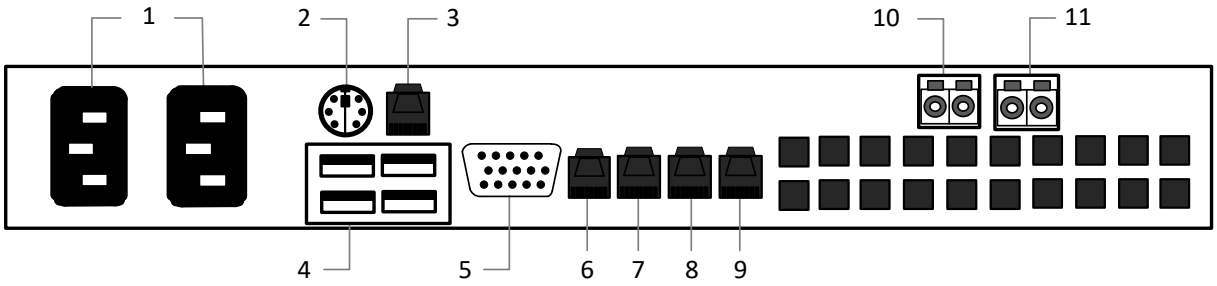
На Рисунок 3 изображена передняя панель прокси-сервера Kraftway для АПК InfoDiode PRO:



1 – Корзина для HDD диска
2 – Привод CD/DVD-ROM
3 – Кнопка включения питания
4 – Кнопка перезагрузки
5 – USB-порты
6 – Разъем для подключения монитора VGA

Рисунок 3. Передняя панель прокси-сервера для АПК InfoDiode PRO

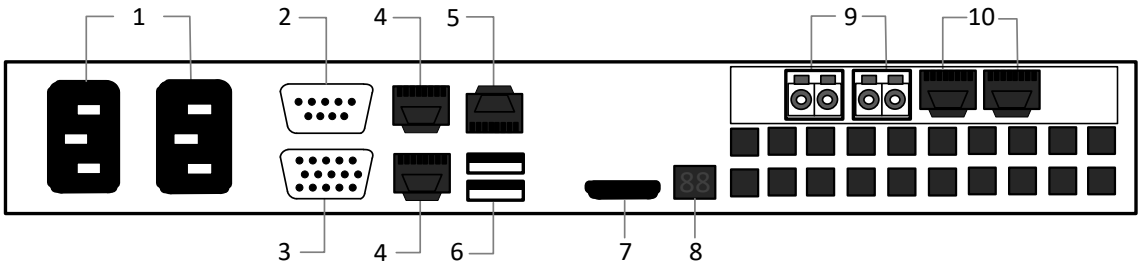
На Рисунок 4 изображена задняя панель прокси-сервера для АПК InfoDiode PRO:



1 – Разъемы для подключения резервированного эл.питания
2 – Разъем для подключения клавиатуры PC/2
3 – Порт RJ-45 для мониторинга сервера по протоколу IPMI 2.0
4 – USB-порты
5 – Разъем для подключения монитора VGA
6-9 – Внешние сетевые интерфейсы ***lan1-lan4***
10-11 – Внутренние оптические интерфейсы ***fc1-fc2***

Рисунок 4. Задняя панель прокси-сервера для АПК InfoDiode PRO

На Рисунок 5 изображена задняя панель прокси-сервера Kraftway (модель EL108) для АПК InfoDiode PRO:



1 – Разъемы для подключения резервированного эл.питания
2 – COM-Порт
3 – Разъем для подключения монитора VGA
4 – Внешние сетевые интерфейсы ***lan1*** и ***lan4***
5 – Порт RJ-45 для мониторинга сервера по протоколу IPMI 2.0
6 – USB-порты
7 – Разъем для подключения монитора HDMI
8 – LED-Дисплей
9 – Внутренние оптические интерфейсы ***fc1*** и ***fc2***
10 – Внешние сетевые интерфейсы ***lan2*** и ***lan3***

Рисунок 5. Задняя панель прокси-сервера (модель EL108) для АПК InfoDiode PRO

4.1 Подготовка к настройке

Задокументируйте в Таблица 5 все настройки оборудования АПК InfoDiode PRO base. Эти данные могут понадобиться для администрирования и резервного восстановления.

Внимание! Конфигурирование устройства следует воспринимать согласно модели «черного ящика» с предоставлением для конфигурирования строго определенного набора команд и параметров, явно указанных в соответствующих эксплуатационных документах. Целостность системных файлов и каталогов, как и разделов на дисках в целом, отслеживается системой контроля целостности. В частности, запрещено создавать новые файлы в любых каталогах, кроме домашних директорий пользователей (/home) и /tmp. Также наложено ограничение (запрещено) самостоятельное изменение основных конфигурационных файлов: smb.conf, vsftpd.conf, sudoers, конфигураций sysctl и других системных конфигурационных файлов, а также включение/выключение служб и изменение параметров служб через средства cli (systemctl, timedatectl и прочее)– явно незадекларированных к изменению в настоящей инструкции.

Самостоятельно изменение конфигурационных файлов вне требований инструкции может привести к нарушению целостности продукта и инциденту информационной безопасности.

Конфигурация сетевых интерфейсов, адресации и т.п. выполняется в соответствии с разделом 4.2.4 настоящего документа.

Таблица 5. Настройки оборудования АПК InfoDiode PRO base

Пункт	**Описание**	**Ваша настройка**	
		InProxy	**OutProxy**
IP-адрес и маска сете вых интер фейсов	IP-адрес и маска интерфейсов управления и данных серверов для доступа к web-интерфейсу и передачи данных. Если ip-адрес интерфейса управления и данных должны быть совмещены (inband-managment), то продублировать адреса	**Управление**	
		Данные	
Маршрут по умолчанию (шлюз)	Сетевой шлюз, на который пакет отправляется в том случае, если маршрут к сети назначения пакета не известен		
Хост сервера Syslog *необязате льно	Указание IP-адреса сервера для сбора syslog-информации разного уровня логирования		
SNMP пароль *необязате льно	Слово или фраза, которая спрашивается для управления сетевыми устройствами (маршрутизатор, коммутатор)		
Domain name server *необязате льно	IP-адрес сервера, используемый для DNS запроса		
Администр ативные данные *необязате льно	Логин и пароль для доступа к web-интерфейсу. После авторизации можно изменить		

4.2 Подключение АПК InfoDiode PRO к корпоративной сети

4.2.1 Подключение к электросети, включение эл.питания АПК InfoDiode PRO

Подключите прокси-серверы, аппаратную компоненту кабелями эл. питания к эл. розеткам и включите кнопку эл. питания на устройствах. Устройства готовы к эксплуатации.

4.2.2 Подключение серверов In-Proxy и Out-Proxy к корпоративной сети

1. Подключите внешний интерфейс данных lan1 к сетевому оборудованию (или к конечному устройству) кабелем вида «витая пара» с коннекторами RJ-45.
2. Подключите внешний интерфейс управления lan4 к сетевому оборудованию (или к конечному устройству) кабелем вида «витая пара» с коннекторами RJ-45.
3. Повторите эти действия со вторым сервером.

4.2.3 Подключение серверов к аппаратной компоненте InfoDiode RACK single:

Подключите один из внутренних интерфейсов данных (fc1/fc2) сервера In-Proxy оптическим кабелем к разъему IN аппаратной компоненты InfoDiode RACK single.

Подключите один из внутренних интерфейсов данных (fc1/fc2) сервера Out-Proxy оптическим кабелем к разъему OUT аппаратной компоненты InfoDiode RACK single.

Ниже на Рисунок 6 представлена схема подключения АПК InfoDiode PRO base к корпоративной сети:

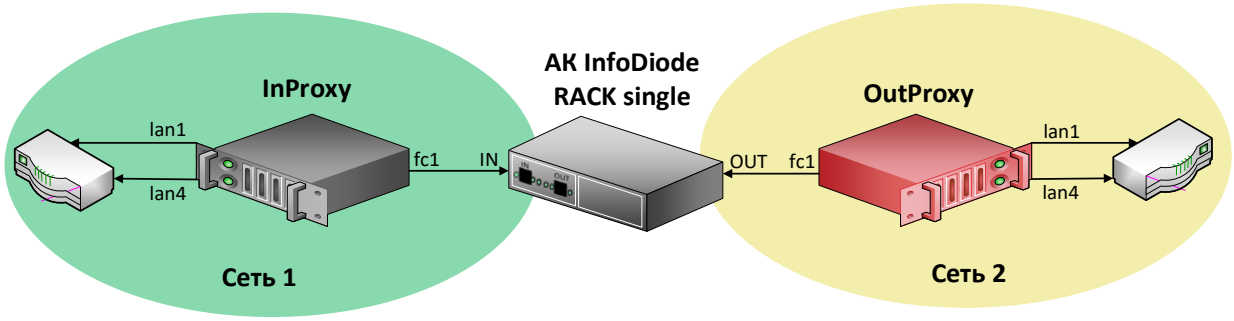


Рисунок 6. Схема подключения АПК InfoDiode PRO base к корпоративной сети.

4.2.4 Проверка и изменение конфигурации прокси-серверов

Для просмотра и изменения текущей конфигурации можно подключиться к InProxy и OutProxy тремя способами:

1. Подключить монитор и клавиатуру непосредственно к физическим серверам InProxy и OutProxy
2. По IPMI (необходима сетевая настройка на IPMI интерфейсе).
3. По SSH

При загрузке сервера заходим в BIOS - Server MGMT - BMC Network Configuration и указываем сетевые настройки (IP-адрес, маску, шлюз по умолчанию) для интерфейса IPMI. Подключаемся через веб-интерфейс, используя любой браузер с поддержкой java, в адресной строке которого вводим IP-адрес IPMI-интерфейса, и, после подключения

проходим авторизацию с использованием имени пользователя и пароля, указанных в документации или заданных пользовательскими настройками (по умолчанию используется логин и пароль *admin/admin1234*).

Внимание! При первой авторизации в терминале (по IPMI или по прямому подключению с помощью клавиатуры и монитора) системы необходимо сменить пароль пользователя *root* на соответствующий рекомендуемым политикам безопасности. Для смены пароля авторизуйтесь как *root*, введите пароль *infodiode,* затем введите новый пароль в ответ на запрос системы. Запомните или зафиксируйте данный пароль согласно правилам и политикам безопасности для вашей организации.

Для доступа по SSH необходимо, чтобы предварительно был настроен IP-адрес на интерфейсе управления, маршрут по умолчанию. Подключитесь к серверу по IP-адресу интерфейса управления lan4. После подключения введите в SSH-консоли логин и пароль *diode/P@ssw0rd*.

Внимание! В составе дистрибутива присутствует утилита pwquality с соответствующим конфигурационным файлом, определяющим парольную политику (требования к сложности пароля установлены согласно требованиям регулятора для СЗИ УД4), а также утилита pam_faillock (определяет блокирование УЗ в случае некорректного ввода пароля и базовую защиту от bruteforce). С учетом этого в системе присутствуют значимые требования к сложности пароля, а нарушение политики может являться препятствием для запуска всей системы и может быть продиагностировано.
По умолчанию применены следующие требования парольной политики:

- В отношении качества пароля - "Длина пароля не менее восьми символов, алфавит пароля не менее 70 символов, пароль должен включать заглавные буквы, цифры и спецсимволы"

В отношении защиты от bruteforce:

- количество неправильных вводов – 4 попытки
- время измерения – 5 минут
- время блокировки - 30 минут

В случае если согласно требованиям организации необходимо применить более "мягкую" парольную политику в части качества пароля - следует внести изменения в файл (/etc/security/pwquality.conf).

После подключения к серверам In-proxy/Out-proxy:

1. Сохраняем текущую конфигурацию командой `infodiode-cli config save -f /tmp/cfg.xml –wp`

2. Чтобы редактировать текущую конфигурацию, откройте файл /tmp/cfg.xml с помощью текстового редактора vim.
3. Найдите блок <subsystem xmlns="urn:ru:amt:diode:config:1.0:network">...</subsystem> и измените сетевые параметры интерфейса управления lan4 и маршрута по-умолчанию (Рисунок 6)
4. Для применения конфигурации InfoDiode необходимо выполнить команду: `infodiode-cli config load -f cfg.xml`

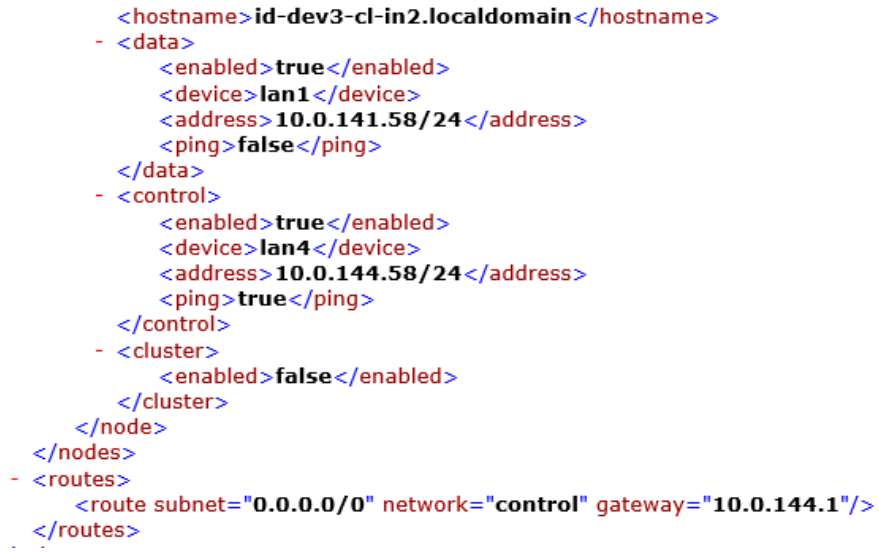


Рисунок 7. Вывод части конфигурационного файла в cli-консоли

Примечание. /tmp/cfg.xml - Имя файла, куда будет выгружена текущая конфигурация ПО InfoDiode -wp - выгрузка конфигурации с паролями

В данном примере:

lan1 – наименование интерфейса данных

lan4 - наименование интерфейса управления

10.0.144.58/24 - сетевой адрес интерфейса управления

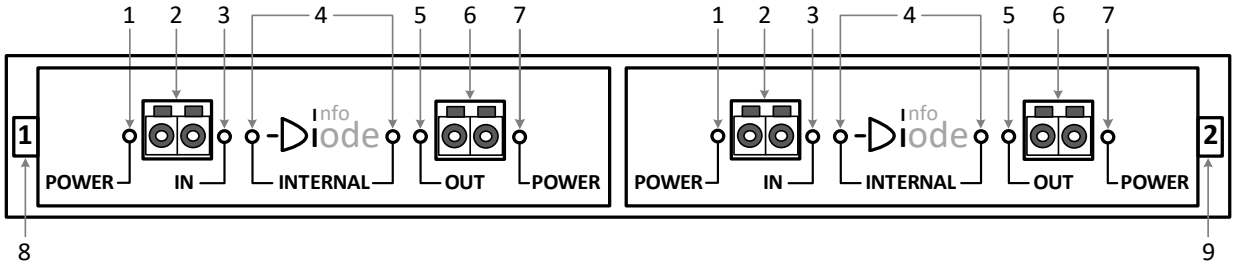
10.0.144.1 - адрес шлюза по-умолчанию

5. Кластерная комплектация

В комплектацию кластерной версии АПК InfoDiode PRO cluster входят:

- Два двойных аппаратных устройства однонаправленной передачи данных АК InfoDiode RACK double с четырьмя разъемами LC-LC;
- Четыре Сервера Kraftway (два In-Proxy и два Out-Proxy) с предустановленным ПО InfoDiode;
- Восемь патч-кордов Multi-mode с коннекторами LC-LC.

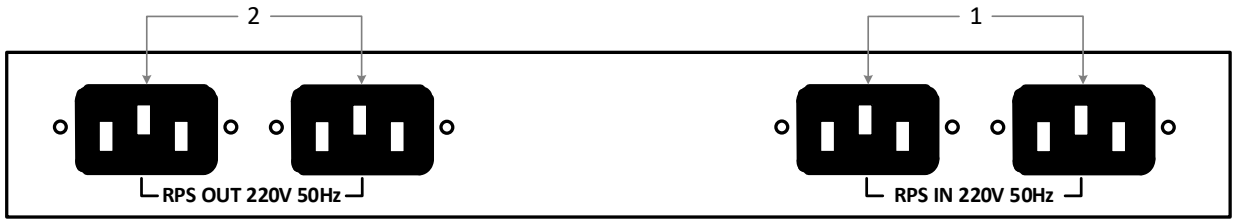
На Рисунок 8 изображена передняя панель двойного аппаратного устройства однонаправленной передачи данных АК InfoDiode RACK double:



1 – Индикатор эл.питания порта IN
2 – Разъем LC-LC для подключения InProxy сервера
3 – Индикатор статуса соединения порта IN
4 – Индикатор статуса однонаправленного соединения
5 – Индикатор статуса соединения порта OUT
6 – Разъем LC-LC для подключения OutProxy сервера
7 – Индикатор эл.питания порта OUT
8 – Первый модуль двойного аппаратного устройства
9 – Второй модуль двойного аппаратного устройства

Рисунок 8. Передняя панель двойного аппаратного устройства однонаправленной передачи данных АК InfoDiode RACK double

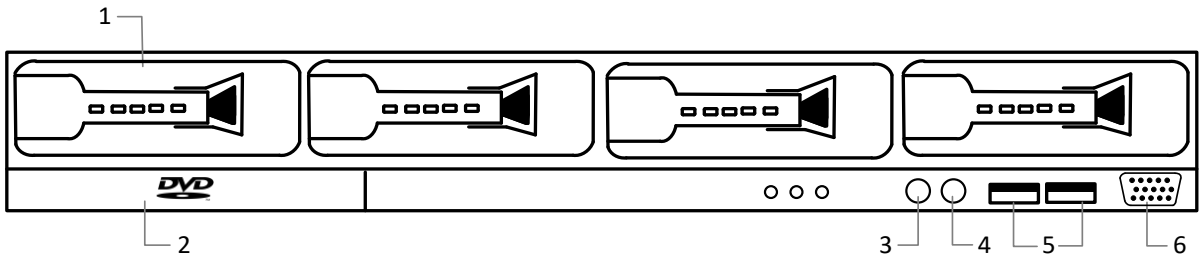
На Рисунок 9 изображена задняя панель двойного аппаратного устройства однонаправленной передачи данных АК InfoDiode RACK double:



1 – Разъемы для подключения резервированного эл.питания IEC портов IN
2 – Разъемы для подключения резервированного эл.питания IEC портов OUT

Рисунок 9. Задняя панель двойного аппаратного устройства однонаправленной передачи данных АК InfoDiode RACK double

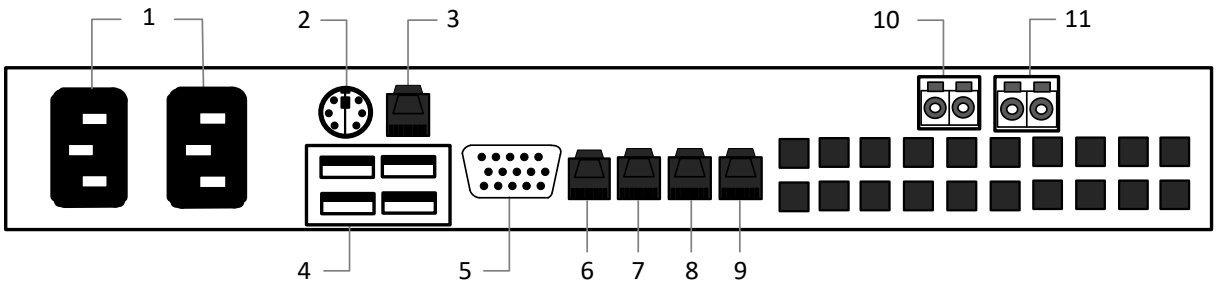
На Рисунок 10 изображена передняя панель прокси-сервера Kraftway для АПК InfoDiode PRO:



1 – Корзина для HDD диска
2 – Привод CD/DVD-ROM
3 – Кнопка включения питания
4 – Кнопка перезагрузки
5 – USB-порты
6 – Разъем для подключения монитора VGA

Рисунок 10. Передняя панель прокси-сервера для АПК InfoDiode PRO

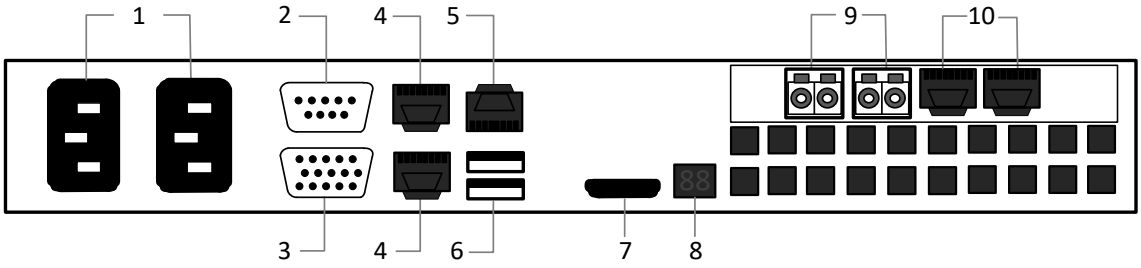
На Рисунок 11 изображена задняя панель прокси-сервера для АПК InfoDiode PRO:



1 – Разъемы для подключения резервированного эл.питания
2 – Разъем для подключения клавиатуры PC/2
3 – Порт RJ-45 для мониторинга сервера по протоколу IPMI 2.0
4 – USB-порты
5 – Разъем для подключения монитора VGA
6-9 – Внешние сетевые интерфейсы ***lan1-lan4***
10-11 – Внутренние оптические интерфейсы ***fc1-fc2***

Рисунок 11. Задняя панель прокси-сервера для АПК InfoDiode PRO

На Рисунок 12 изображена задняя панель прокси-сервера Kraftway (модель EL108) для АПК InfoDiode PRO



1 – Разъемы для подключения резервированного эл.питания
2 – COM-Порт
3 – Разъем для подключения монитора VGA
4 – Внешние сетевые интерфейсы ***lan1*** и ***lan4***
5 – Порт RJ-45 для мониторинга сервера по протоколу IPMI 2.0
6 – USB-порты
7 – Разъем для подключения монитора HDMI
8 – LED-Дисплей
9 – Внутренние оптические интерфейсы ***fc1*** и ***fc2***
10 – Внешние сетевые интерфейсы ***lan2*** и ***lan3***

Рисунок 12. Задняя панель прокси-сервера (модель EL108) для АПК InfoDiode PRO

5.1 Подготовка к настройке

Задокументируйте все настройки оборудования АПК InfoDiode PRO cluster в Таблица 6. Эти данные могут понадобиться для администрирования и резервного восстановления.

Внимание! Конфигурирование устройства следует воспринимать согласно модели «черного ящика» с предоставлением для конфигурирования строго определенного набора команд и параметров, явно указанных в соответствующих эксплуатационных документах. Целостность системных файлов и каталогов, как и разделов на дисках в целом, отслеживается системой контроля целостности. В частности, запрещено создавать новые файлы в любых каталогах, кроме домашних директорий пользователей (/home) и /tmp. Также наложено ограничение (запрещено) самостоятельное изменение основных конфигурационных файлов: smb.conf, vsftpd.conf, sudoers, конфигураций sysctl и других системных конфигурационных файлов, а также включение/выключение служб и изменение параметров служб через средства cli (systemctl, timedatectl и прочее)– явно незадекларированных к изменению в настоящей инструкции.

Самостоятельно изменение конфигурационных файлов вне требований инструкции может привести к нарушению целостности продукта и инциденту информационной безопасности.

Конфигурация сетевых интерфейсов, адресации и т.п. выполняется в соответствии с разделом 5.2.4 настоящего документа.

Таблица 6. Настройки оборудования кластер АПК InfoDiode PRO cluster

Пункт	**Описание**	**Ваша настройка**	
		InProxy_1 (Узел 1)	**InProxy_2 (Узел 2)**
Виртуальный IP	IP-адрес, совместно используемый узлами	**Для публичного доступа**	
		Для управления	
IP-адрес и маска сетевых интерфейсов	IP-адрес и маска интерфейсов управления и данных серверов для доступа к web-интерфейсу и передачи данных.	**Управление**	
		Данные	
		Внутренний (Кластер)	
Маршрут по умолчанию (шлюз)	Сетевой шлюз, на который пакет отправляется в том случае, если маршрут к сети назначения пакета не известен		
Хост сервера Syslog *необязательно	Указание IP-адреса сервера для сбора syslog-информации разного уровня логирования		
SNMP пароль *необязательно	Слово или фраза, которая спрашивается для управления сетевыми устройствами (маршрутизатор, коммутатор)		
Domain name server *необязательно	IP-адрес сервера, используемый для DNS запроса		
Административные данные *необязательно	Логин и пароль для доступа к web-интерфейсу. После авторизации можно изменить		

Пункт	**Описание**	**Ваша настройка**	
		OutProxy_1 (Узел 1)	**OutProxy_2 (Узел 2)**
Виртуальный IP	IP-адрес, совместно используемый узлами	**Для публичного доступа**	
		Для управления	
IP-адрес и маска сетевых интерфейсов	IP-адрес и маска интерфейсов управления и данных серверов для доступа к web-интерфейсу и передачи данных.	**Управление**	
		Данные	
		Внутренний (Кластер)	
Маршрут по умолчанию (шлюз)	Сетевой шлюз, на который пакет отправляется в том случае, если маршрут к сети назначения пакета не известен		
Хост сервера Syslog *необязательно	Указание IP-адреса сервера для сбора syslog-информации разного уровня логирования		
SNMP пароль *необязательно	Слово или фраза, которая спрашивается для управления сетевыми устройствами (маршрутизатор, коммутатор)		
Domain name server *необязательно	IP-адрес сервера, используемый для DNS запроса		
Административные данные *необязательно	Логин и пароль для доступа к web-интерфейсу. После авторизации можно изменить		

5.2 Подключение кластера АПК InfoDiode PRO к корпоративной сети

5.2.1 Подключение к электросети, включение эл.питания АПК InfoDiode PRO

Подключите прокси-серверы, аппаратные компоненты кабелями эл. питания к эл. розетке и включите кнопку эл. питания на устройствах. Устройства готовы к эксплуатации.

5.2.2 Подключение серверов In-Proxy и Out-Proxy к корпоративной сети

1. Подключите интерфейс данных lan1 к сетевому оборудованию (или к конечному устройству) кабелем вида «витая пара» с коннекторами RJ-45.
2. Подключите интерфейс управления lan4 к сетевому оборудованию (или к конечному устройству) кабелем вида «витая пара» с коннекторами RJ-45.
3. Повторите эти действия с другими серверами.
4. Для каждой пары серверов In-Proxy и Out-Proxy необходимо кабелем вида «витая пара» с коннекторами RJ-45 (в комплекте) выполнить их соединение по внешним сетевым интерфейсам (по умолчанию, lan3).

5.2.3 Подключение серверов к аппаратным компонентам InfoDiode RACK double

Подключение InProxy-1:

Подключите внутренний интерфейс fc1 к разъему IN1 одного АК InfoDiode RACK double, интерфейс fc2 к разъему IN2 другого АК InfoDiode RACK double.

Подключение InProxy-2:

Подключите внутренний интерфейс fc1 к разъему IN1 одного АК InfoDiode RACK double, интерфейс fc2 к разъему IN2 другого АК InfoDiode RACK double.

Подключение OutProxy-1:

Подключите внутренний интерфейс fc1 к разъему OUT1 одного из АК InfoDiode RACK double, интерфейс fc2 к разъему OUT2 того же АК InfoDiode RACK double.

Подключение OutProxy-2:

Подключите внутренний интерфейс fc1 к разъему OUT1 другого АК InfoDiode RACK double, интерфейс fc2 к разъему OUT2 этого же АК InfoDiode RACK double.

Ниже на Рисунок 13 представлена схема подключения кластерной версии АПК InfoDiode PRO cluster к корпоративной сети:

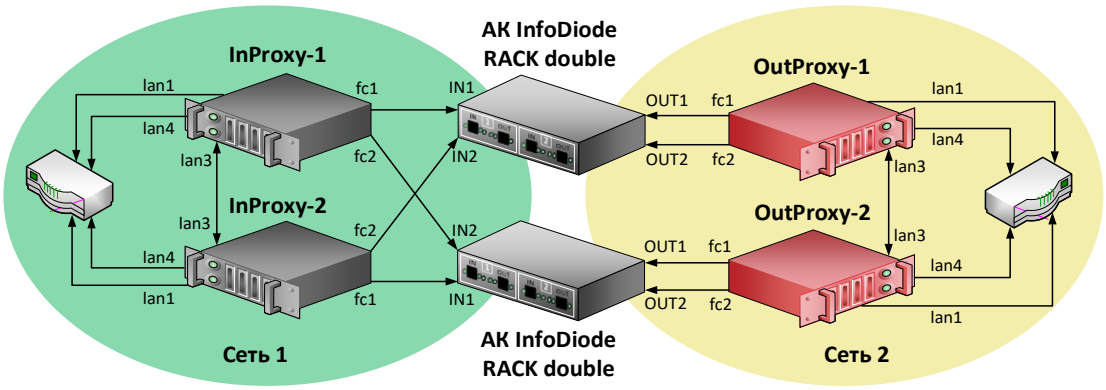


Рисунок 13. Схема подключения кластерной версии АПК InfoDiode PRO cluster к корпоративной сети.

5.2.4 Проверка и изменение конфигурации прокси-серверов

Для просмотра и изменения текущей конфигурации можно подключиться к InProxy и OutProxy тремя способами:

1. Подключить монитор и клавиатуру непосредственно к физическим серверам InProxy и OutProxy
2. По IPMI (необходима сетевая настройка на IPMI интерфейсе).
3. По SSH

При загрузке сервера заходим в BIOS - Server MGMT - BMC Network Configuration и указываем сетевые настройки (IP-адрес, маску, шлюз по умолчанию) для интерфейса IPMI. Подключаемся через веб-интерфейс, используя любой браузер с поддержкой java, в адресной строке которого вводим IP-адрес IPMI-интерфейса, и, после подключения проходим авторизацию с использованием имени пользователя и пароля, указанных в документации или заданных пользовательскими настройками (по умолчанию используется логин и пароль *admin/admin1234*).

Внимание! При первой авторизации в терминале (по IPMI или по прямому подключению с помощью клавиатуры и монитора) системы необходимо сменить пароль пользователя *root* на соответствующий рекомендуемым политикам безопасности. Для смены пароля авторизуйтесь как *root*, введите пароль *infodiode,* затем введите новый пароль в ответ на запрос системы. Запомните или зафиксируйте данный пароль согласно правилам и политикам безопасности для вашей организации.

Для доступа по SSH необходимо, чтобы предварительно был настроен IP-адрес на интерфейсе управление, маршрут по умолчанию. Подключитесь к серверу по IP-адресу интерфейса управления lan4. После подключения введите в SSH-консоли логин и пароль *diode/P@ssw0rd*.

Внимание! В составе дистрибутива присутствует утилита pwquality с соответствующим конфигурационным файлом, определяющим парольную политику (требования к сложности пароля установлены согласно требованиям регулятора для СЗИ УД4), а также утилита pam_faillock (определяет блокирование УЗ в случае некорректного ввода пароля и базовую защиту от bruteforce). С учетом этого в системе присутствуют значимые требования к сложности пароля, а нарушение политики может являться препятствием для запуска всей системы и может быть продиагностировано.

По умолчанию применены следующие требования парольной политики:

- В отношении качества пароля - "Длина пароля не менее восьми символов, алфавит пароля не менее 70 символов, пароль должен включать заглавные буквы, цифры и спецсимволы"

В отношении защиты от bruteforce:

- количество неправильных вводов – 4 попытки
- время измерения – 5 минут
- время блокировки - 30 минут

В случае если согласно требованиям организации необходимо применить более "мягкую" парольную политику в части качества пароля - следует внести изменения в файл (/etc/security/pwquality.conf).

После подключения к серверам In-proxy/Out-proxy:

1. Сохраняем текущую конфигурацию командой `infodiode-cli config save -f /tmp/cfg.xml -wp`
2. Чтобы редактировать текущую конфигурацию, откройте файл /tmp/cfg.xml с помощью текстового редактора vim.
3. Найдите блок <subsystem xmlns="urn:ru:amt:diode:config:1.0:network">...</subsystem> и измените сетевые параметры интерфейса управления lan4 и маршрута по-умолчанию (Рисунок 12)
4. Для применения конфигурации InfoDiode необходимо выполнить команду: `infodiode-cli config load -f cfg.xml`

```
    <hostname>inproxy-1-2.localdomain</hostname>
  - <data>
        <enabled>true</enabled>
        <device>lan1</device>
        <address>10.0.141.234/24</address>
        <ping>false</ping>
    </data>
  - <control>
        <enabled>true</enabled>
        <device>lan4</device>
        <address>10.0.144.234/24</address>
        <ping>true</ping>
        <autoneg>true</autoneg>
    </control>
  - <cluster>
        <enabled>true</enabled>
        <device>lan3</device>
        <address>172.20.0.2/24</address>
        <ping>false</ping>
    </cluster>
  </node>
</nodes>
- <routes>
    <route subnet="0.0.0.0/0" network="control" gateway="10.0.144.1"/>
</routes>
```

Рисунок 14. Вывод части конфигурационного файла в cli-консоли

Примечание.
/tmp/cfg.xml - Имя файла, куда будет выгружена текущая конфигурация ПО InfoDiode
-wp - выгрузка конфигурации с паролями

В данном примере:

lan1 – наименование интерфейса данных

lan4 - наименование интерфейса управления

lan3 – наименование внутреннего интерфейса кластера (ip-адрес задается по-умолчанию, в процессе эксплуатации не меняется)

10.0.144.234/24 - сетевой адрес интерфейса управления

10.0.144.1 - адрес шлюза по-умолчанию

6. Настройка АПК InfoDiode PRO

Настройка производится в web-интерфейсе сервера, доступ к которому можно получить, подключившись к серверу по его IP-адресу:

1. В строке браузера вводим адрес интерфейса управления, проходим аутентификацию (см. Рисунок 15).

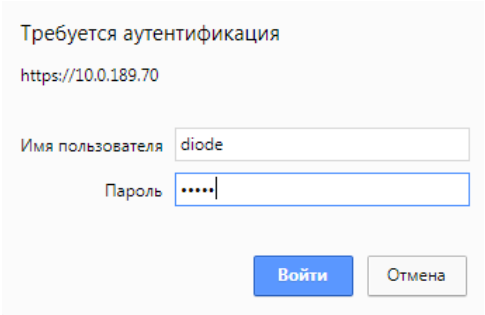


Рисунок 15. Аутентификация

Примечание. Перед любой настройкой необходимо включать режим «Изменить конфигурацию».

2. Заходим в «Параметры сервера», переходим в «Сетевые интерфейсы». При необходимости включаем интерфейс «данные» и изменяем его настройки: выбираем нужный порт и указываем ip-адрес.
3. В настройке «Сетевые маршруты» в случае необходимости можно указать статические маршруты для интерфейсов управления и данных.

Примечание. Чтобы клиент мог передавать трафик на интерфейс данных InProxy, на самом сервере InProxy необходим маршрут через интерфейс данных к источнику трафика, в том случае, если источник трафика не расположен в одной сети с интерфейсом данных (например, интерфейс данных в сети 10.0.141.0/24, а источник трафика - в 10.0.183.0/24), а маршрут по умолчанию идет не через интерфейс данных. В случае отсутствия маршрута трафик от источника будет отфильтрован rp_filter

4. Для кластерной конфигурации указываем виртуальные IP-адреса интерфейсов данные/управления

6.1 Настройка передачи файлов по FTP

1. На серверах In-Proxy и Out-Proxy во вкладке «Управление пользователями» добавляем группу и пользователя, выбрав группу, к которой он будет определен.
2. Во вкладке «Прокси-сервисы»:
   – Включаем «Общие настройки».
   – В настройке «FTP» включаем конфигурацию FTP.

- На сервере In-Proxy в настройке «Папки общего доступа» нажимаем на «сохранить и добавить» и вводим название папки и группу, для которой она будет доступна.
- На сервере Out-Proxy в настройке «Передача файлов» добавляем канал передачи (название канала передачи должно совпадать с названием папки на In-Proxy сервере). Указываем все данные пользователя для аутентификации на внешний сервер, IP-адрес внешнего сервера, на который будут приходить данные от Out-Proxy сервера.

3. Сохраняем настройки и применяем конфигурацию.
4. Проверяем правильную настройку FTP во вкладке «Мониторинг»:
   - На In-Proxy/Out-Proxy сервере в настройке «История сообщений» выбираем канал передачи, добавленный для FTP передачи, и переходим на него.
   - Отправляем тестовое сообщение с In-Proxy на Out-Proxy / с Out-Proxy на конечное устройство будет отправлено самостоятельно, если настроена пересылка на удаленный хост. Отправка осуществляется нажатием кнопки «Отправить сообщение».
   - Нажимаем на кнопку «Обновить», если сообщение отправлено, в столбце «Байт передано» выводится объем переданного сообщения в зеленом окне, если не отправилось – объем переданного сообщения, равный 0, в прозрачном окне.

Примечание. Учетная запись пользователя, заданная для папки общего доступа на In-Proxy сервере, будет использована для аутентификации между FTP-клиентом и FTP-сервером In-Proxy, а учетная запись пользователя, назначенная в свойствах канала передачи на вкладке «передача файлов» на сервере Out-Proxy - для аутентификации на удаленном FTP-сервере

6.2 Настройка потоковой передачи трафика по UDP

1. Во вкладке «Потоковые сервисы»:
   - Переходим в настройку «UDP туннелирование» и включаем ее на всех серверах In-Proxy и Out-Proxy.
   - Добавляем правило туннелирования UDP-трафика на InProxy нажатием кнопки «Добавить правило» и указываем IP-адрес и порт источника, IP-адрес (интерфейса In-Proxy сервера АПК InfoDiode PRO, на который планируется передача трафика) и порт назначения трафика, при необходимости указываем правила NAT (типовое использование – сокрытие адреса источника и назначения).
   - Добавляем правило туннелирования UDP-трафика на OutProxy нажатием кнопки «Добавить правило» и указываем IP-адрес и порт источника (которые должны соответствовать значениям в правиле NAT, в случае если правила NAT используются) и IP-адрес и порт назначения трафика (которые должны соответствовать значениям в правиле NAT, в случае если правила NAT используются). При необходимости указываем правила NAT (типовое использование – адрес интерфейса данных Out-Proxy подставляем как источник, и адрес конечного хоста как адрес назначения).
2. Заходим в «Параметры сервера», переходим в «Сетевые маршруты».

- На In-Proxy сервере добавляем маршрут, указывая подсеть назначения в соответствии с правилами UDP туннелирования и выбираем сетевой интерфейс «Диод», через который будет направлен потоковый трафик на OutProxy.
- На Out-Proxy сервере добавляем один маршрут, указывая подсеть назначения в соответствии с правилами UDP туннелирования, адрес шлюза сети, в которой расположен интерфейс данных Out-Proxy сервера, выбираем сетевой интерфейс «Данные». Добавляем второй маршрут для приема UDP-трафика с In-Proxy сервера, указывая подсеть источника в соответствии с правилами UDP туннелирования, выбираем сетевой интерфейс «Диод».
- Сохраняем настройки и применяем конфигурацию.

6.2.1 Пример настройки передачи.

В данном примере выполняется передача UDP-трафика от источника с адресом zz.zz.zz.zz/zz к приемнику с адресом aa.aa.aa.aa/aa. В процессе передачи применяются правила NAT для адреса назначения.

В web-интерфейсе In-Proxy сервера выполняются следующие настройки:

1. Добавляем правило туннелирования UDP-трафика:
   - Указываем IP-адрес/подсеть источника трафика: zz.zz.zz.zz/zz.
   - Указываем IP-адрес назначения (IP-адрес интерфейса данных In-Proxy сервера) и порт: xx.xx.xx.xx/xx:xx.
   - Указываем правила NAT: источника: dd.dd.dd.dd/dd, назначения: yy.yy.yy.yy/yy
2. Указываем сетевой маршрут:
   - Задаем подсеть назначения: yy.yy.yy.yy/yy
   - Выбираем сетевой интерфейс: Диод.

В web-интерфейсе Out-Proxy сервера выполняются следующие настройки:

1. Добавляем правило туннелирования UDP-трафика:
   - Указываем IP-адрес/подсеть источника трафика: dd.dd.dd.dd/dd.
   - Задаем IP-адрес и порт назначения: yy.yy.yy.yy/yy:yy
   - Задаем правила NAT: источника: bb.bb.bb.bb, назначения: aa.aa.aa.aa.
2. Указываем сетевые маршруты:
   1) Задаем подсеть источника для приема UDP-трафика: dd.dd.dd.dd/dd
      Выбираем сетевой интерфейс: Диод.
   2) Задаем подсеть назначения: aa.aa.aa.aa/aa

      Выбираем сетевой интерфейс: Данные.

6.3 Настройка передачи электронной почты

1. На In-Proxy сервере во вкладке «Прокси-сервисы» Включаем настройку «Электронная почта»
2. На In-Proxy сервере в настройке «Электронная почта» выбираем группу доступа, порт, максимальный размер письма.
3. На Out-Proxy сервере в настройке «Электронная почта» указываем IP-адрес почтового сервера в поле «Хост», порт, логин и пароль пользователя для авторизации на почтовом сервере.

4. Сохраняем настройки и применяем конфигурацию.
5. Проверяем правильную настройку передачи почты во вкладке «Мониторинг»:
3. На In-Proxy/Out-Proxy сервере в настройке «История сообщений» выбираем канал передачи «mail», и переходим на него.
4. Отправляем тестовое сообщение с In-Proxy на Out-Proxy/ с Out-Proxy на конечное устройство нажатием кнопки «Отправить сообщение».
5. Нажимаем на кнопку «Обновить», если сообщение отправлено, в столбце «Байт передано» выводится объем переданного сообщения в зеленом окне, если не отправилось – объем переданного сообщения, равный 0, в прозрачном окне.