ООО «НПО «ФРАКТЕЛ»

УТВЕРЖДЕН

РКДЕ.5014107-05 0134–ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МЕЖСЕТЕВОГО ЭКРАНА ССПТ-2 ВЕРСИИ 1.3

Руководство администратора

РКДЕ.5014107-05 0134

Листов 366

Санкт-Петербург

2014

Подп. и дата	
Инв. № дубл.	
Взам.инв.№	
Подп. и дата	
Инв. № подл.	

№ изм.	**Подпись**	**Дата**

© **ООО «НПО «ФРАКТЕЛ»**, 2006 - 2014.
Ул. Политехническая, д. 28А, Санкт-Петербург, 194064 Российская Федерация
Телефон/Факс: **+7 (812)-552-4512**
Документ: AM_SSPT-2(1.3-p1.2).pdf
E-mail: **info@fractel.ru** WWW: **http://www.fractel.ru**

№ изм.	**Подпись**	**Дата**

АННОТАЦИЯ

Настоящее руководство содержит описание общих принципов функционирования, порядок настройки и управления **Межсетевым экраном ССПТ-2 версии 1.3** РКДЕ.401350.005 исполнений РКДЕ.401350.005-01 - РКДЕ.401350.005-94 (далее – ССПТ-2), функционирующим под управлением встроенной операционной системы и программного обеспечения (МЕЖСЕТЕВОЙ ЭКРАН ССПТ-2 ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ РКДЕ.5014107-05 01).

Руководство содержит описание общих принципов функционирования, порядок настройки и управления ПО ССПТ-2 в составе межсетевого экрана ССПТ-2.

Руководство предназначено для специалистов в области сетевой безопасности и администраторов сетей, использующих ССПТ-2 для решения вопросов, связанных с ограничением доступа к информационным и сетевым ресурсам в сетях Ethernet.

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ 8

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ ПО ССПТ-2 10

2. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ССПТ-2 12

2.1. Управление доступом 12

2.1.1. Пакетная фильтрация 12
2.1.2. Контроль соединений 16
2.1.3. Сокрытие субъектов (объектов) и/или прикладных функций защищаемой сети и трансляция сетевых адресов 18
2.1.4. Правила фильтрации и фильтрация с учетом даты/времени 18
2.1.5. Технология скрытной фильтрации 23

2.2. Идентификация и аутентификация 24

2.3. Регистрация 24

2.4. Администрирование: идентификация и аутентификация 28

2.4.1. Локальное администрирование 28
2.4.2. Удаленное администрирование 29
2.4.3. Разграничение прав пользователей 33

2.5. Администрирование: регистрация действий 34

2.6. Администрирование: простота использования 45

2.7. Целостность 46

2.8. Восстановление и защита от сбоев 47

2.9. Тестирование 48

2.10. Режимы работы 49

2.10.1. Автономный старт 49
2.10.2. Трансляция трафика 49
2.10.3. Режим высокой готовности 49
2.10.4. Режим скрытной фильтрации 50
2.10.5. Режим трансляции сетевых адресов 50

2.11. Устойчивость к сетевым атакам 51

3. АДМИНИСТРИРОВАНИЕ ССПТ-2 - ПОДГОТОВКА К РАБОТЕ 54

3.1. Комплект поставки 54

3.2. Кабели и соединения 54

3.3. Включение в компьютерную сеть 55

3.4. Требования к управляющему компьютеру 57

4. АДМИНИСТРИРОВАНИЕ ССПТ-2 – ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ 58

4.1. Запуск и вход в систему 58

4.1.1. Авторизация 58
4.1.2. Использование для подключения к ССПТ-2 системной консоли 61
4.1.3. Использование для подключения к ССПТ-2 последовательного порта (COM) 62
4.1.4. Использование для подключения к ССПТ-2 управляющего сетевого интерфейса (Eth.C) 63

4.2. Наборы правил 64

4.2.1. Предустановленные дополнительные наборы правил 64
4.2.2. Инициализация текущей конфигурации ССПТ-2 значениями по умолчанию 65

4.3. Останов и перезагрузка управляющей операционной системы 65

4.4. Командный интерфейс администратора 66

4.5. Управление списком пользователей ССПТ-2 81

4.6. Системные настройки 84

4.6.1. Проверка целостности 85
4.6.2. Поверка аппаратного обеспечения и системных ресурсов 88
4.6.3. Установка системного времени и даты 90
4.6.4. Использование протокола NTP 92

4.7. Структура и редактирование правил фильтрации 93

4.7.1. Структура правил фильтрации 93
4.7.2. Редактирование правил в таблицах 96
4.7.3. Группы VLAN 97
4.7.4. Интервалы времени 99
4.7.5. MAC-правила фильтрации 103
4.7.6. ARP-правила фильтрации 109
4.7.7. Временные IP-правила фильтрации 116
4.7.8. IP-правила фильтрации 121
4.7.9. IPX-правила фильтрации 132
4.7.10. Правила фильтрации прикладного уровня 139
4.7.11. Правила фильтрации протокола HTTP 141
4.7.12. Правила фильтрации протокола SMTP 148

4.7.13. Правила фильтрации протокола FTP 153
4.7.14. Правила фильтрации сервисов SQL 159
4.7.15. Правила фильтрации других прикладных протоколов 165
4.7.16. Работа с правилами фильтрации 170
4.7.17. Дополнительные наборы правил 173
5. АДМИНИСТРИРОВАНИЕ ССПТ-2 – РЕГИСТРАЦИЯ 177
5.1. Общие положения 177
5.2. Журнал регистрации событий 178
5.3. Журнал регистрации трафика 189
5.3.1. Регистрация пакетов 189
5.3.2. Регистрация сессий 192
5.4. Журнал регистрации системных сообщений 195
5.5. Выгрузка журналов на FTP сервер 197
5.6. Выгрузка системных сообщений на SYSLOG сервер 198
6. АДМИНИСТРИРОВАНИЕ ССПТ-2 – ОСНОВНЫЕ РЕЖИМЫ 200
6.1. Режимы фильтрации 200
6.1.1. Режим пакетной фильтрации 201
6.1.2. Режим управления сессиями 205
6.1.3. Режим трансляции сетевых адресов 228
6.1.4. Управление процессом фильтрации 253
6.2. Трансляция (зеркалирование) трафика 254
6.3. Система фильтрации высокой готовности на основе ССПТ-2 256
6.3.1. Организация системы фильтрации высокой готовности в режиме «активный/резервный» 257
6.3.2. Организация системы фильтрации высокой готовности в режиме балансировки 265
6.3.3. Организация системы фильтрации высокой готовности в режиме Spanning Tree 272
6.3.4. Синхронизация конфигурации и правил фильтрации 278
7. АДМИНИСТРИРОВАНИЕ ССПТ-2 – WEB ИНТЕРФЕЙС 279
7.1. Общие положения 279
7.2. Вход в систему, главное окно 280
7.3. Настройки конфигурации и режимов 284
7.3.1. Системные настройки 284
7.3.2. Управление пользователями 291
7.3.3. Настройки интерфейсов 294

7.3.4. Настройка устройства для работы в системе фильтрации высокой готовности 298
7.3.5. Настройка устройства для работы в режиме трансляции адресов (NAT) 300
7.3.6. Настройка устройства для идентификации пользователей через RADIUS - сервер .. 307
7.4. Правила фильтрации 309
7.4.1. Управление глобальными правилами и наборами правил 309
7.4.2. Управление MAC правилами 313
7.4.3. Управление ARP правилами 317
7.4.4. Управление IPX правилами 322
7.4.5. Управление IP правилами 326
7.4.6. Управление временными IP правилами 332
7.4.7. Управление правилами фильтрации прикладного уровня 335
7.4.8. Управление группами VLAN 339
7.4.9. Управление интервалами времени 342
7.4.10. Возврат к предыдущему состоянию правил фильтрации и статистика использования правил 345
7.5. Управление сессиями 347
7.6. Регистрация 349
7.7. Аутентификацией входящих и исходящих запросов 360
7.8. Остановка процесса фильтрации и выход из системы 364

СПИСОК СОКРАЩЕНИЙ

АС – автоматизированная система

ЛВС – локальная вычислительная сеть

ПО – программное обеспечение

УЦ – Удостоверяющий Центр

ARP – Address Resolution Protocol

BPF – Berkeley Packet Filter

BOFL – Breath OF Life

CSS – Cascading Style Sheets

ECN - Explicit Congestion Notification

FTP – File Transfer Protocol

HTML – HyperText Markup Language

HTTP – HyperText Transfer Protocol

ICMP – Internet Control Message Protocol

IP – Internet Protocol

IPX – Internetwork Packet eXchange

LAN – Local Area Network

MAC – Media Access Control

NAT – Network Address Translation

NTP – Network Time Protocol

OUI – Organizational Unique Identifier

POP3 – Post Office Protocol 3

RARP – Reverse Address Resolution Protocol

RADIUS – Remote Authentication Dial In User Service

SAP – Service Accesss Point

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Management Protocol

TCP – Transmission Control Protocol

TLS – Transport Layer Security

TOS – Type Of Service

TTL – Time To Live

UDP – User Datagaram Protocol

URL – Universal Resource Locator

VLAN – Virtual Local Area Network

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ ПО ССПТ-2

ПО ССПТ-2 предназначено для работы в составе программно-аппаратного средства "Межсетевой экран ССПТ-2" РКДЕ.401350.005. Межсетевой экран ССПТ-2 (далее – изделие) выполнен в виде локального (однокомпонентного) устройства, реализующего контроль за информацией, которая циркулирует между отдельными подсистемами обработки информации внутри автоматизированной системы (АС) и/или между АС. Изделие обеспечивает защиту информации в АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения об ее распространении в (из) АС. Изделие используется для защиты АС, в которых обрабатывается информация одинакового предельно допустимого уровня конфиденциальности или секретности.

Изделие применяется для разделения сегментов информационной сети внутри или между АС классов 3А-1В, с целью обеспечения защиты информации от несанкционированного доступа (НСД) посредством:

а) фильтрации сетевых пакетов, передаваемых в локальных вычислительных сетях (ЛВС) внутри АС или между АС. Фильтрация пакетов (передача пакета в защищаемую ЛВС или из неё, или запрет передачи - удаление пакета) осуществляется на основе анализа параметров заголовка пакета по совокупности критериев, устанавливаемых правилами фильтрации для разных уровней модели взаимодействия открытых систем (OSI);

б) управления виртуальными транспортными соединениями между отдельными узлами ЛВС внутри или между АС. Управление виртуальными транспортными соединениями (разрешение или запрет соединения) осуществляется на основе результатов анализа параметров соединений и/или запросов на установление соединений;

в) контроля данных передаваемых на прикладном уровне модели взаимодействия открытых систем. Контроль данных (анализ данных и их передача или запрет передачи) осуществляется по заданным критериям, в том числе, с учетом направ-

ления потока данных.

Предусмотрена реализация изделия на ряде аппаратных средств, в виде исполнений, отличающихся друг от друга типоразмерами корпуса, количеством и пропускной способностью фильтрующих интерфейсов (исполнения РКДЕ.401350.005-01 - РКДЕ.401350.005-94).

Изделие может использоваться в ЛВС, построенных на базе технологии Ethernet с пропускной способностью 10/100/1000/10000 Мбит/с.

Внимание!!! Изделие не предназначено для выполнения функций маршрутизатора, и не может его заменить.

2. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ССПТ-2

2.1. Управление доступом

2.1.1. Пакетная фильтрация

ПО ССПТ-2 обеспечивает пакетную фильтрацию сетевого трафика, т.е. анализ пакетов информации (по полям заголовков) по совокупности критериев и принятие решения о разрешении или запрете их передачи в защищаемый сегмент сети или из него на основе заданных правил. Фильтрация сетевого трафика может осуществляться на различных уровнях сетевого взаимодействия.

ПО ССПТ-2 обеспечивает:

- фильтрацию проходящих через межсетевой экран ССПТ-2 объектов на сетевом уровне (пакетов) и фильтрацию по служебной информации (сетевым адресам);

- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

- фильтрацию с учетом любых значимых полей сетевых пакетов.

На **канальном уровне** ПО ССПТ-2 обеспечивает анализ и пакетную фильтрацию по полям заголовков кадров:

1) протокола Ethernet II (Ethernet DIX), фильтрация осуществляется по содержанию следующих полей заголовка кадра канального уровня:

- MAC - адрес отправителя;

- MAC - адрес получателя;

- код протокола, пакеты которого инкапсулированы непосредственно в кадр протокола Ethernet II (IP v.4, IP v.6, ARP, RARP, IPX и др.);

2) протокола IEEE 802.3/LLC, фильтрация осуществляется по содержанию следующих полей заголовка кадра канального уровня:

- MAC - адрес отправителя;

- MAC - адрес получателя;

- код протокола, пакеты которого инкапсулированы непосредственно в кадр протокола IEEE 802.3/LLC (IP, IPX, STP);

3) протокола IEEE 802.3 Raw, фильтрация осуществляется по содержанию следующих полей заголовка кадра канального уровня:

- MAC - адрес отправителя;

- MAC - адрес получателя;

4) протокола IEEE 802.3-SNAP, фильтрация осуществляется по содержанию следующих полей заголовка кадра канального уровня:

- MAC - адрес отправителя;

- MAC - адрес получателя;

- код производителя (OUI) и код типа протокола (CDP и др.), пакеты которого инкапсулированы непосредственно в кадр протокола IEEE 802.3-SNAP;

5) пакетов протокола IEEE 802.1p/Q (VLAN) по идентификатору/группе идентификаторов виртуальной локальной вычислительной сети (ВЛВС).

6) пакетов протоколов ARP/RARP, фильтрация осуществляется по содержанию следующих полей в заголовке ARP - пакета:

- MAC-адрес отправителя;

- IP-адрес отправителя;

- MAC-адрес получателя;

- IP-адрес получателя;

- тип сообщения (запрос, ответ).

На **сетевом уровне** ПО ССПТ-2 обеспечивает анализ и пакетную фильтрацию по полям заголовков пакетов:

1) для протокола IPX, фильтрация осуществляется по содержанию следующих полей в заголовке IPX - пакета:

- адрес сети/узла источника;

- сокет (идентификатор инкапсулированного протокола) источника;

- адрес сети/узла приемника;

- сокет (идентификатор инкапсулированного протокола) приемника;

- тип пакета;

2) для протокола IP v.6, фильтрация осуществляется по коду протокола в режиме разрешить/пропустить;

3) для протокола IP v.4, фильтрация осуществляется по содержанию следующих полей в заголовке пакета:

- IP-адрес источника;

- IP-адресприемника;

- поле *Тип сервиса* (Type of Service) и его субполя: *Приоритет* (Precedence), *Задержка* (Delay), *Пропускная способность* (Throughput), *Надежность* (Reliability), *ECN;*

- длина пакета;

- флаг фрагментации MF и смещение фрагмента;

- время жизни пакета (TTL);

- код протокола, пакеты которого инкапсулированы непосредственно в IP - пакеты.

При этом обеспечивается возможность фильтрации пакетов протокола IP v.4 с инкапсулированными сообщениями протокола ICMP, фильтрация осуществляется по следующим параметрам:

1) тип ICMP-сообщения;

2) код ICMP-сообщения.

На **транспортном уровне** ПО ССПТ-2 обеспечивает фильтрацию следующих протоколов транспортного уровня, использующих на сетевом уровне протокол IP v.4:

1) протокол TCP, фильтрация осуществляется по следующим параметрам:

- порт источника;

- порт назначения;

- флаги управления потоком (фильтрация по инициатору соединения);

2) протокол UDP, фильтрация осуществляется по следующим параметрам:

- порт источника;

- порт назначения.

На **прикладном уровне** ПО ССПТ-2 обеспечивает фильтрацию следующих протоколов прикладного уровня:

1) HTTP;

2) SMTP;

3) FTP;

4) протоколы реляционных систем управления базами данных (СУБД) (Oracle SQL*Net, MS-SQL, PostgreSQL, MySQL);

5) других прикладных протоколов, заданных кодом в соответствии с RFC 1700.

Фильтрация осуществляется с учетом направления потока данных по результатам анализа (с учетом регистра) следующих данных:

1) для протокола HTTP:

- имя или фрагмент имени сетевого устройства (хоста), к которому происходит обращение;

- HTTP – метод, используемый при обращении;

- имя или фрагмент имени запрашиваемого файла;

- данные (последовательность алфавитно-цифровых символов ASCII, до 64 символов);

- данные со смещением (последовательность бинарных данных длиной до 16 байт, расположенная в указанном месте прикладных данных);

2) для протокола SMTP:

- почтовый адрес или фрагмент почтового адреса отправителя;

- почтовый адрес или фрагмент почтового адреса получателя;

- данные (последовательность алфавитно-цифровых символов ASCII, до 64 символов);

- данные со смещением (последовательность бинарных данных длиной до 16 байт, расположенная в указанном месте прикладных данных);

3) для протокола FTP:

- команды FTP;

- имя или фрагмент имени файла, передаваемого по протоколу FTP;

- имя или фрагмент имени пользователя, обращающегося к серверу FTP;

- пароль или фрагмент пароля пользователя, обращающегося к серверу FTP;

- данные (последовательность алфавитно-цифровых символов ASCII, до 64 символов);

- данные со смещением (последовательность бинарных данных длиной до 16 байт, расположенная в указанном месте прикладных данных);

4) для протоколов обращений к системам управления базами данных:

SQL – запрос (команда и ее параметры) или фрагмент запроса;

- данные (последовательность алфавитно-цифровых символов ASCII, до 64 символов);

- данные со смещением (последовательность бинарных данных длиной до 16 байт, расположенная в указанном месте прикладных данных);

5) для других прикладных протоколов:

- данные (последовательность алфавитно-цифровых символов ASCII, до 64 символов);

- данные со смещением (последовательность бинарных данных длиной до 16 байт, расположенная в указанном месте прикладных данных).

На всех уровнях фильтрации ПО ССПТ-2 обеспечивает возможность фильтрации пакетов с учетом даты/времени (т.е. определения временного интервала действия процесса фильтрации по заданным параметрам).

2.1.2. Контроль соединений

ПО ССПТ-2 обеспечивает возможность выявления среди общего трафика потоков данных (сессий), в том числе виртуальных соединений, между парами адресатов (инициатор соединения – клиент, второй участник сессии - сервер) и контроль корректности последовательностей пакетов в пределах этого потока (кон-

троль сессий). Сессии формируются на основании установок администратора при определении условий фильтрации IP-пакетов. Контроль сессий поддерживается для следующих протоколов:

1) TCP, по-умолчанию включен режим глубоко контроля TCP-сессий, при котором осуществляется:

- контроль неизменности параметров отправителя и получателя пакетов на протяжении всей сессии;

- контроль корректности переходов между состояниями виртуального соединения TCP в соответствии с флагами управления;

- контроль корректности номеров последовательностей;

При отключенном режиме глубокого контроля TCP-сессий осуществляется только контроль неизменности параметров отправителя и получателя пакетов на протяжении всей сессии.

2) UDP, при этом осуществляется контроль неизменности параметров отправителя и получателя пакетов на протяжении всей сессии;

3) ICMP (только для режима утилиты ping), при этом осуществляется контроль неизменности параметров отправителя и получателя пакетов, и неизменность значения поля идентификатора на протяжении всей сессии.

ПО ССПТ-2 обеспечивает возможность управления сессиями:

- возможность возобновления неактивной в течение заданного времени (тайм-аута) не завершенной сессии если не произошло корректного прекращения соединения;

- прекращение незавершенной неактивной сессии после окончания заданного тайм-аута;

- возможность прекращения сессии по результатам анализа данных протоколов прикладного уровня;

- возможность прекращения сессии администратором.

2.1.3. Сокрытие субъектов (объектов) и/или прикладных функций защищаемой сети и трансляция сетевых адресов

Для обеспечения сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети и трансляции сетевых адресов в ПО ССПТ-2 предусмотрена возможность выполнения обратимого преобразования адресов (функция NAT).

ПО ССПТ-2 обеспечивает возможность выполнения обратимого преобразования адресов, но только для одной, фиксированной для всех исполнений, пары фильтрующих интерфейсов (Eth.0 и Eth.1). При этом, один из этих фильтрующих интерфейсов (Eth.0) определен как внешний интерфейс (для подключения внешней сети), а другой (Eth.1) - как внутренний интерфейс (для подключения защищаемой сети). Остальные фильтрующие интерфейсы (при их наличии) определены, как интерфейсы демилитаризованной зоны.

Функция обратимого преобразования адресов выполняется по установке администратора только при обработке пакетов сессий, при условии, что инициаторами соединений (клиентами) являются сетевые устройства защищаемого сегмента, подключенного к интерфейсу Eth.1. Поэтому, при поступлении IP- пакета на интерфейс Eth.1 производится его проверка на соответствие установленным для внутреннего интерфейса правилам фильтрации. Функция обратимого преобразования выполняется только тогда, когда по результатам проверки пакета создана сессия по установленному IP – правилу или контролируемый IP- пакет принадлежит установленной ранее сессии. Функция обратимого преобразования адресов выполняется и в том случае, если производится обращение извне на установленный IP интерфейс Eth.0 и на внешний порт, указанный администратором в таблице соответствия.

2.1.4. Правила фильтрации и фильтрация с учетом даты/времени

Пакетная фильтрация и управление сессиями в ССПТ-2 обеспечивается специальным программным модулем ПО ССПТ-2 – **пакетным фильтром** на основе определяемых администратором ССПТ-2 правил фильтрации. Правила фильтрации определяют значения контролируемых параметров (параметров фильтрации) и

обеспечивают возможность задания списка параметров (как диапазона, так и одиночных). Правила фильтрации имеют многоуровневую структуру в соответствии с уровнями сетевого взаимодействия, на которых выполняется пакетная фильтрация.

Решение по фильтрации принимается для каждого кадра (сетевого пакета) в соответствии с установленными администратором правилами фильтрации. Определены следующие типы правил фильтрации:

1) **MAC- правила**, которые определяют:

- значения анализируемых параметров для фильтрации кадров протоколов Ethernet II (Ethernet DIX), IEEE 802.3/LLC, IEEE 802.3 Raw, IEEE 802.3-SNAP;

- значения анализируемых параметров пакетов протокола IEEE 802.1p/Q (VLAN);

- интервал времени, в течение которого правило используется в процессе фильтрации;

- действие, выполняемое над кадром или пакетом;

- необходимость регистрации информации о кадре или пакете;

2) **ARP- правила**, которые определяют:

- значения анализируемых параметров для фильтрации пакетов протоколов ARP/RARP;

- значения анализируемых параметров пакетов протокола IEEE 802.1p/Q (VLAN);

- интервал времени, в течение которого правило используется в процессе фильтрации;

- действие, выполняемое над пакетом;

- необходимость регистрации информации о пакете;

3) **IPX- правила**, которые определяют:

- значения анализируемых параметров для фильтрации пакетов протокола IPX;

- значения анализируемых параметров пакетов протокола IEEE 802.1p/Q (VLAN);

- интервал времени, в течение которого правило используется в процессе фильтрации;

- действие, выполняемое над пакетом;

- необходимость регистрации информации о пакете;

4) **IP- правила**, которые определяют:

- значения анализируемых параметров для фильтрации пакетов протокола IP версии 4;

- значения анализируемых параметров пакетов протокола IEEE 802.1p/Q (VLAN);

- значения анализируемых параметров пакетов протокола IP версии 4 с инкапсулированными сообщениями протокола ICMP;

- значения анализируемых параметров пакетов протокола IP версии 4 с инкапсулированными сегментами протокола TCP;

- значения анализируемых параметров пакетов протокола IP версии 4 с инкапсулированными дейтограммами протокола UDP;

- условия формирования и контроля параметров сессии;

- значение допустимого тайм-аута неактивности сессии;

- правила прикладного уровня, используемые для фильтрации пакетов на прикладном уровне при контроле сессии;

- интервал времени, в течение которого правило используется в процессе фильтрации;

- действие, выполняемое над пакетом;

- необходимость регистрации информации о пакете или сессии;

5) **правила прикладного уровня**, которые определяют:

- значения анализируемых данных протоколов прикладного уровня;

- действие, выполняемое над пакетом или сессией;

- необходимость регистрации информации о пакете или сессии.

ПО ССПТ-2 обеспечивает следующий порядок применения правил фильтрации:

1) MAC- правила;

2) ARP-, IPX- или IP – правила, в зависимости от типа инкапсулированного в кадр протокола;

3) правила прикладного уровня, в зависимости от установок (списка правил прикладного уровня) в IP – правиле.

Для правил фильтрации предусмотрена возможность выполнения следующих действий:

1) передача пакета на проверку соответствия правилам следующего уровня фильтрации (если следующий уровень фильтрации не предусмотрен, то осуществляется передача пакета на выходные сетевые фильтрующие интерфейсы);

2) передача пакета на выходные сетевые фильтрующие интерфейсы изделия, заданные в правиле фильтрации;

3) запрет передачи (удаление) пакета через выходные сетевые интерфейсы изделия, заданные в правиле фильтрации.

После проверки кадра на соответствие установленному MAC - правилу, ПО ССПТ-2 обеспечивает возможность передачи кадра на проверку соответствия правилам следующего уровня фильтрации (ARP, IP или IPX), если параметры проверяемого кадра соответствуют установленному MAC- правилу.

После проверки кадра на соответствие установленному IP - правилу, ПО ССПТ-2 обеспечивает возможность передачи IP - пакета на проверку соответствия правилам прикладного уровня, если параметры проверяемого пакета соответствуют установленному IP- правилу.

ПО ССПТ-2 обеспечивает возможность установки в каждой группе до 1024 правил фильтрации каждого типа. Каждое правило имеет номер. Номер правила определяется как целое число в диапазоне значений от 1 до 65535. Не допускается существование нескольких правил фильтрации одного типа с одинаковыми номерами.

ПО ССПТ-2 обеспечивает возможность отключения без удаления любого из MAC-, ARP-, IPX-, IP-правила и правила прикладного уровня. Неактивные правила

не рассматриваются при анализе заголовков пакетов.

MAC-, ARP-, IPX- и IP-правила фильтрации могут быть условными и безусловными. Безусловные правила фильтрации (если они имеют статус "активно") активны всегда, т.е. в течение всего времени работы изделия. Условные правила фильтрации (если они имеют статус "активно") активны только в определенные промежутки времени. Эти промежутки времени носят название интервалов времени, которые задаются в отдельной таблице интервалов времени. Может быть определено до 1024 интервалов времени. Каждый интервал времени имеет номер. Номер интервала определяется как целое число в диапазоне значений от 1 до 65535. Не допускается существование нескольких интервалов времени с одинаковыми номерами.

Для типов MAC-, ARP-, IPX- и IP-правил фильтрации предусмотрены MAC-, ARP-, IPX- и IP - глобальные правила. Глобальное правило каждого типа применяется в том случае, когда значения полей заголовков обрабатываемого в данный момент времени кадра или пакета не удовлетворяют ни одному из существующих правил данной группы. В глобальных правилах задается действие (удалить или пропустить), выполняемое над таким пакетом. Глобальные правила фильтрации всегда являются безусловными, и их нельзя удалить.

Первоначально (первое включение изделия) в изделии нет установленных правил фильтрации, а все глобальные правила предписывают удаление сетевых пакетов. Таким образом, при первом включении изделие не пропускает сетевые пакеты через свои интерфейсы.

ПО ССПТ-2 обеспечивает возможность удаления любого из установленных ранее MAC-, ARP-, IPX-, IP-правил и правил прикладного уровня.

Для учета в основных правилах фильтрации идентификаторов VLAN трафика (IEEE 802.1p/Q) ПО ССПТ-2 обеспечивает возможность установки вспомогательных структур - VLAN групп.

Для противодействия сетевым атакам дополнительно могут быть установлены временные IP- правила. Особенности временных IP – правил заключаются в

том, что:

1) IP- пакеты проверяются на соответствие временным IP- правилам перед проверкой на соответствие основным IP- правилам;

2) временные IP- правила только удаляют пакеты, удовлетворяющие их параметрам;

3) временные IP- правила не сохраняются при перезагрузке или отключении изделия и не могут быть деактивированы.

Временные IP- правила определяют IP-адреса источника/ приемника IP – пакета и порты источника/ приемника IP –пакета. ПО ССПТ-2 обеспечивает возможность удаления любого из установленных ранее временных IP- правил.

2.1.5. Технология скрытной фильтрации

Эффективность применения ССПТ-2 достигается за счет использования технологии скрытной фильтрации (режим “stealth”) – инновационного решения, защищенного Патентом РФ № 2214623, позволяющего скрывать для средств удаленного сетевого мониторинга место расположения ССПТ-2, что повышает надежность функционирования и позволяет эффективно наращивать производительность системы информационной безопасности.

Основные особенности применения режима “stealth” следующие:

1) фильтрующие интерфейсы ССПТ-2, подключаемые с защищаемым сегментам ЛВС, работают в режиме **приема и обработки всего трафика**, передаваемого в данных сегментах;

2) пакет, прошедший обработку подсистемой фильтрации ССПТ-2 и передаваемый на любой из выходных фильтрующих интерфейсов, **всегда оставляется без изменения** – не изменяются ни заголовки протоколов, ни данные.

Применение режима “stealth” позволяет устанавливать межсетевые экраны в существующие ЛВС без изменения политики маршрутизации, так как использование ССПТ-2 в любом сегменте сети не требует изменения ее адресной топологии.

2.2. Идентификация и аутентификация

ПО ССПТ-2 обеспечивает возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.

В режиме трансляции сетевых адресов ПО ССПТ-2 поддерживает режим ограничения доступа к сетевым ресурсам для пользователей, не прошедших процедуру аутентификации. В данном режиме каждому пользователю ЛВС требуется пройти процедуру аутентификации на ССПТ-2 перед началом работы с сетевыми ресурсами, расположенными за межсетевым экраном. Для этого пользователю ЛВС необходимо запустить утилиту аутентификации, предустановленную на компьютере, и указать свой идентификатор и пароль выданный администратором ССПТ-2. В случае успешного прохождения аутентификации данному пользователю будет разрешен доступ к сетевым ресурсам через ССПТ-2; в случае неуспешной аутентификации запросы данного пользователя к сетевым ресурсам будут блокироваться ПО ССПТ-2.

Для обеспечения устойчивости идентификации и аутентификации пользователей ЛВС к пассивному и/или активному прослушиванию сети обмен информацией между пользователями ЛВС и ССПТ-2 защищается «Программной библиотекой защиты конфиденциальной информации «АГАВА-С» версии 5.1» (формуляр РАУГ.14001-04 30). Данная библиотека имеет Сертификат соответствия СФ/114-1207 от 18 ноября 2008 г., выданный ФСБ РФ (на основании лицензии №341СА-001001 ООО «Р-Альфа»).

В других режимах реализация технологии “stealth” исключает возможность входящих и исходящих запросов к ресурсам ПО ССПТ-2 с рабочих станций (абонентов) и сетевых устройств подключенных к фильтрующим интерфейсам сегментов сети.

2.3. Регистрация

ПО ССПТ-2 обеспечивает возможность регистрации и учета фильтруемых

пакетов и контролируемых сессий (в том числе виртуальных соединений), обработанных пакетным фильтром ПО ССПТ-2. Информация о зарегистрированном трафике (данные), принятом на фильтрующие интерфейсы и обработанном ССПТ-2, подразделяется на следующие категории:

1) **пакеты** – информация о пакетах, обработанных пакетным фильтром ПО ССПТ-2 по правилам фильтрации. Информация о каждом зарегистрированном пакете представляется в виде иерархической последовательности записей от канального до прикладного уровня включительно;

2) **сессии** – информация о сессиях, обработанных подсистемой управления сессиями пакетного фильтра ПО ССПТ-2.

Используемая подсистема регистрации данных обеспечивает однократность регистрации каждого пакета с сохранением следующих основных параметров:

1) время регистрации пакета или сессии с точностью до микросекунды;

2) номера входного и выходного фильтрующих интерфейсов;

3) цепочка правил фильтрации, по которым был обработан пакет (регистрация пакета) или идентификатор потоковой сессии (регистрация сессии);

4) действие, выполненное над пакетом, в результате его обработки в пакетном фильтре (регистрация пакетов);

5) протокольные заголовки всех уровней, присутствующих в пакете (регистрация пакета);

6) данные о параметрах сессии (регистрация сессии).

Отображаемая информация о зарегистрированном пакете включает следующие параметры:

1) на уровне кадров Ethernet:

- тип кадра Ethernet;

- код вложенного протокола;

- MAC-адреса отправителя и получателя;

2) на уровне протоколов ARP/RARP :

- MAC-адреса отправителя и получателя;

- IP-адреса отправителя и получателя;

- Тип ARP-сообщения;

3) на межсетевом уровне (IP):

- IP-адреса отправителя и получателя;

- протокол верхнего уровня;

- признаки фрагментации пакета;

- длина пакета;

4) на межсетевом уровне (IPX):

- сеть/адрес источника и приемника;

- тип сокета источника и приемника;

- тип пакета;

5) на транспортном уровне:

- для протоколов TCP и UDP - адреса портов отправителя и получателя

- для протокола TCP - номер последовательности и номер подтверждения, флаги управления (в том числе запрос на установление виртуального соединения);

6) для протокола ICMP - тип и код сообщения;

7) на прикладном уровне - заголовок прикладного протокола.

Используемая подсистема регистрации данных обеспечивает однократность регистрации каждой сессии с сохранением следующих основных параметров:

- номер сессии;

- номер ip-правила, по которому данная сессия была создана;

- номер сработавшего правила прикладного уровня;

- номера фильтрующих интерфейсов, через которые установлено соединение;

- IP-адрес клиента и IP-адрес сервера;

- протокол транспортного уровня;

- порт клиента и порт сервера;

- протокол прикладного уровня;

- время начала сессии и время окончания сессии;

- причина удаления сессии из таблицы сессий;
- тайм-аут неактивности для сессии;
- количество пакетов, переданных от клиента к серверу;
- количество пакетов, переданных от сервера к клиенту;
- количество байт данных, переданных от клиента к серверу;
- количество байт данных, переданных от сервера к клиенту.

ПО ССПТ-2 обеспечивает сортировку информации по времени регистрации и возможность выборки информации по следующим параметрам (или совокупности параметров):

- номера входных/выходных интерфейсов;
- тип и номер правила;
- тип кадра Ethernet;
- MAC-адреса источника и получателя кадра;
- тип пакета (arp, ip, icmp, udp, tcp, ipx или другой);
- IP-адреса источника и приемника пакета;
- действие, произведенное над пакетом (удален, пропущен или передан на следующий уровень контроля);
- диапазон времени регистрации.

ПО ССПТ-2 обеспечивает сигнализацию попыток нарушения установленных правил фильтрации посредством вывода на монитор администратора информации об общих результатах фильтрации проходящего трафика пакетов. ПО ССПТ-2 обеспечивает программируемую реакцию на попытки несанкционированного изменения программных модулей и конфигурационных файлов путем прямого редактирования, минуя использование штатных средств администрирования ССПТ-2 и на нарушение контрольных сумм.

ПО ССПТ-2 обеспечивает выгрузку и хранение на удаленном FTP сервере регистрационной информации (данные) об обрабатываемом трафике.

ПО ССПТ-2 обеспечивает функциональность подсистемы регистрации с помощью специального программного модуля – **сервера регистрации**.

2.4. Администрирование: идентификация и аутентификация

2.4.1. Локальное администрирование

Локальное администрирование ССПТ-2 осуществляется через устройства ввода – вывода, (монитор и клавиатура), подключаемые непосредственно к изделию (интерфейс стандарта VGA для подключения монитора и интерфейс стандарта PS/2 или USB для подключения клавиатуры). Для локального администрирования ПО ССПТ-2 предоставляет администратору в качестве средства администрирования **интерфейс командной строки**. Интерфейс командной строки предоставляет возможность локального администрирования ССПТ-2 в **интерактивном** режиме.

Интерфейс командной строки обеспечивает возможность:

- просмотра информации о состоянии изделия и режимах его работы, а также текущей статистической информации;
- просмотра и выборки зарегистрированной информации об обработанных пакетах;
- просмотра и выборки зарегистрированной информации о действиях администратора и пользователей с возможностью поиска необходимых сообщений;
- просмотра системных сообщений изделия;
- просмотра установленных интервалов времени;
- просмотра установленных правил фильтрации;
- просмотра и управления учетными записями пользователей (добавление, удаление и редактирование идентификатора, пароля и прав доступа пользователя), имеющих право работы с изделием;
- удаления информации о зарегистрированных пакетах (очистки регистрационных журналов);
- останова управляющей операционной системы изделия;
- останова и запуска процесса фильтрации;
- запуска процедуры контроля целостности и отображение результатов контроля;

- изменения режимов работы изделия и установки параметров конфигурации фильтров;

- первоначальной установки и изменения IP – адреса управляющего интерфейса типа Ethernet;

- установки, удаления и изменения интервалов времени с возможностью записи произведенных изменений в файл интервалов времени и сообщением подсистеме фильтрации о необходимости изменения интервалов времени, действующих в настоящий момент;

- установки, удаления и изменения правил фильтрации с возможностью записи произведенных изменений в файлы правил и сообщением подсистеме фильтрации о необходимости изменения правил, действующих в настоящий момент;

- установки режима сохранения зарегистрированной информации об обработанных пакетах на внешнем сервере;

- включения/отключения WEB – интерфейса.

ПО ССПТ-2 обеспечивает идентификацию и аутентификацию администратора ССПТ-2 при его локальных запросах на доступ по паролю условно-постоянного действия. Каждый администратор имеет личный идентификатор, на основании которого определяются его права по управлению ССПТ-2.

Пароль содержит от 6 до 128 буквенно-цифровых символов. Идентификатор - от 2 до 16 буквенно-цифровых символов.

Доступ неидентифицированного пользователя, подлинность идентификации которого при аутентификации не подтвердилась, при локальном администрировании не возможен.

2.4.2. Удаленное администрирование

ПО ССПТ-2 обеспечивает возможность аутентификации входящих и исходящих запросов при удаленном администрировании методами, устойчивыми к пассивному и/или активному прослушиванию сети.

Удаленное администрирование ССПТ-2 осуществляться с управляющего

компьютера двумя способами:

- через асинхронный последовательный интерфейс (выделен последовательный интерфейс стандарта RS232), с использованием механизма удаленного доступа на базе протокола PPP (Point-to-Point Protocol);

- через сетевой интерфейс типа Ethernet (выделен сетевой управляющий интерфейс типа Ethernet с производительностью до 100 или до 1000 Мб/с, в зависимости от исполнения).

Удаленное администрирование осуществляется посредством интерфейса командной строки. Интерфейс командной строки предоставляет возможность удаленного администрирования ССПТ-2 в интерактивном режиме.

Внимание!!! **При любом способе удаленного управления межсетевым экраном должен использоваться выделенный канал управления, защищенный от несанкционированного использования организационно-техническими методами.**

Для обеспечения устойчивости идентификации и аутентификации к активному воздействию на процесс управления со стороны канала связи и перехвату информации в канале управления при удаленном управлении с использованием интерфейса командной строки в ССПТ-2 (на основе лицензии №341СА-001001 ООО «Р-Альфа») используется «Программная библиотека защиты конфиденциальной информации «АГАВА-С» версии 5.1» (формуляр РАУГ.14001-04 30). Данная библиотека имеет Сертификат соответствия СФ/114-1207 от 18 ноября 2008 г., выданный ФСБ РФ.

В качестве дополнительного средства удаленного администрирования, в ССПТ-2 предусмотрена возможность использования WEB - интерфейса и SNMP-интерфейса администратора.

Удаленное управление по WEB – интерфейсу допускается только по выделенному каналу, устойчивость идентификации и аутентификации к активному воздействию на процесс управления и перехвату информации в котором обеспечивается организационно-административными мерами. Поэтому в конфигурации изде-

лия по умолчанию управление по WEB - интерфейсу администратора не предусмотрено. WEB – интерфейс активируется только по каналу локального управления командой администратора, имеющего полные полномочия.

Удаленное управление через SNMP-интерфейс администратора реализуется при помощи стандартного MIB браузера, взаимодействующего с SNMP сервером, функционирующим на ССПТ-2, по защищенному каналу управления на базе протокола SNMPv3.

Для обеспечения устойчивости идентификации и аутентификации к активному воздействию на процесс управления со стороны канала связи и перехвату информации в канале управления при удаленном управлении с использованием WEB-интерфейса должен использоваться выделенный канал управления, размещенный на охраняемой территории и контролируемый организационно-административными методами или внешними, по отношению к ССПТ-2, средствами криптографической защиты информации.

В ПО ССПТ-2 предусмотрена возможность идентификации и аутентификации пользователя ССПТ-2 через RADIUS-сервер по протоколу RADIUS. Обмен данными с RADIUS сервером происходит на этапе авторизации ССПТ-2 , после того как пользователь ввел имя и пароль.

Для обеспечения устойчивости идентификации и аутентификации к активному воздействию на процесс управления со стороны канала связи и перехвату информации в канале управления при авторизации через RADIUS-сервер должен использоваться выделенный канал управления, размещенный на охраняемой территории и контролируемый организационно-административными методами. В конфигурации изделия по умолчанию, авторизация пользователя через RADIUS-сервер не предусмотрена. Механизм удаленной авторизации пользователя через RADIUS-сервер активируется командой администратора, имеющего полные полномочия.

ПО ССПТ-2 обеспечивает идентификацию и аутентификацию администратора ССПТ-2 при его удаленных запросах на доступ по паролю условно-постоянного действия. Каждый администратор имеет личный идентификатор, на основании ко-

торого определяются его права по управлению ССПТ-2.

Пароль содержит от 6 до 128 буквенно-цифровых символов. Идентификатор - от 2 до 16 буквенно-цифровых символов.

Доступ неидентифицированного пользователя, подлинность идентификации которого при аутентификации не подтвердилась, не возможен.

ПО ССПТ-2 обеспечивает возможность наложения ограничений на адреса, с которых осуществляется удаленное администрирование определением списка разрешенных IP- адресов управляющих компьютеров, с которых может осуществляться удаленное администрирование.

Средства удаленного администрирования обеспечивают возможность:

- просмотра информации о состоянии изделия и режимах его работы, а также текущей статистической информации;

- просмотра и выборки зарегистрированной информации об обработанных пакетах;

- просмотра и выборки зарегистрированной информации о действиях администратора и пользователей с возможностью поиска необходимых сообщений;

- просмотра системных сообщений изделия;

- просмотра установленных интервалов времени;

- просмотра установленных правил фильтрации;

- просмотра и управления учетными записями пользователей (добавление, удаление и редактирование идентификатора, пароля и прав доступа пользователя), имеющих право работы с изделием;

- удаления информации о зарегистрированных пакетах (очистки регистрационных журналов);

- останова управляющей операционной системы изделия;

- останова и запуска процесса фильтрации;

- запуска процедуры контроля целостности и отображение результатов контроля;

- изменения режимов работы изделия и установки параметров конфигурации

фильтров;

- установки, удаления и изменения интервалов времени с возможностью записи произведенных изменений в файл интервалов времени и сообщением подсистеме фильтрации о необходимости изменения интервалов времени, действующих в настоящий момент;

- установки, удаления и изменения правил фильтрации с возможностью записи произведенных изменений в файлы правил и сообщением подсистеме фильтрации о необходимости изменения правил, действующих в настоящий момент;

- установки режима сохранения зарегистрированной информации об обработанных пакетах на внешнем сервере;

- изменения IP – адреса управляющего интерфейса типа Ethernet;

- загрузки на управляющий компьютер (УК) и выгрузки с УК на изделие файлов правил фильтрации, интервалов времени и конфигурации изделия.

2.4.3. Разграничение прав пользователей

ПО ССПТ-2 обеспечивает разграничение прав пользователей при локальном и удаленном администрировании в соответствии со следующими уровнями доступа:

- управление изделием с правами Администратора (полный доступ);

- управление изделием с правами доступа оператора на просмотр информации и выполнение операций, соответствующих установленным Администратором привилегиям;

- управление с правами доступа оператора только на просмотр информации.

ПО ССПТ-2 обеспечивает возможность определения списка разрешенных IP- адресов управляющих компьютеров, с которых может осуществляться удаленное администрирование.

ПО ССПТ-2 обеспечивает возможность работы с правами администратора в одно и тоже время только одному пользователю. В том случае, если при работе одного пользователя с правами Администратора по каналу локального или удаленно-

го администрирования осуществляется попытка подключения второго пользователя с правами Администратора, то права доступа для второго пользователя автоматически ограничиваются до прав на просмотр информации, при этом второй пользователь получает соответствующее предупреждение.

ПО ССПТ-2 обеспечивает сигнализацию попыток нарушения установленных правил фильтрации посредством вывода на монитор администратора сигнала о несанкционированной попытке изменения правил фильтрации.

ПО ССПТ-2 обеспечивает функциональность подсистемы авторизации с помощью специального программного модуля – сервера авторизации.

2.5. Администрирование: регистрация действий

ПО ССПТ-2 обеспечивает регистрацию и хранение действий администратора и системных сообщений (событий), возможность выгрузки и хъранения журналов регистрации событий на удаленный FTP-сервер, и отправки (по мере возникновения) системных сообщений на удаленный SYSLOG-сервер.

Событие отражает факт изменения состояния, конфигурационных параметров либо режима функционирования ПО ССПТ-2, произошедших в результате действий пользователей или в следствие возникновения сбоев или ошибок в работе ПО ССПТ-2.

ПО ССПТ-2 обеспечивает регистрацию:

- входа/выхода администратора;
- загрузки и инициализации операционной системы ССПТ-2 и ее останова;
- действий администратора по изменению и загрузке правил фильтрации;
- действий администратора по изменению конфигурационных параметров ССПТ-2;
- действий администратора по управлению ССПТ-2 (запуск/останов пакетного фильтра, сброс файлов регистрации и т. д.).

В параметрах регистрации события всегда указывается:

- дата и время регистрируемого события с учетом часового пояса;

- код и описание события;

- идентификатор администратора ССПТ-2, действия которого привели к регистрации данного события;

- IP адрес управляющего компьютера в случае удаленного администрирования.

Регистрируемые события подразделяются на:

1) **информационные сообщения** – предназначены для информирования администратора о событиях, не нарушающих нормальную работу программного обеспечения ССПТ-2:

- 0x1001 - Останов устройства;
- 0x1002 - Перезагрузка устройства;
- 0x1003 - Запуск пакетного фильтра;
- 0x1004 - Останов пакетного фильтра;
- 0x1005 - Перезапуск пакетного фильтра;
- 0x1006 - Проверка целостности программного обеспечения;
- 0x1007 – Включение WEB-интерфейса;
- 0x1008 – Отключение WEB-интерфейса;
- 0x100f - Установка правила в значения по умолчанию;
- 0x1010 - Добавление правила фильтрации;
- 0x1011 - Изменение правила фильтрации;
- 0x1012 - Удаление правила фильтрации;
- 0x1013 - Загрузка дополнительного набора правил;
- 0x1014 - Сохранение дополнительного набора правил;
- 0x1015 - Удаление дополнительного набора правил;
- 0x1016 - Откат к предыдущему состоянию набора правил;
- 0x1017 - Копирование MAC-правила;
- 0x1018 - Перенос MAC-правила;
- 0x1019 - Копирование ARP-правила;
- 0x101a - Перенос ARP-правила;

- 0x101b - Копирование IP-правила;
- 0x101c - Перенос IP-правила;
- 0x101d - Копирование IPX-правила;
- 0x101e - Перенос IPX-правила;
- 0x101f - Копирование IPTMP-правила;
- 0x1020 - Очистка текущей регистрации пакетов;
- 0x1021 - Выгрузка файлов регистрации на FTP-сервер;
- 0x1022 - Очистка текущей регистрации сессий;
- 0x1023 - Включение выгрузки системных сообщений на SYSLOG-сервер;
- 0x1024 - Отключение выгрузки системных сообщений на SYSLOG-сервер;
- 0x1025 - IP-адрес SYSLOG сервера изменен;
- 0x1026 - Дополнительный набор правил загружен с удаленного хоста;
- 0x1027 - Дополнительная конфигурация загружена с удаленного хоста;
- 0x1029 - Перенос IPTMP-правила;
- 0x102a - Копирование интервала времени;
- 0x102b - Перенос интервала времени;
- 0x102c - Копирование AP-праила;
- 0x102d - Перенос AP-правила;
- 0x102e - Перенос группы VLAN;
- 0x102f - Сброс статистики в правилах;
- 0x1030 - Изменение конфигурации ССПТ-2;
- 0x1031 - Включение регистрации пакетов;
- 0x1032 - Изменение системного времени;
- 0x1033 - Настройка выгрузки файлов регистрации на FTP-сервер;
- 0x1034 - Включение режима управления сессиями;
- 0x1036 - Изменение настроек зеркалирования интерфейсов;
- 0x1037 - Изменение настроек тайм-аутов сессий;
- 0x1039 - Установка IP-адреса управляющего интерфейса;
- 0x103a - Удаление IP-адреса управляющего интерфейса;

- 0x103b - Отключение фильтрующего интерфейса;
- 0x103c - Включение фильтрующего интерфейса;
- 0x103d - Изменение скорости передачи фильтрующего интерфейса;
- 0x103e - Изменение режима передачи фильтрующего интерфейса;
- 0x103f - Переименование фильтрующего интерфейса;
- 0x1040 - Установка маршрута по умолчанию;
- 0x1041 - Удаление маршрута по умолчанию;
- 0x1042 - Добавление новой записи в список доступа;
- 0x1043 - Удаление записи из списка доступа;
- 0x1044 - Очистка списка доступа;
- 0x1045 - Включение маршрута по умолчанию;
- 0x1046 - Отключение маршрута по умолчанию;
- 0x1047 - Включение зеркалирования интерфейсов;
- 0x1048 - Отключение зеркалирования интерфейсов;
- 0x1049 - Включение выгрузки на FTP-сервер;
- 0x104a - Отключение выгрузки на FTP-сервер;
- 0x104b - Сброс настроек выгрузки на FTP-сервер;
- 0x104c - Отключение режима управления сессиями;
- 0x104d - Включение регистрации пакетов, отброшенных механизмом управления сессиями;
- 0x104e - Отключение регистрации пакетов, отброшенных механизмом управления сессиями;
- 0x104f - Включение фильтрации на прикладном уровне;
- 0x1050 - Отключение фильтрации на прикладном уровне;
- 0x1051 - Включение создания сессий по умолчанию для IP-правил;
- 0x1052 - Отключение создания сессий по умолчанию для IP-правил;
- 0x1053 - Изменение тайм-аутов для TCP;
- 0x1054 - Изменение тайм-аутов для UDP;
- 0x1055 - Изменение тайм-аутов для ICMP;

- 0x1056 - Изменение тайм-аутов для других протоколов;
- 0x1057 - Изменение размера таблицы сессий;
- 0x1058 - Очистка таблицы сессий;
- 0x1059 - Удаление сессии;
- 0x105a - Установка тайм-аутов в значения по умолчанию;
- 0x105b - Сброс настроек зеркалирования интерфейсов;
- 0x105c - Сохранение текущей конфигурации;
- 0x105d - Сохранение дополнительной конфигурации;
- 0x105e - Удаление дополнительной конфигурации;
- 0x105f - Загрузка дополнительной конфигурации;
- 0x1060 - Загрузка конфигурации по умолчанию;
- 0x1061 - Отключение управляющего интерфейса;
- 0x1062 - Включение управляющего интерфейса;
- 0x1063 - Изменение режима передачи управляющего интерфейса;
- 0x1064 - Изменение скорости передачи управляющего интерфейса;
- 0x1065 - Изменение системной даты;
- 0x1066 - Включение синхронизации по NTP;
- 0x1067 - Отключение синхронизации по NTP;
- 0x1068 - Сброс настроек синхронизации по NTP;
- 0x1069 - Установка IP-адреса NTP-сервера;
- 0x106a - Синхронизация по NTP выполнена;
- 0x106b - Изменение настроек синхронизации по NTP;
- 0x106c - Включение регистрации событий NTP-синхронизации;
- 0x106d - Отключение регистрации событий NTP-синхронизации;
- 0x106e - Изменение периода NTP-синхронизации;
- 0x106f - Изменение часового пояса;
- 0x1070 - Отключение регистрации пакетов;
- 0x1071 - Включение сигнализации обнаружения flood-атак;
- 0x1072 - Отключение сигнализации обнаружения flood-атак;

- 0x1073 - Включение режима обнаружения flood-атак;
- 0x1074 - Отключение режима обнаружения flood-атак;
- 0x1075 - Изменение порогового значения обнаружения flood-атаки;
- 0x1076 - Включение регистрации flood-атак;
- 0x1077 - Отключение регистрации flood-атак;
- 0x1078 - Изменение комментария временного IP-правила для заблокированной flood-атаки;
- 0x1079 - Изменение времени жизни временного IP-правила для заблокированной flood-атаки;
- 0x1100 - Вход пользователя;
- 0x1101 - Выход пользователя;
- 0x1102 - Добавление пользователя;
- 0x1103 - Удаление пользователя;
- 0x1104 - Изменение пароля пользователя;
- 0x1105 - Изменение привилегий пользователя;
- 0x1106 - Отключение пользователя;
- 0x1107 - Включение пользователя;
- 0x1108 - Изменение пароля системного пользователя;
- 0x1109 – Аутентификация сетевого пользователя;
- 0x1200 - Включение NAT;
- 0x1201 - Отключение NAT;
- 0x1202 - Установка диапазона портов NAT;
- 0x1203 - Установка внешнего адреса NAT;
- 0x1204 - Удаление внешнего адреса NAT;
- 0x1205 - Установка маршрута по умолчанию NAT;
- 0x1207 - Установка внутреннего адреса NAT;
- 0x1208 - Удаление внутреннего адреса NAT;
- 0x1209 - Включение регистрации NAT;
- 0x120a - Отключение регистрации NAT;

- 0x120b - Установка внешнего MAC-адреса NAT;
- 0x120c - Удаление внешнего MAC-адреса NAT;
- 0x120d - Добавление записи в ARP-таблицу NAT;
- 0x120e - Удаление записи из ARP-таблицы NAT;
- 0x120f - Очистка ARP-таблицы NAT;
- 0x1210 - Добавление записи в таблицу переадресации NAT;
- 0x1211 - Удаление записи из таблицы переадресации NAT;
- 0x1212 - Очистка таблицы переадресации NAT;
- 0x1213 - Включение переадресации NAT из DMZ;
- 0x1214 - Отключение переадресации NAT из DMZ;
- 0x1215 - Включение переадресации NAT с внешнего интерфейса;
- 0x1216 - Отключение переадресации NAT с внешнего интерфейса;
- 0x1217 - Включение аутентификации пользователей ;
- 0x1218 - Отключение аутентификации пользователей ;
- 0x1219 - Добавление сетевого пользователя;
- 0x121a - Удаление сетевого пользователя;
- 0x121b - Включение сетевого пользователя;
- 0x121c - Отключение сетевого пользователя;
- 0x121d – Прерывание работы сетевого пользователя;
- 0x121e – Смена пароля сетевого пользователя;
- 0x121f – Изменение тайм-аута неактивности сетевых пользователей;
- 0x1220 – Изменение параметров сетевого пользователя;
- 0x1221 – Добавление записи в файл ключей аутентификации;
- 0x1222 – Удаление записи из файла ключей аутентификации;
- 0x1223 – Обновление записи в файле ключей аутентификации;
- 0x1300 - Изменение режима резервирования;
- 0x1301 - Включение резервирования;
- 0x1302 - Отключение резервирования;
- 0x1303 - Изменение смежного резервного устройства;

- 0x1304 - Установка параметров резервирования в значения по умолчанию;
- 0x1305 - Включение синхронизации сессий;
- 0x1306 - Отключение синхронизации сессий;
- 0x1309 - Включение синхронизации правил;
- 0x130a - Отключение синхронизации правил;
- 0x130c - Синхронизация правил инициирована;
- 0x130d - Изменение тайм-аута неактивности для командного интерфейса;
- 0x130e - Изменение скорости передачи при резервировании;
- 0x130f - Изменение режима передачи при резервировании;
- 0x1310 - Синхронизация конфигурации инициирована;
- 0x1311 - Синхронизация правил завершена;
- 0x1312 - Синхронизация конфигурации выполнена;
- 0x1400 - Использование RADIUS включено;
- 0x1401 - Использование RADIUS отключено;
- 0x1402 - Тайм-аут ожидания ответа от RADIUS-сервера изменен;
- 0x1403 - Количество обращений к RADIUS серверу изменено;
- 0x1404 - Конфигурация RADIUS сервера изменена;

2) **предупреждения** – предназначены для информирования администратора о событиях, не нарушающих нормального функционирования программного обеспечения ССПТ-2, однако являющихся нестандартными или некорректными с точки зрения логики работы ССПТ-2:

- 0x2001 - Принят свой собственный кадр Ethernet;
- 0x2002 - Принят неподдерживаемый кадр Ethernet;
- 0x2003 - Недостаточно привилегий для выполнения операции;
- 0x2004 - Набор выходных интерфейсов пустой;
- 0x2005 - Неверная регистрация пользователя;
- 0x2006 - Выход незарегистрированного пользователя;
- 0x2007 - Flood-атака обнаружена и заблокирована;
- 0x2008 - Сервер высокой готовности изменил состояние устройства;

- 0x2009 - Доступ запрещен в соответствии со списком доступа;
- 0x200a - Пакет вне окна приемника;
- 0x200b - Повторный пакет;
- 0x200c - Неверная регистрация пользователя через RADIUS;
- 0x200d - Изменение режима резервирования - перевыборы;
- 0x200e - Изменение режима резервирования - отказ смежного устройства;
- 0x200f - Синхронизация правил не завершена;
- 0x2010 - Синхронизация конфигурации не завершена;
- 0x2011 - Отказ в аутентификации сетевого пользователя;

3) **ошибки** - предназначены для информирования администратора о событиях, нарушающих нормальную работу программного обеспечения ССПТ-2 и требующих специальных действий по их обработки.

В свою очередь, сообщения об ошибках подразделяются на:

1) Общесистемные ошибки:

- 0x3001 - Ошибка ввода/вывода на интерфейс;
- 0x3002 - Ошибка операционной системы;
- 0x3003 - Ошибка в файле конфигурации ССПТ;
- 0x3004 - Ошибка выгрузки файлов регистрации на FTP-сервер;
- 0x3005 - Нарушена целостность программного обеспечения ССПТ;

2) ошибки, обнаруженные при обработке пакетов:

- 0x3006 - Сессия не добавлена - некорректный набор флагов;
- 0x3007 - Сессия не добавлена - таблица переполнена;
- 0x3008 - Сессия не добавлена - ошибка распределения памяти;
- 0x3009 - Сессия не добавлена - неверный номер правила;
- 0x300a - Контекст сессии - неверный входной интерфейс;
- 0x300b - Контекст сессии - не установлен флаг ACK;
- 0x300c - Контекст сессии - неверный набор флагов;
- 0x300d - Контекст сессии - неверный номер последовательности;
- 0x300e - Контекст сессии - неверный номер подтверждения;

- 0x300f - Контекст сессии - неизвестное состояние;
- 0x3100 - NAT - ARP-таблица заполнена;
- 0x3101 - NAT - не найден соответствующий ARP-запрос;
- 0x3102 - NAT - неизвестный тип ARP-сообщения;
- 0x3103 - NAT - неверный IP-адрес источника;
- 0x3104 - NAT - неверный IP-адрес приемника;
- 0x3105 - NAT - внутренний пакет;
- 0x3106 - NAT - нет свободных портов;
- 0x3107 - NAT - таблица обратных потоков заполнена;
- 0x3108 - NAT - недопустимое ICMP-сообщение;
- 0x3109 - NAT - недопустимый протокол;
- 0x310a - NAT - сессия не создана по пакету;
- 0x310b - NAT - неверный пакет с внешнего интерфейса;
- 0x310c - NAT - не найдена соответствующая сессия;
- 0x310d - NAT - не найдена соответствующая запись в ARP-таблице;
- 0x310e - Неверная длина заголовка IP-пакета;
- 0x310f - Некорректный фрагментированный IP-пакет;
- 0x3110 - NAT - фрагментированный пакет;
- 0x3111 - Некорректная длина IP-пакета;
- 0x3112 - Пакет не аутентифицирован.

ПО ССПТ-2 обеспечивает сортировку информации по времени регистрации и возможность выборки информации по следующим параметрам (или совокупности параметров):

- тип события;
- диапазон времени регистрации события.

ПО ССПТ-2 обеспечивает невозможность удаления зарегистрированных событий.

ПО ССПТ-2 обеспечивает регистрацию запуска программ и порождения процессов (заданий, задач), относящихся к программной части ССПТ-2 . В журнале

регистрации системных сообщений регистрируются запуски и другие события, связанные с реализацией инициированных процессов и работой следующих программ:

- Программа «Пакетный фильтр» fnp_filtd;
- Программа «Командный интерпретатор» fnpsh;
- Программа «Командный сервер» fnp_shd;
- Программа «Сервер терминального доступа» fnp_cryd;
- Программа «Сервер регистрации» fnp_logd;
- Программа «Сервер авторизации» fnp_authd;
- Программа «Сервер высокой готовности» fnp_had;
- Программа «Сервер проверки контрольных сумм» fnp_csd;
- Программа инициализации ПО ССПТ-2 fnpsign;
- Программа выгрузки файлов регистрации на FTP сервер logftp.

В параметрах регистрации указываются:

- дата и время регистрируемого события;
- наименование ПО ССПТ-2 (fnp);
- код процесса;
- имя программного модуля
- описание события.

При регистрации системных сообщений на удаленном SYSLOG - сервере в параметрах регистрации указаны:

- дата и время регистрируемого события;
- IP-адрес управляющего Ethernet - интерфейса ССПТ-2 ;
- код процесса;
- имя программного модуля
- описание события.ПО ССПТ-2 обеспечивает функциональность подсистемы регистрации с помощью специального программного модуля – **сервера регистрации**.

2.6. Администрирование: простота использования

ПО ССПТ-2 обеспечивает возможность управления настройкой фильтров с отображением состояния фильтров, а также доступ к информации об интегральном состоянии изделия и проходящем трафике пакетов.

ПО ССПТ-2 обеспечивает возможность удаленного управления, в том числе возможность конфигурирования фильтров, просмотра и анализа (выборки по заданным параметрам) регистрационной информации.

При формировании многокомпонентного МЭ ПО ССПТ-2 обеспечивает возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

ПО ССПТ-2 обеспечивает простоту настройки фильтра, с поэтапным углублением в более подробную настройку, с большим числом контролируемых параметров.

ПО ССПТ-2 обеспечивает возможность временного отключения любого (кроме глобальных и временных IP-правил) правила фильтрации без его удаления.

При настройке правил и интервалов времени ПО ССПТ-2 обеспечивает возможность задания списка значений параметров (как диапазона, так и одиночных), для которых это имеет смысл.

ПО ССПТ-2 обеспечивает возможность просмотра правил фильтрации и их сортировки для просмотра по следующим параметрам:

- номера правил;
- обозначения входных и выходных интерфейсов;
- адреса и порты отправителя и получателя;
- номера интервалов времени.

При удаленном администрировании ПО ССПТ-2 обеспечивает возможность загрузки/выгрузки:

- файла настроек изделия;
- файла правил фильтрации.

ПО ССПТ-2 обеспечивает возможность сохранение файлов регистрации пакетов и сессий, и файлов регистрации действий администратора на удаленном FTP - сервере хранения данных, и возможность сохранение файлов системных сообщений на удаленном SYSLOG- сервере хранения данных.

ПО ССПТ-2 обеспечивает возможность использования технологии скрытной фильтрации (режим “stealth“), позволяющей скрывать для средств удаленного сетевого мониторинга место расположения изделия и эффективно наращивать производительность системы информационной безопасности.

Основные особенности применения режима “stealth” следующие:

- фильтрующие интерфейсы ССПТ-2, подключаемые с защищаемым сегментам ЛВС, работают в режиме **приема и обработки всего трафика**, передаваемого в данных сегментах;

- пакет, прошедший обработку подсистемой фильтрации ССПТ-2 и передаваемый на любой из выходных фильтрующих интерфейсов, **остается без изменения** – не изменяются ни заголовки протоколов, ни данные.

За счет применения режима “stealth“ ПО ССПТ-2 обеспечивает возможность подключения сегментов сети к фильтрующим интерфейсам без изменений в адресном пространстве подключаемых сегментов.

2.7. Целостность

ПО ССПТ-2 содержит подсистему контроля целостности программной и информационной части ССПТ-2.

Подсистема контроля целостности обеспечивает возможность проверки администратором целостности исполняемых файлов системы фильтрации и операционной системы. Проверка осуществляется по контрольным суммам (хеш-функциям) длиной более 4 байт.

Подсистема контроля целостности обеспечивает возможность проверки администратором целостности данных, относящихся к процессу фильтрации, в частности, конфигурационных файлов (конфигурация фильтра и правила фильтрации).

Проверка осуществляется по контрольным суммам (хеш-функциям) длиной не менее 4 байт. Контрольные суммы изменяются при изменении параметров конфигурации изделия или действующих правил фильтрации.

Автоматически проверка контроля целостности основных компонентов ОС ССПТ-2, программных модулей ПО ССПТ-2 и всех конфигурационных файлов осуществляется как при запуске ССПТ-2, так и динамически, на основе периодической проверки контрольных сумм файлов, содержащих перечисленные выше компоненты.

Таким образом, подсистема контроля целостности предотвращает попытки несанкционированного изменения программных модулей и конфигурационных файлов, как с использованием инструментов управления, так и путем прямого редактирования, минуя использование штатных средств администрирования ССПТ-2.

При обнаружении нарушения контрольной суммы подсистема контроля целостности выполняет следующие действия:

- останов пакетного фильтра;

- регистрация события о нарушении контрольной суммы с указанием имени файла;

- перевод сервера авторизации в однопользовательский режим работы – доступ администратора к ССПТ-2 будет возможен только с системной консоли ССПТ-2 и только для администратора с идентификатором “admin”.

2.8. Восстановление и защита от сбоев

ПО ССПТ-2 обеспечивает возможность восстановления после сбоев и отказов электропитания и, как следствие, возможных сбоев (не фатальных) в работе программного обеспечения и оборудования.

В эксплуатационной документации дано описание процедур восстановления, которые обеспечивают восстановление его свойств в полном объеме. Среднее время восстановления работоспособного состояния изделия после сбоев не превышает 6 минут при нормальных климатических условиях по ГОСТ 21552 - 84.

ПО ССПТ-2 предусматривает возможность обеспечения оперативного восстановления свойств межсетевого экранирования при сбоях ПО и отказах (включая фатальные) оборудования. Для этого предусмотрена возможность формирования многокомпонентного ССПТ-2, работающего в режиме фильтрации высокой готовности. В этом режиме два ССПТ-2 работают как одна логическая система фильтрации. При пропадании питания, выходе из строя аппаратных компонентов или отказе программных компонентов одного из изделий, работающего в логической системе фильтрации, обеспечиваетмс восстановление (за счет ресурсов второго изделия) процесса фильтрации в прежнем объеме за время не более 10 секунд.

2.9. Тестирование

ПО ССПТ-2 обеспечивает возможность регламентного тестирования:

- реализации правил фильтрации;
- процесса идентификации и аутентификации администратора;
- процесса регистрации действий администратора защиты;
- процесса контроля за целостностью программной части и конфигурации ССПТ-2;
- неизменности процедур управления и исправность тракта управления;
- процесса регистрации;
- процесса формирования и поддержания изолированной программной среды;
- процедуры восстановления.

Методика регламентного тестирования размещена в Паспорте на ССПТ-2 РКДЕ.401350.005 ПС.

2.10. Режимы работы

2.10.1. Автономный старт

ПО ССПТ-2 обеспечивает автономный старт и автоматический переход к режиму фильтрации ССПТ-2 при подаче электропитания. При этом режим фильтрации осуществляется в соответствии с ранее установленными правилами. Время готовности изделия не превышает четырех минут.

В режиме фильтрации ПО ССПТ-2 обеспечивает передачу сетевых пакетов с одного его интерфейса на другой, если не установлено правил фильтрации, запрещающих это.

В режиме останова фильтра (процесса фильтрации) ПО ССПТ-2 обеспечивает запрет пропуска пакетов между фильтрующими интерфейсами изделия.

2.10.2. Трансляция трафика

ПО ССПТ-2 обеспечивает возможность передачи полного, входящего или исходящего трафика с одного фильтрующего интерфейса на другой. Номера интерфейсов задаются администратором. В этом случае на выбранный интерфейс передаются (без обработки правилами фильтрации) все, входящие или исходящие пакеты, проходящие через другой выделенный интерфейс. Способность ПО ССПТ-2 выделять трафик, проходящий через любой фильтрующий интерфейс (зеркалирование трафика) позволяет администратору выделить необходимый трафик для анализа внешними средствами (например, сенсорами).

2.10.3. Режим высокой готовности

ПО ССПТ-2 обеспечивает возможность работы ССПТ-2 в режиме высокой готовности («горячего» резерва процесса фильтрации). В этом режиме два ССПТ-2 подключаются к сегментам АС параллельно (с использованием сетевых коммутирующих устройств) и работают как одна логическая система фильтрации. При этом обеспечивается возможность настройки нескольких вариантов режима «горя-

чего» резерва процесса фильтрации по схемам “активный/резервный” или “активный/активный”.

ССПТ-2 связаны между собой через сетевой управляющий интерфейс и обмениваются сообщениями с целью выявления отказов и переключения режимов работы для каждого изделия.

При пропадании питания изделия, выходе из строя аппаратных компонентов или отказе программных компонентов изделия, работающего в режиме фильтрации ПО ССПТ-2 обеспечивает восстановление процесса фильтрации, прерванного по указанным причинам, в прежнем объеме за время не более 10 секунд.

ПО ССПТ-2 обеспечивает функциональность подсистемы горячего резервирования посредством специального программного модуля – сервера высокой готовности.

2.10.4. Режим скрытной фильтрации

ПО ССПТ-2 обеспечивает *скрытый режим работы* или *Stealth-режим*. При этом режиме обеспечивается сохранность MAC- адреса в заголовке Ethernet – кадра или ARP- пакета, и IP –адреса в заголовке IP-пакета или ARP- пакета, который поступил на фильтрующие интерфейсы, прошел обработку в изделии и передан на выходной интерфейс (исключение - режим трансляции сетевых адресов адресов). Таким образом, в результате обработки пакета не изменяются ни заголовки протоколов, ни данные (исключение - режим трансляции сетевых адресов).

2.10.5. Режим трансляции сетевых адресов

ПО ССПТ-2 обеспечивает:

- возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети путем ограничения доступа из внешней сети (во внутреннюю сеть должны пропускаться только пакеты, принадлежащие к контролируемым сессиям). Если для пакета из внешней сети не находится сессии в таблице контролируемых сессий (пакет – инициатор соединения), такой пакет не пропускается;

- возможность трансляции сетевых адресов путём подмены внутренней адресов и портов сети.

ПО ССПТ-2 обеспечивает трансляцию адресов (передачу из внутренней сети во внешнюю и обратно) для следующих протоколов:

- TCP;
- UDP;
- ICMP-сообщения типа «Эхо-запрос» и «Эхо-ответ».

Пакеты остальных протоколов в этом режиме не передаются из внутренней сети во внешнюю сеть и обратно.

2.11. Устойчивость к сетевым атакам

ПО ССПТ-2 обеспечивает устойчивость ССПТ-2 к сетевым атакам (ССПТ-2 продолжает функционировать в заданном режиме) направленным через любой входной фильтрующий интерфейс на средства вычислительной техники, подключенные к любому выходному фильтрующему интерфейсу. Изделие обладает устойчивостью к сетевым DoS – атакам следующих типов:

1) Ping flooding. Эта атака посылает продолжительные серии эхо-запросов по протоколу ICMP. Атакуемая система тратит свои вычислительные ресурсы, отвечая на эти запросы. Таким образом, существенно снижается производительность системы и возрастает загруженность каналов связи;

2) SYN flooding. Эта атака воздействует на атакуемую систему следующим образом. При установлении соединения по протоколу TCP приемная сторона, получив запрос на соединение (пакет с флагом SYN), посылает источнику ответ (пакет с флагами SYN и ACK) о готовности установить это соединение. При этом система размещает в своей памяти служебную запись об устанавливаемом соединении и хранит ее до тех пор, пока источник не пришлет пакет-подтверждение либо не истечет время ожидания данного пакета. Злоумышленник посылает большое количество запросов на установление соединения без передачи пакетов подтверждения. Вследствие этого происходит резкое снижение производительности и при

определенных обстоятельствах аварийное завершение системы. Атака может проводиться как на хост, так и на сегмент сети;

3) DNS flooding - эта атака направлена на сервера имен Интернет. Она заключается в передаче большого числа DNS запросов и приводит к тому, что у пользователей нет возможности обращаться к сервису имен и, следовательно, блокируется работа обычных пользователей;

4) Win Nuke attack – эта атака поражает Windows-системы, в которых в прикладном процессе не была предусмотрена возможность приема срочных данных, что приводило к краху системы;

5) Tear drop attack – эта атака использует ошибку, возникающую при подсчете длины фрагмента во время сборки пакета.

Для противодействия сетевым атакам предусмотрена возможность установки временных IP- правил.

ПО ССПТ-2 имеет встроенный механизм блокировки атак типа flood или «затопление» (например, SYN-flood или ICMP-flood). Данный вид атак связан с направлением потока пакетов высокой интенсивности на атакуемый хост, вследствие чего, последний не имеет возможности продолжать свое функционирование. ССПТ-2 обнаруживает и предотвращает такие атаки следующим образом:

- постоянно контролируются значения интенсивности создания сессий (количество созданных сессий в секунду) и интенсивности пакетов в сессии (количество пакетов в секунду для каждой сессии);

- в случае, если значение интенсивности создания сессий превысит некоторое пороговое значение, различное для различных протоколов, срабатывает механизм блокировки: в таблице сессий производится поиск IP-адресов, больше других участвующих в создании сессий, после чего в таблицу временных IP-правил добавляется правило, блокирующее доступ с/на эти адреса. Данная проверка осуществляется для протоколов TCP, UDP и ICMP;

- в случае, если значение интенсивности пакетов в сессии превысит некоторое пороговое значение, различное для различных протоколов, срабатывает меха-

низм блокировки: в таблицу временных IP-правил добавляется правило, блокирующее доступ с/на эти адреса. Данная проверка осуществляется для протоколов UDP и ICMP.

3. АДМИНИСТРИРОВАНИЕ ССПТ-2 - ПОДГОТОВКА К РАБОТЕ

3.1. Комплект поставки

В комплект поставки ССПТ-2 входят:

1) Межсетевой экран ССПТ-2 РКДЕ.401350.005 в одном из исполнений (РКДЕ.401350.005-01 - РКДЕ.401350.005-94);

2) Утилита доступа по защищенному каналу fnptel и драйвер нуль-модема «Null-modem PPP connection with FNP-2 Firewall»;

3) Кабель питания 220 В/50 Гц;

4) Кабель соединительный нуль-модемный с 9-контактными гнездовыми разъемами (DB 9). Используется для соединения ССПТ-2 с управляющим компьютером по последовательному порту RS-232;

5) Паспорт РКДЕ.401350.005 ПС;

6) Руководство администратора РКДЕ.5014107-05 0134.

3.2. Кабели и соединения

Разъемы ССПТ-2 имеют следующие маркировку и назначение:

1) **Console, Kbd** – консоль операционной системы. Консоль состоит из двух соединителей – соединитель для подключения VGA-монитора (Console) и соединитель PS/2 или USB для подключения клавиатуры (Kbd);

2) **COM** – соединитель последовательного порта RS-232, к которому подключается управляющий компьютер при помощи кабеля Null-модема.

3) **Eth 0, Eth 1, … , Eth N** – соединители фильтрующих интерфейсов Ethernet, к которым подключаются защищаемые сегменты локальной сети, их количество зависит от исполнения ССПТ-2. Используемый тип кабеля – «витая пара», тип соединителя – RJ45;

4) **Eth C** – соединитель управляющего интерфейса Ethernet.

Подключение к ССПТ-2 технических средств управления может быть выпол-

нено одним из трех способов:

1) Через **системную консоль**. Для подключения системной консоли необходимы VGA-монитор и PS/2 или USB-клавиатура. Монитор и клавиатура подключаются к соединителям **Console** и **Kbd** соответственно, расположенным на задней панели корпуса ССПТ-2;

2) Через **асинхронный последовательный интерфейс** (стандарт RS232) с использованием механизма удаленного доступа на базе протокола PPP (*Point-to-Point Protocol*). Для подключения к ССПТ-2 через асинхронный последовательный интерфейс необходим нуль-модемный кабель (входит в комплект поставки). Нуль-модемный кабель подключается к соединителю **COM**, расположенному на задней панели корпуса ССПТ-2. С другой стороны нуль-модемный кабель подключается к свободному порту RS-232 управляющего компьютера;

3) Через **управляющий Ethernet-интерфейс**. Для подключения к ССПТ-2 по управляющему Ethernet-интерфейсу **Eth C** необходим кабель "витая пара" (категории 5):

- перекрестный (*cross-over*) кабель для непосредственного подключения управляющего компьютера;

- прямой кабель для подключения управляющего компьютера через концентратор (хаб или коммутатор).

3.3. Включение в компьютерную сеть

Пример схемы включения ССПТ-2 в компьютерную сеть приводится на рисунке 3.1.

Перед включением ССПТ-2 в компьютерную сеть необходимо:

- подготовить к работе управляющий компьютер в соответствии с выбранным способом управления ССПТ-2;

- подключить ССПТ-2 к питающей электрической сети и включить его, фильтрующие интерфейсы ССПТ-2 также должны быть подключены к защищаемым сегментам сети.

Пример включения ССПТ-2 в компьютерную сеть

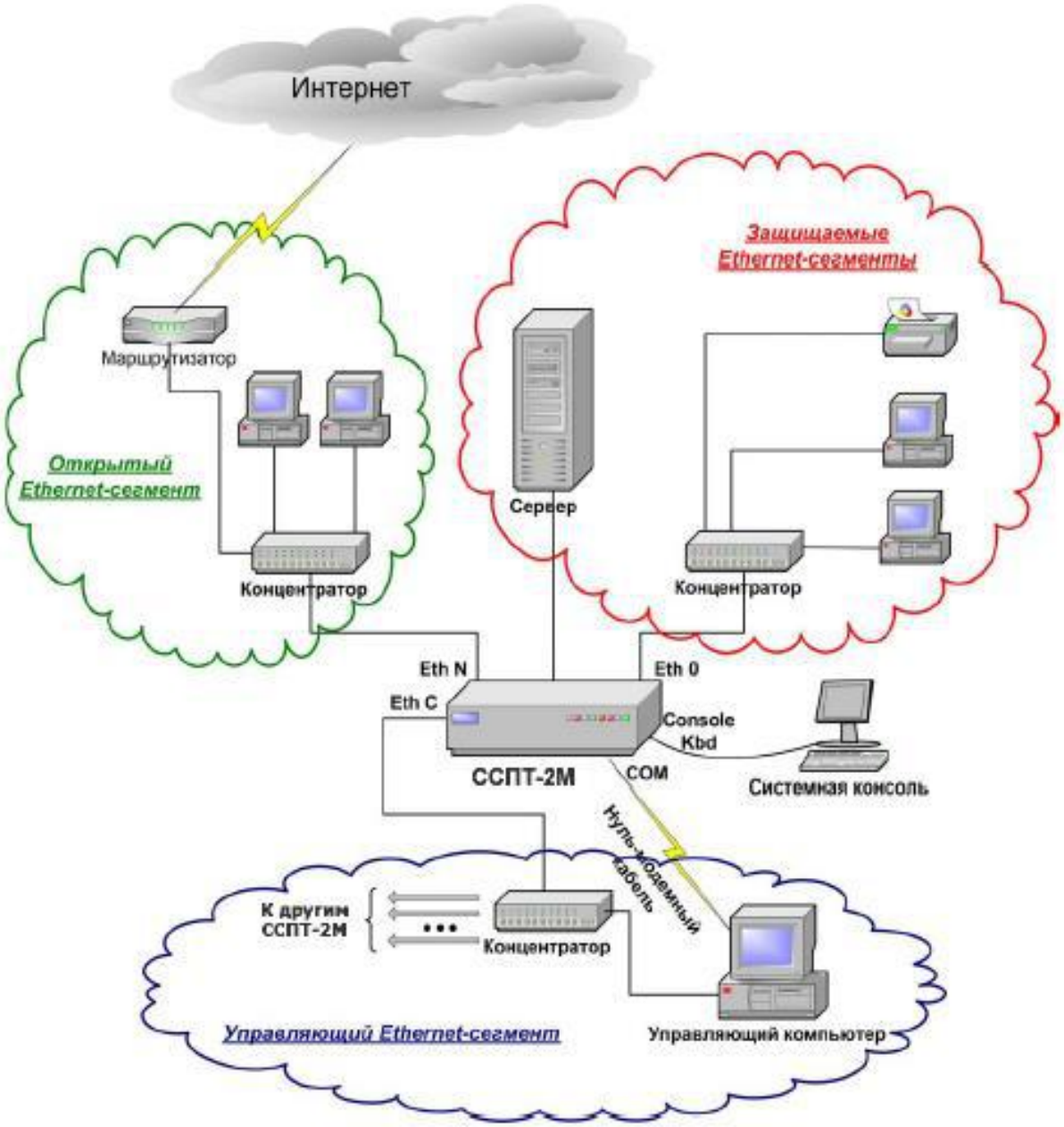

Рисунок 3.1

Сегменты сети подключаются к фильтрующим интерфейсам ССПТ-2 кабелями "витая пара" (категория 5):

- прямыми кабелями для подключения концентраторов (хабов или коммутаторов);

- перекрестными (*cross-over*) кабелями для непосредственного подключения отдельных компьютеров.

Фильтрующие интерфейсы ССПТ-2 являются равнозначными по своему функциональному назначению, и поэтому разделение сегментов сети на открытый и защищаемые – условно и определяется лишь настройкой правил фильтрации ССПТ-2. Необходимо учитывать, что при первом включении (по умолчанию) ССПТ-2 будет блокировать прохождение пакетов.

3.4. Требования к управляющему компьютеру

Управляющий компьютер – это персональный компьютер общего назначения, который используется для удаленного управления и настройки параметров функционирования ССПТ-2. Управляющий компьютер должен работать под управлением одной из следующих операционных систем:

1) Microsoft Windows® 2000/XP;

2) FreeBSD версий 5.x/6.x/7.x;

3) на базе ядра Linux версий не ниже 2.4.x.

Управляющий компьютер должен быть оснащен последовательным портом RS-232 для подключения к ССПТ-2 по нуль-модемному кабелю и адаптером Ethernet для подключения к сети управления.

На управляющем компьютере должны быть установлены утилита доступа по защищенному каналу fnptel и драйвер нуль-модема Null-modem PPP connection with FNP-2 Firewall, входящие в комплект поставки. Установка поставляемого ПО осуществляется в соответствии с Руководствами, размещенными на поставляемом носителе.

4. АДМИНИСТРИРОВАНИЕ ССПТ-2 – ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

4.1. Запуск и вход в систему

4.1.1. Авторизация

В ССПТ-2 определено два уровня авторизации, который последовательно должен пройти пользователь, чтобы получить доступ к управлению по интерфейсу командной строки:

- системная авторизация (авторизация в управляющей операционной системе);
- авторизация пользователя ССПТ-2.

Для авторизации в управляющей операционной системе используется следующие параметры:

- имя пользователя (login): **fnpsh**;
- пароль по умолчанию: **FilterD**.

После прохождения авторизации в управляющей операционной системе необходимо пройти авторизацию пользователя ССПТ-2. По умолчанию используются следующие параметры:

- имя пользователя (login): **admin**;
- пароль по умолчанию: **FilterD**.

Внимание!!! **Перед началом эксплуатации межсетевого экрана пользователь (администратор безопасности) должен изменить установленные по умолчанию пароли. Порядок изменения паролей приведен в пункте 7.3.2 настоящего Руководства.**

В ССПТ-2 существует возможность удаленной аутентификации и авторизации по протоколу RADIUS. Обмен данными с RADIUS сервером происходит на этапе авторизации ССПТ-2, после того как пользователь ввел имя и пароль. Таким

образом, при использования RADIUS будет выполнена следующая последовательность действий:

- авторизация в управляющей операционной системе. Указывается имя пользователя **fnpsh** и пароль **FilterD** (по умолчанию). При этом происходит обращение к локальной базе данных пользователей управляющей операционной системы;

- авторизация пользователя ССПТ-2. Указывается имя пользователя (например, **admin**) и пароль (например, **FilterD**). Эти данные передаются на RADIUS сервер, который по ним проводит аутентификацию. В случае успешной аутентификации (указанное имя пользователя существует и соответствует паролю, зарегистрированному в базе данных RADIUS сервера) пользователь получает доступ к командному интерфейсу ССПТ-2 с правами, предоставленными RADIUS-сервером по указанному имени. В случае неудачной аутентификации (указанное имя пользователя не зарегистрировано в базе данных RADIUS сервера или указанный пароль не соответствует указанному имени пользователя) происходит аутентификация в локальной базе данных пользователей ССПТ-2.

При авторизации на RADIUS сервере пользователям могут быть выданы следующие привилегии:

- *администратор* с полными правами «чтение/запись»;

- *оператор* с правами «только чтение».

Для выдачи привилегии *администратора* необходимо настроить RADIUS сервер таким образом, чтобы при успешной аутентификации пользователей, обладающих правами администратора, в ответе на запрос аутентификации сервер высылал параметр **SERVICE_TYPE** со значением **Administrative-User**. Если при успешной аутентификации RADIUS сервер не высылает параметр **SERVICE_TYPE**, считается, что зарегистрировался пользователь с правами *оператора*.

Для настройки использования для аутентификации и авторизации RADIUS сервера необходимо проделать следующие шаги:

- настроить параметры первичного RADIUS сервера с помощью команды

radius server master, указав в качестве аргументов IP-адрес сервера, секретный ключ сервера и порт на сервере, на который высылаются запросы аутентификации:

fnpsh> user radius server master 193.19.4.54 radseckey 1645
FNPSH-I-30B4-Конфигурация RADIUS сервера изменена
fnpsh>

- при необходимости с помощью команды radius server slave можно настроить вторичный RADIUS сервер, к которому будет происходить обращение в случае отсутствия ответа от первичного сервера:

fnpsh> user radius server slave 193.19.4.59 slaveseckey 1645
FNPSH-I-30B4-Конфигурация RADIUS сервера изменена
fnpsh>

- включить использование протокола RADIUS с помощью команды radius enable:

fnpsh> user radius enable
FNPSH-I-30B2-Использование RADIUS включено
fnpsh>
fnpsh> user radius show
Использование RADIUS: включено
Тайм-аут ожидания: 5
Количество обращений к серверу: 3
Первичный (MASTER) сервер: 193.19.4.54
Секретный ключ: radseckey
Порт: 1645
Вторичный (SLAVE) сервер: 193.19.4.59
Секретный ключ: slaveseckey
Порт: 1645
fnpsh>

После проделанных шагов при очередной попытке получения доступа к командному интерфейсу администратора ССПТ-2 будет использоваться аутентификация и авторизация на RADIUS сервере. По умолчанию тайм-аут ожидания ответа от RADIUS сервера составляет 5 секунд (его можно изменить с помощью команды radius timeout), количество попыток обращений к каждому RADIUS серверу по умолчанию 3 (этот параметр можно изменить с помощью команды radius retry). В случае недоступности указанных RADIUS серверов (введены неверные IP-адреса

серверов или они недоступны) общая задержка при получении доступа к командному интерфейсу администратора ССПТ-2 может составлять до 30 секунд (в случае использования значений по умолчанию).

Для отключения аутентификации и авторизации по RADIUS используется команда:

fnpsh>user radius disable
Отключить использование RADIUS? (Y/N) [N]: y
FNPSH-I-30B3-Использование RADIUS отключено
fnpsh>

4.1.2. Использование для подключения к ССПТ-2 системной консоли

Для первого подключения к ССПТ-2 удобно использовать управляющую консоль ССПТ-2. Чтобы получить доступ командному интерфейсу администратора через управляющую консоль необходимо:

- отключить питание на ССПТ-2;
- подключить монитор и клавиатуру к соответствующим разъемам на задней панели ССПТ-2 (питание на мониторе должно быть отключено);
- включить питание на ССПТ-2 и мониторе.

После загрузки управляющей операционной системы ССПТ-2 на экран будет выдано приглашение операционной системы, после чего необходимо последовательно пройти системную авторизацию и авторизацию ССПТ-2:

login: fnpsh
Password: *******
Межсетевой экран ССПТ-2
Командный интерфейс, версия 1.0
ЗАО "НПО РТК", 2006. Все права защищены

Имя пользователя: admin
Пароль: *******

FNPSH-I-3001-Успешная авторизация пользователя
fnpsh>

4.1.3. Использование для подключения к ССПТ-2 последовательного порта (COM)

Подключение к командному интерфейсу администратора возможно с управляющего компьютера через последовательный порт RS-232. Связь с ССПТ-2 осуществляется с использованием механизма удаленного доступа на базе протокола PPP (*Point-to-Point Protocol*).

Для установления связи с ССПТ-2 необходимо выполнить следующие действия:

1) Остановить управляющую операционную систему и отключить электропитание на ССПТ-2;

2) Остановить управляющую операционную систему и отключить электропитание на управляющем компьютере;

3) Соединить последовательные порты ССПТ-2 и управляющего компьютера с помощью нуль-модемного кабеля (входит в комплект поставки). Включить электропитание на ССПТ-2 и управляющем компьютере;

4) Осуществить настройку соединения удаленного доступа, используя в списке выбора устройств «Null-modem PPP connection with FNP-2 Firewall» в соответствии с Руководством, размещенном на поставляемом носителе;

5) Установить соединение с ССПТ-2 с использованием утилиты доступа по защищенному каналу fnptel, в соответствии с Руководством, размещенном на поставляемом носителе.

В случае успешного соединения на экран будет выдано приглашение операционной системы, после чего необходимо последовательно пройти системную авторизацию и авторизацию ССПТ-2.

FreeBSD/i386 (fnp2) (ttyd0)

login: fnpsh
Password: *******
Межсетевой экран ССПТ-2
Командный интерфейс, версия 1.0
(c) ЗАО "НПО РТК", 2006. Все права защищены
Имя пользователя: admin
Пароль: *******
FNPSH-I-3001-Успешная авторизация пользователя
fnpsh>

4.1.4. Использование для подключения к ССПТ-2 управляющего сетевого интерфейса (Eth.C)

Подключение к командному интерфейсу администратора возможно с управляющего компьютер через управляющий интерфейс Eth.C ССПТ-2. Для этого необходимо выполнить следующие действия:

1) Установить IP-адрес управляющего интерфейса на ССПТ-2. Для этого необходимо получить доступ к командному интерфейсу администратора через управляющую консоль или последовательный порт и установить IP-адрес управляющего интерфейса, например:

fnpsh> interface control address 192.168.2.1/255.255.255.0
FNPSH-I-3024-IP адрес управляющего интерфейса изменен
fnpsh>

2) Установить соответствующий IP-адрес (из тойже IP-подсети, что и адрес управляющего интерфейс) на Ethernet-интерфейсе управляющего компьютера;

3) Соединить Ethernet-интерфейс управляющего компьютера и управляющий интерфейс (Eth.C) ССПТ-2;

4) С использованием утилиты доступа по защищенному каналу fnptel установить соединение управляющего компьютера с ССПТ-2 по сети Ethernet. После установки соединения в окне терминальной программы будет выдано приглашение операционной системы, после чего необходимо последовательно пройти систем-

ную авторизацию и авторизацию ССПТ-2.

login: fnpsh
Password: *******
Межсетевой экран ССПТ-2
Командный интерфейс, версия 1.0
(c) ЗАО "НПО РТК", 2006. Все права защищены
Имя пользователя: admin
Пароль: *******
FNPSH-I-3001-Успешная авторизация пользователя
fnpsh>

4.2. Наборы правил

4.2.1. Предустановленные дополнительные наборы правил

Межсетевой экран ССПТ-2 поставляется с настройками по умолчанию, запрещающими передачу пакетов через его фильтрующие интерфейсы. Для разрешения передачи всех пакетов через ССПТ-2 можно воспользоваться функцией загрузки дополнительных наборов правил. В ССПТ-2 имеется два предустановленных дополнительных набора правил: default_accept (набор правил, разрешающий передачу всех пакетов) и default_drop (набор правил, запрещающий передачу всех пакетов). Чтобы загрузить дополнительный набор правил, необходимо воспользоваться командой rule load:

fnpsh> rule load default_accept
Загрузить дополнительный набор правил (режим управления сессиями)? (Y/N)[N]: y
FNPSH-I-304A-Таблица сессий очищена
FNPSH-I-301E-Дополнительный набор правил загружен
fnpsh>

После выполнения приведенной выше команды все пакеты будут пропускаться через фильтрующие интерфейсы ССПТ-2.

Для инициализации текущего набора правил правилами по умолчанию пред-

назначена команда **rule default**. После выполнения этой команды прохождение пакетов через ССПТ-2 будет запрещено.

4.2.2. Инициализация текущей конфигурации ССПТ-2 значениями по умолчанию

Для инициализации текущей конфигурации ССПТ-2 значениями по умолчанию используется команда **conf[ig] def[ault]**. Требуемые привилегии: cfg.

Команда назначает параметрам текущей конфигурации ССПТ значения по умолчанию в соответствии с таблицей 4.1.

Таблица 4.1 - Значения по умолчанию параметров конфигурации ССПТ

Параметр	Значение по умолчанию
Управляющий интерфейс	отключен
IP адрес/маска управляющего интерфейса	10.234.28.71/255.255.0.0
Скорость/режим передачи управляющего интерфейса	auto
Список доступа	очищен
Маршрут по умолчанию	отключен
IP адрес шлюза	удален
Фильтрующие интерфейсы	включены
Скорость/режим передачи фильтрующих интерфейсов	auto
Зеркалирование интерфейсов	отключено

Пример:

fnpsh> config default
Загрузить конфигурацию по умолчанию? (Y/N) [N]: y
FNPSH-I-3052-Конфигурация по умолчанию загружена

4.3. Останов и перезагрузка управляющей операционной системы

Для корректного останова управляющей операционной системы (УОС) и отключения устройства предназначена команда **system halt**:

fnpsh> system halt
Выключить устройство? (Y/N) [N]: y
FNPSH-I-3006-Устройство будет выключено через две минуты. Выход ...

Для отключения ССПТ-2 необходимо произвести останов УОС и отключить электропитание.

Для перезагрузки УОС предназначена команда **system reboot**:

fnpsh> system reboot
Перегрузить устройство? (Y/N) [N]:
FNPSH-I-3007-Устройство будет перезагружено через две минуты. Выход ...

4.4. Командный интерфейс администратора

ПО ССПТ-2 предоставляет администратору в качестве средства администрирования интерфейс командной строки как для локального (с системной консоли ССПТ-2), так и для удаленного администрирования.

Интерфейс командной строки администрирования обеспечивает возможность:

1) просмотра информации о состоянии изделия, режимах его работы и текущей статистической информации, обеспечивающей сигнализацию попыток нарушения установленных правил фильтрации посредством вывода на монитор администратора информации об общих результатах фильтрации проходящего трафика пакетов;

2) просмотра и выборки зарегистрированной информации об обработанных пакетах;

3) просмотра и выборки зарегистрированной информации о действиях администратора и пользователей с возможностью поиска необходимых сообщений;

4) просмотра системных сообщений изделия;

5) просмотра установленных интервалов времени;

6) просмотра установленных правил фильтрации;

7) просмотра и управления учетными записями пользователей (добавление,

удаление и редактирование идентификатора, пароля и прав доступа пользователя), имеющих право работы с изделием;

8) удаления информации о зарегистрированных пакетах (очистки регистрационных журналов);

9) останова управляющей операционной системы изделия;

10) останова и запуска процесса фильтрации;

11) запуска процедуры контроля целостности и отображение результатов контроля;

12) изменения режимов работы изделия и установки параметров конфигурации фильтров;

13) установки, удаления и изменения интервалов времени с возможностью записи произведенных изменений в файл интервалов времени и сообщением подсистеме фильтрации о необходимости изменения интервалов времени, действующих в настоящий момент;

14) установки, удаления и изменения правил фильтрации с возможностью записи произведенных изменений в файлы правил и сообщением подсистеме фильтрации о необходимости изменения правил, действующих в настоящий момент;

15) установки режима сохранения зарегистрированной информации об обработанных пакетах на внешнем сервере;

16) загрузки со станции управления на изделие и выгрузки с изделия на станцию управления текстового файла, содержащего правила фильтрации и интервалы времени, и файла конфигурации ССПТ-2.

Далее приводится перечень всех команд командного интерфейса ССПТ-2. Таблица 4.2 содержит краткое описание команд – синтаксис, требуемые привилегии и назначение.

В описании синтаксиса команд приводятся максимально допустимые сокращения ключевых слов командного языка ССПТ-2, обозначаемые парой квадратных скобок - '[]'. Например, описание **conf[ig] def[ault]** означает, что данная команда может быть введена одним из следующих способов:

fnpsh> conf def (максимально допустимое сокращение)
fnpsh> config default

и т.д.

Таблица 4.2 – Команды командного интерфейса ССПТ-2

Команда	**Требуемые привилегии**	**Описание**
conf[ig] def[ault]	cfg	Инициализация текущей конфигурации значениями по умолчанию
conf[ig] lis[t]	read	Просмотр списка дополнительных конфигураций
conf[ig] lo[ad] <имя_конфигурации>	cfg и pf	Загрузка дополнительной конфигурации
conf[ig] rem[ove] <имя_конфигурации>	cfg	Удаление дополнительной конфигурации
conf[ig] sav[e] <имя_конфигурации>	cfg	Сохранение текущей конфигурации в дополнительной
conf[ig] sh[ow] [<имя_конфигурации>]	read	Просмотр параметров текущей или дополнительной конфигурации
Exit	read	Завершение сеанса работы пользователя
fil[ter] rest[art]	pf	Перезапуск пакетного фильтра
fil[ter] start	pf	Запуск пакетного фильтра
fil[ter] statu[s]	read	Вывод информации о состоянии пакетного фильтра
fil[ter] stop	pf	Останов пакетного фильтра
gate[way] del[ete]	cfg	Удаление маршрута по умолчанию
gate[way] dis[able]	cfg	Отключение маршрута по умолчанию
gate[way] en[able]	cfg	Включение маршрута по умолчанию
gate[way] set <IP_адрес>	cfg	Установка IP адреса шлюза
gate[way] sh[ow]	read	Вывод состояния настроек маршрута по умолчанию
help	read	Вывод краткой справки по всем категориям команд
interf[ace] cont[rol] acl add <IP_адрес/маска>	cfg	Добавление записи в список доступа
interf[ace] cont[rol] acl cl[ear]	cfg	Очистка списка доступа
interf[ace] cont[rol] acl del[ete] <IP_адрес/маска>	cfg	Удаление записи из списка доступа
interf[ace] cont[rol] acl sh[ow]	read	Просмотр элементов списка доступа

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
interf[ace] cont[rol] addr[ess] <IP_адрес/маска>	cfg	Назначение IP адреса управляющему интерфейсу. Также можно вводить IP адрес управляющего интерфейса без маски, по умолчанию берется маска, соответствующая классу IP адреса
interf[ace] cont[rol] dis[able]	cfg	Отключение управляющего интерфейса
interf[ace] cont[rol] dup[lex] {half|ful[l]}	cfg	Установка режима передачи управляющего интерфейса
interf[ace] cont[rol] en[able]	cfg	Включение управляющего интерфейса
interf[ace] cont[rol] med[ia] {auto|10|100|1000}	cfg	Установка скорости передачи управляющего интерфейса
interf[ace] cont[rol] ping <IP_адрес>	read	Проверка доступности узлов в управляющей сети
interf[ace] cont[rol] sh[ow]	read	Просмотр настроек и состояния управляющего интерфейса
interf[ace] fil[ter] {all|<номер>|<имя>} dis[able]	cfg	Отключение фильтрующего интерфейса
interf[ace] fil[ter] {all|<номер>|<имя>} dup[lex] {half|ful[l]}	cfg	Установка режима передачи фильтрующего интерфейса
interf[ace] fil[ter] {all|<номер>|<имя>} med[ia] {auto|10|100|1000}	cfg	Установка скорости передачи фильтрующего интерфейса
interf[ace] fil[ter] {<номер>|<имя>} mir[ror] <имя> {all|in|out}	cfg	Установка параметров зеркалирования фильтрующих интерфейсов
interf[ace] fil[ter] {<номер>|<имя>} mir[ror] del[ete]	cfg	Удаление параметров зеркалирования фильтрующих интерфейсов
interf[ace] fil[ter] {<номер>|<имя>} mir[ror] dis[able]	cfg	Отключение режима зеркалирования фильтрующих интерфейсов
interf[ace] fil[ter] {<номер>|<имя>} ren[ame] <новое_имя>	cfg	Переименование фильтрующего интерфейса
interf[ace] fil[ter] {all|<номер>|<имя>} sh[ow]	read	Вывод информации о состоянии фильтрующего интерфейса

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
interf[ace] fil[ter] {all|<номер>|<имя>} stats	read	Вывод информации о статистике трафика на фильтрующем интерфейсе
log ev[ent] sh[ow] [<критерии_отбора>]	read	Просмотр зарегистрированных событий
log export ftp cl[ear]	log или cfg	Удаление параметров выгрузки файлов регистрации по FTP
log export ftp en[able]	log или cfg	Включение выгрузки файлов регистрации по FTP
log export ftp del[ete]	log или cfg	Удаление параметров выгрузки файлов регистрации по FTP
log export ftp dis[able]	log или cfg	Отключение выгрузки файлов регистрации по FTP
log export ftp set <IP_адрес> <путь> <вход> [<пароль>]	log или cfg	Установка параметров выгрузки файлов регистрации по FTP
log exp[ort] sysl[og] dis[able]	log или cfg	Отключение выгрузки системных сообщений на SYSLOG-сервер
log exp[ort] sysl[og] en[able]	log или cfg	Включение выгрузки системных сообщений на SYSLOG-сервер
log exp[ort] sysl[og] serv[er] <IP_адрес>	log или cfg	Установка IP-адреса SYSLOG-сервера
log pack[et] cl[ear]	log	Очистка регистрации пакетов
log pack[et] dis[able]	log	Отключение режима регистрации пакетов
log pack[et] en[able]	log	Включение режима регистрации пакетов
log pack[et] sh[ow] [<критерии_отбора>]	read	Просмотр зарегистрированных пакетов
log ses[sion] cl[ear]	log	Очистка регистрации сессий
log ses[sion] sh[ow] [<критерии_отбора>]	read	Просмотр зарегистрированных сессий
log sysl[og] sh[ow]	read	Просмотр системных сообщений
log sh[ow]	read	Просмотр параметров подсистемы регистрации
nat arp add <запись>	cfg или pf	Добавление записи в ARP таблицу
nat arp cl[ear]	cfg или pf	Очистка ARP таблицы
nat arp del[ete] <запись>	cfg или pf	Удаление записи из ARP таблицы
nat arp sh[ow]	read	Просмотр записей ARP таблицы

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
nat aut[hentication] en[able]	cfg или pf	Включение аутентификации сетевых пользователей
nat aut[hentication] dis[able]	cfg или pf	Отключение аутентификации сетевых пользователей
nat aut[hentication] timeo[ut]	cfg или pf	Изменение тайм-аута неактивности сетевых пользователей
nat dis[able]	cfg или pf	Отключение режима NAT
nat en[able]	cfg или pf	Включение режима NAT
nat key add <IP_адрес>	admin	Добавление записи в файл ключей аутентификации
nat key del[ete] <IP_адрес>	admin	Удаление записи из файла ключей аутентификации
nat key upd[ate] <IP_адрес>	admin	Обновление записи в файле ключей аутентификации
nat key sh[ow] [<IP_адрес>]	admin	Вывод записей из файла ключей аутентификации
nat log dis[able]	cfg или pf	Отключение регистрации пакетов, отбрасываемых NAT
nat log en[able]	cfg или pf	Включение регистрации пакетов, отбрасываемых NAT
nat port <порт_мин>-<порт_макс>	cfg или pf	Установка диапазона портов для NAT
nat priva[te] del[ete]	cfg или pf	Удаление параметров внутреннего интерфейса NAT
nat priva[te] ip <IP_адрес/маска>	cfg или pf	Установка IP адреса внутреннего интерфейса NAT
nat priva[te] mac <MAC_адрес>	cfg или pf	Установка MAC адреса внутреннего интерфейса NAT
nat pub[lic] del[ete]	cfg или pf	Удаление параметров внешнего интерфейса NAT
nat pub[lic] gate[way] <IP_адрес>	cfg или pf	Установка шлюза для внешнего интерфейса NAT
nat pub[lic] ip <IP_адрес/маска>	cfg или pf	Установка IP адреса внешнего интерфейса NAT
nat pub[lic] mac <MAC_адрес>	cfg или pf	Установка MAC адреса внешнего интерфейса NAT
nat red[irect] add <запись>	cfg или pf	Добавление записи в таблицу переадресации NAT

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
nat red[irect] cl[ear]	cfg или pf	Очистка таблицы переадресации NAT
nat red[irect] del[ete] <запись>	cfg или pf	Удаление записи из таблицы переадресации NAT
nat red[irect] dmz dis[able]	cfg или pf	Отключение переадресации с интерфейсов DMZ
nat red[irect] dmz en[able]	cfg или pf	Включение переадресации с интерфейсов DMZ
nat red[irect] pub[lic] dis[able]	cfg или pf	Отключение переадресации с внешнего интерфейса
nat red[irect] pub[lic] en[able]	cfg или pf	Включение переадресации с внешнего интерфейса
nat red[irect] sh[ow]	read	Просмотр записей таблицы переадресации NAT
nat sh[ow]	read	Просмотр параметров NAT
nat us[er] add <пользователь> <параметры>	admin	Добавление сетевого пользователя
nat us[er] cl[ear] <пользователь>	admin	Сброс сетевого пользователя
nat us[er] del[ete] <пользователь>	admin	Удаление сетевого пользователя
nat us[er] dis[able] <пользователь>	admin	Отключение сетевого пользователя
nat us[er] en[able] <пользователь>	admin	Включение сетевого пользователя
nat us[er] ed[it] <пользователь> <параметры>	admin	Редактирование параметров сетевого пользователя
nat us[er] lis[t]	read	Вывод базы данных сетевых пользователей
nat us[er] pass[word] <пользователь>	admin	Изменение пароля сетевого пользователя
nat us[er] sh[ow]	read	Вывод списка активных сетевых пользователей
rese[rv] conf[ig] sync[hronize]	cfg или ha	Выполнение немедленной синхронизации конфигурации
rese[rv] def[ault]	cfg или ha	Установка параметров подсистемы высокой готовности в значения по умолчанию
rese[rv] dis[able]	cfg или ha	Отключение подсистемы высокой готовности

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
rese[rv] en[able]	cfg или ha	Включение подсистемы высокой готовности
rese[rv] mod[e] {bal[ance]|mas[ter]|sla[ve]|stp}	cfg или ha	Установка режимов подсистемы высокой готовности
rese[rv] neighbour <IP_адрес>	cfg или ha	Установка IP адреса парного устройства для подсистемы высокой готовности
rese[rv] rul[e] sync[hronize]	cfg или ha	Выполнение немедленной синхронизации правил фильтрации для подсистемы высокой готовности
rese[rv] sh[ow]	read	Просмотр параметров подсистемы высокой готовности
rese[rv] interf[ace] act[ive] med[ia] <значение>	cfg или ha	Установка скорости фильтрующих интерфейсов для активного состояния устройства
rese[rv] interf[ace] act[ive] dup[lex] <значение>	cfg или ha	Установка дуплекса фильтрующих интерфейсов для активного состояния устройства
rese[rv] interf[ace] bl[ocked] med[ia] <значение>	cfg или ha	Установка скорости фильтрующих интерфейсов для заблокированного состояния устройства
rese[rv] interf[ace] bl[ocked] dup[lex] <значение>	cfg или ha	Установка дуплекса фильтрующих интерфейсов для заблокированного состояния устройства
rul[e] add <определение_правила>	rules	Добавление правила фильтрации в текущий набор
rul[e] copy <сущ_правило> <новое_правило>	rules	Копирование правила фильтрации в текущем наборе
rul[e] def[ault]	rules	Установка текущего набора правил в состояние по умолчанию
rul[e] del[ete] <идентификатор_правила>	rules	Удаление правила фильтрации из текущего набора
rul[e] ed[it] <определение_правила>	rules	Изменение существующего правила фильтрации в текущем наборе
rul[e] lis[t]	read	Просмотр списка дополнительных наборов правил
rul[e] lo[ad] <имя_набора_правил>	rules	Загрузка дополнительного набора правил

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
rul[e] mov[e] <тип> <сущ_номер> <новый_номер>	rules	Перенос правила фильтрации в текущем наборе
rul[e] sav[e] <имя_набора_правил>	rules	Сохранение текущего набора правил в дополнительном
rul[e] stats cl[ear]	pf	Сброс статистики трафика по текущему набору правил фильтрации
rul[e] stats sh[ow]	read	Просмотр статистики трафика по текущему набору правил
rul[e] rem[ove] <имя_набора_правил>	rules	Удаление дополнительного набора правил
rul[e] roll[back]	rules	Откат к предыдущему состоянию текущего набора правил
rul[e] sh[ow] [<имя_набора_правил>]	read	Просмотр списка правил фильтрации текущего или дополнительного наборов правил
ses[sion] ap dis[able]	cfg или pf	Отключение использования AP правил
ses[sion] ap en[able]	cfg или pf	Включение использования AP правил
ses[sion] deept[cp] dis[able]	cfg или pf	Отключение глубокого контроля TCP
ses[sion] deept[cp] en[able]	cfg или pf	Включение глубокого контроля TCP
ses[sion] dis[able]	cfg или pf	Отключение режима управления сессиями
ses[sion] en[able]	cfg или pf	Включение режима управления сессиями
ses[sion] fl[ood] ala[rm] dis[able]	cfg или pf	Отключение сигнализации обнаружения flood-атак
ses[sion] fl[ood] ala[rm] en[able]	cfg или pf	Включение сигнализации обнаружения flood-атак
ses[sion] fl[ood] dis[able]	cfg или pf	Отключение блокировки flood-атак
ses[sion] fl[ood] en[able]	cfg или pf	Включение блокировки flood-атак
ses[sion] fl[ood] rul[e] com[ments] <комметарий>	cfg или pf	Редактирование комментария для временного IP правила, блокирующего flood-атаку
ses[sion] fl[ood] rul[e] lif[etime]	cfg или pf	настройка времени жизни временного IP правила, блокирующего flood-атаку

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
ses[sion] fl[ood] rul[e] log dis[able]	cfg или pf	Отключение регистрации пакетов во временном IP правиле, блокирующем flood-атаку
ses[sion] fl[ood] rul[e] log en[able]	cfg или pf	Включение регистрации пакетов во временном IP правиле, блокирующем flood-атаку
ses[sion] fl[ood] thr[eshold] def[ault]	cfg или pf	Установка пороговых значений обнаружения flood-атак по умолчанию
ses[sion] fl[ood] thr[eshold] icmp <порог>	cfg или pf	Установка порогового значения обнаружения flood-атак для протокола ICMP
ses[sion] fl[ood] thr[eshold] tcp <порог>	cfg или pf	Установка порогового значения обнаружения flood-атак для протокола TCP
ses[sion] fl[ood] thr[eshold] udp <порог>	cfg или pf	Установка порогового значения обнаружения flood-атак для протокола UDP
ses[sion] ip dis[able]	cfg или pf	Отключение создания сессий по умолчанию для IP правил фильтрации
ses[sion] ip en[able]	cfg или pf	Включение создания сессий по умолчанию для IP правил фильтрации
ses[sion] log dis[able]	cfg или pf	Отключение регистрации пакетов, отброшенных механизмом управления сессиями
ses[sion] log en[able]	cfg или pf	Включение регистрации пакетов, отброшенных механизмом управления сессиями
ses[sion] mac dis[able]	cfg или pf	Отключение использования данных канального уровня в управлении сессиями
ses[sion] mac en[able]	cfg или pf	Включение использования данных канального уровня в управлении сессиями
ses[sion] sh[ow]	read	Просмотр параметров управления сессиями
ses[sion] tab[le] cl[ear]	pf	Очистка таблицы сессий
ses[sion] tab[le] cl[ear] nol[og]	pf	Ускоренная очистка таблицы сессий

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
ses[sion] tab[le] del[ete] <номер_сессии>	pf	Удаление сессии из таблицы сессий
ses[sion] tab[le] sh[ow] [<параметры_выборки>]	read	Просмотр таблицы сессий
ses[sion] tab[le] siz[e] <размер_таблицы>	cfg или pf	Изменение размера таблицы сессий
ses[sion] timeo[ut] def[ault]	cfg или pf	Установка тайм-аутов сессий в значения по умолчанию
ses[sion] timeo[ut] icmp {est[ablished]|syn} <тайм_аут>	cfg или pf	Установка тайм-аута сессий для протокола ICMP
ses[sion] timeo[ut] tcp {est[ablished]|fin|syn} <тайм_аут>	cfg или pf	Установка тайм-аута сессий для протокола TCP
ses[sion] timeo[ut] udp {est[ablished]|syn} <тайм_аут>	cfg или pf	Установка тайм-аута сессий для протокола UDP
syst[em] fnpsh his[tory] cl[ear]	read	Очистка буфера введенных команд
syst[em] fnpsh his[tory] sh[ow]	read	Просмотр буфера введенных команд
syst[em] fnpsh v[iewer] <просмотрщик>	read	Установка просмотрщика по умолчанию для fnpsh
syst[em] fnpsh pass[word]	admin	Изменение пароля fnpsh
syst[em] fnpsh timeo[ut] <тайм_аут>	cfg или sys	Установка тайм-аута неактивности для командного интерфейса
syst[em] halt	sys	Останов устройства
syst[em] ich[eck]	read	Проверка целостности программного обеспечения ССПТ-2
syst[em] password	user	Изменение пароля системного пользователя
syst[em] reboot	sys	Перезагрузка устройства
syst[em] sh[ow]	read	Вывод информации о программном и аппаратном обеспечении ССПТ-2
sys[tem] snmp ena[ble]	admin	Включение SNMP-интерфейса **(Данная команда доступна только с системной консоли)**
sys[tem] snmp dis[able]	admin	Отключение SNMP-интерфейса **(Данная команда доступна только с системной консоли)**
sys[tem] snmp pass[word]	admin	Изменение пароля SNMP-интерфейса **(Данная команда доступна только с системной консоли)**

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
syst[em] status	read	Вывод информации о состоянии ресурсов операционной системы ССПТ-2
syst[em] time ntp del[ete]	cfg	Удаление параметров синхронизации времени по NTP
syst[em] time ntp dis[able]	cfg	Отключение синхронизации времени по NTP
syst[em] time ntp en[able]	cfg	Включение синхронизации времени по NTP
syst[em] time ntp log dis[able]	cfg	Отключение регистрации NTP запросов
syst[em] time ntp log en[able]	cfg	Включение регистрации NTP запросов
syst[em] time ntp serv[er] <IP_адрес>	cfg	Установка IP адреса NTP сервера
syst[em] time ntp timeo[ut] <тайм_аут>	cfg	Установка тайм-аута опроса NTP сервера
syst[em] time ntp upd[ate]	cfg	Синхронизация времени с NTP сервером
syst[em] time set {<ГГГГ/ММ/ДД [ЧЧ:ММ:СС]>| <ЧЧ:ММ:СС>	sys	Установка системного времени
syst[em] time sh[ow]	read	Вывод системного времени и параметров синхронизации по NTP
syst[em] time zone [<файл_часового_пояса>]	sys	Установка часового пояса
us[er] add <имя_пользователя> <привилегии>	admin	Добавление нового пользователя
syst[em] web en[able]	admin	Включение WEB интерфейса
syst[em] web dis[able]	admin	Отключение WEB интерфейса
us[er] add <имя_пользователя> <привилегии>	admin	Добавление нового пользователя
us[er] del[ete] <имя_пользователя>	admin	Удаление пользователя
us[er] dis[able] <имя_пользователя>	admin	Отключение пользователя
us[er] en[able] <имя_пользователя>	admin	Включение пользователя
us[er] lis[t]	read	Просмотр списка существующих пользователей

Продолжение таблицы 4.2

Команда	Требуемые привилегии	Описание
us[er] pass[word] <имя_пользователя> [[<старый_пароль>] <новый_пароль>]	admin	Изменение паролей пользователей
us[er] privi[lege] <имя_пользователя> <привилегии>	admin	Изменение привилегий пользователя
us[er] rad[ius] dis[able]	user	Отключение RADIUS авторизации
us[er] rad[ius] en[able]	user	Включение RADIUS авторизации
us[er] rad[ius] ret[ry] <число_попыток>	user	Установка максимального количества попыток обращения к RADIUS серверу
us[er] rad[ius] serv[er] <тип> <IP_адрес> <ключ> <порт>	user	Настройка параметров RADIUS авторизации
us[er] rad[ius] sh[ow]	user	Просмотр параметров RADIUS авторизации

Командный интерфейс администратора имеет следующие настраиваемые параметры:

1) Тайм-аут неактивности. При срабатывании данного тайм-аута (что означает отсутствие запросов от пользователя в течение данного промежутка времени) пользователь принудительно отключается от командного интерфейса администратора. Значение по умолчанию тайм-аута неактивности – 600 секунд. Диапазон допустимых значений: 10-3600 секунд. Для изменения тайм-аута неактивности предназначена команда system fnpsh timeout:

fnpsh> system fnpsh timeout 3600
FNPSH-I-3088-Тайм-аут неактивности командного интерфейса изменен
fnpsh>

2) Просмоторщик (режим просмотра информации) по умолчанию. Для удобства просмотра больших объемов информации (таблицы правил фильтрации, параметры конфигурации) в командном интерфейсе администратора предусмотрены следующие режимы просмотра (просмоторщики):

- **internal:** используется внутренний полноэкранный просмоторщик команд-

ного интерфейса;

- **more:** используется постраничный вывод информации с возможностью передвижения назад и вперед;

- **no:** просмоторщики не используется, информация выводится на экран полностью (возможно частичное исчезновение информации вверху экрана).

По умолчанию используется внутренний просмоторщик (internal). Для изменения просмоторщика по умолчанию используется команда system fnpsh viewer:

fnpsh> system fnpsh viewer more
FNPSH-I-3087-Режим просмотра изменен
fnpsh>

Установка нового просмоторщика по умолчанию действует только на один сеанс работы в командном интерфейсе администратора. При выходе из командного интерфейса настройка данного параметра теряется.

3) Пароль системной авторизации (системного пользователя). Для системной авторизации используется пользователь с именем fnpsh. Для изменения пароля данного пользователя предусмотрена команда system fnpsh password:

fnpsh> system fnpsh password
Старый пароль: *********
Новый пароль: *********
Новый пароль повторно: *********
FNPSH-I-309E-Пароль системного пользователя изменен
fnpsh>

Данная команда запрашивает старый пароль пользователя и в случае правильного указания старого пароля предоставляет возможность ввести новый пароль.

4) Буфер истории команд. Для просмотра буфера истории команд предусмотрена команда system fnpsh history show :

fnpsh> system fnpsh history show
Буфер истории команд:
1 - system time ntp log ?
2 - system time ntp log enable
3 - system time ntp

4 - system time ntp update 193.13.18.5
5 - system fnpsh
6 - system fnpsh history
7 - system fnpsh history show
fnpsh>

Для очистки буфера истории команд предусмотрена команда system fnpsh history clear:

fnpsh> system fnpsh history clear
Очистить буфер истории команд? (Y/N) [N]: y
FNPSH-I-3022-Буфер истории команд очищен
fnpsh>

Буфер истории команд содержит 100 последних команд, введенных пользователем, и хранится в течение одного сеанса, т.е. по окончании работы пользователя его история команд теряется.

4.5. Управление списком пользователей ССПТ-2

Командный интерфейс ССПТ-2 предоставляет следующие команды управления списком пользователей:

us[er] add - добавить нового пользователя;

us[er] del[ete] - удалить существующего пользователя;

us[er] dis[able] - блокировать пользователя;

us[er] en[able] - деблокировать пользователя;

us[er] list - просмотр существующих пользователей;

us[er] pass[word] - сменить пароль пользователю;

us[er] privil[ege] - изменить набор привилегий пользователю;

us[er] show - просмотр работающих в данный момент пользователей.

Для добавления нового пользователя используется команда **user add <имя_пользователя><привилегии>,** где **<имя_пользователя>** должно отвечать следующим ограничениям:

- длина имени пользователя должна быть от **2** до **16** символов включительно;

- допустимые символы в имени пользователя - строчные латинские буквы (**a-z**), цифры (**0-9**) и нижнее подчеркивание (_), а **<привилегии>** определяют право на работу добавляемого пользователя с различными подсистемами ССПТ-2, каждая привилегия имеет символическое имя.

1) **log** – привилегия для работы с подсистемой регистрации

2) **cfg** – привилегия для настройки параметров ССПТ-2.

3) **rules** – привилегия для работы с правилами фильтрации.

4) **pf** – привилегия для работы с подсистемой фильтрации.

5) **sys** – привилегия для общего управления устройством.

6) **ha** – привилегия для работы с подсистемой высокой готовности.

7) **user –** управление пользователями (только для пользователя **admin**).

Список команд в соответствии с необходимыми привилегиями приведен в таблице 4.2.

Списки привилегий могут задаваться перечислением символических имен привилегий. Последние перечисляются в списке через запятую. Например, 'sys,cfg,user'. Все привилегии могут быть заменены привилегией full. Не допускается указывать в списке одну и ту же привилегию более одного раза. Наряду с перечисленными выше именами привилегий имеются еще два специальных имени:

- **read** - означает отсутствие каких бы то ни было привилегий (режим "только чтение");

- **full** - означает полный набор привилегий, что соответствует списку всех привилегий и привилегии управления списком пользователей.

Подсистема авторизации управляет списком "занятых" привилегий. Список содержит привилегии, которые уже предоставлены активным на данный момент пользователям. Это необходимо для того, чтобы одной и той же привилегией обладал один и только один активный на данный момент пользователь.

Права активного (авторизованного) пользователя определяются списком его текущих привилегий, которые формируются подсистемой авторизации на основе

списка привилегий из учетной записи пользователя и списка "занятых" привилегий по следующим правилам:

- на стадии авторизации пользователя сравниваются список привилегий пользователя, полученный из его учетной записи, со списком "занятых" привилегий;

- из списка привилегий пользователя исключаются привилегии, входящие в список "занятых" привилегий.

Таким образом, формируется список текущих привилегий пользователя;

На основе сформированного списка текущих привилегий корректируется список "занятых" привилегий. В него включаются все привилегии из списка текущих привилегий;

Пользователь начинает работу с привилегиями, входящими в его список текущих привилегий. Если список текущих привилегий оказался пустым, то такой пользователь будет работать в режиме "только чтение";

При выходе пользователя из списка "занятых" привилегий исключаются привилегии, входившие в список текущих привилегий данного пользователя. Таким образом, эти привилегии освобождаются для других пользователей, которые будут авторизоваться в дальнейшем. Данная процедура обеспечивает сохранение целостности всех структур данных ССПТ-2 за счет того, что не может возникнуть ситуации, когда два и более активных пользователя обладают одной и той же привилегией одновременно. Для любого пользователя ССПТ-2, за исключением пользователя admin, может быть изменен набор привилегий.

При выполнении команды **user add** подсистема авторизации осуществляет интерактивный запрос пароля нового пользователя.

Пароли пользователей должны отвечать следующим ограничениям:

- длина пароля должна быть от 6 до 128 символов включительно;

- допустимые символы - любые печатаемые (отображаемые) символы набора ASCII.

Для изменения привилегий пользователя используется команда **us[er]**

privil[ege] <имя_пользователя> <список_привилегий>.

Для изменения пароля пользователя используется команда **us[er] pass[word] <имя_пользователя> [[<старый_пароль>] <новый_пароль>]**.

Для просмотра зарегистрированных пользователей используется команда **us[er] list**. При выполнении этой команды подсистема авторизации выводит на экран список имен всех зарегистрированных пользователей и их статуса (блокирован/не блокирован).

Для просмотра работающих в данный момент пользователей используется команда **us[er] show**. При выполнении этой команды подсистема авторизации выводит на экран список имен всех работающих в данный момент пользователей.

Для блокировки всех полномочий пользователя без его удаления из списка пользователей используется команда **us[er] dis[able] <имя_пользователя>**.

Для разблокировки всех полномочий пользователя используется команда **us[er] en[able] <имя_пользователя>**.

Для удаления пользователя используется команда **us[er] del[ete] <имя_пользователя>**.

4.6. Системные настройки

Системные настройки ССПТ-2 реализует группа команд system, которая позволяет выполнить следующие действия:

1) проверка целостности информационных и исполняемых файлов программного обеспечения ССПТ-2;

2) просмотр параметров аппаратного обеспечения устройства;

3) просмотр параметров использования системных ресурсов;

4) изменение системной даты/времени;

5) настройка протокола NTP для синхронизации времени;

6) изменение параметров командного интерфейса администратора;

7) перезагрузка и отключение устройства.

4.6.1. Проверка целостности

Проверка целостности конфигурационных и исполняемых файлов программного обеспечения ССПТ-2 производится в целях контроля за несанкционированным изменением этих файлов (путем прямого редактирования/замены без использования штатных средств администрирования ССПТ-2). Проверка целостности осуществляется подсистемой контроля целостности в следующих случаях:

- при запуске программного обеспечения ССПТ-2;
- периодически во время работы программного обеспечения ССПТ-2;
- по запросу администратора.

При обнаружении нарушения контрольной суммы одного из проверяемых файлов подсистема контроля целостности выполняет следующие действия:

- останов пакетного фильтра;
- регистрация события о нарушении контрольной суммы с указанием имени файла;
- перевод сервера авторизации в однопользовательский режим работы – доступ администратора к ССПТ-2 будет возможен только в режиме командного интерфейса, только с системной консоли ССПТ-2 и только для администратора с идентификатором “admin”. В случае, если нарушена контрольная сумма одного из конфигурационных файлов, администратор имеет возможность восстановить данный файл путем загрузки конфигурации по умолчанию с помощью соответствующих команд.

Для того, чтобы проверить контрольные суммы по запросу администратора, предназначена команда **system icheck**.

Данная команда проверяет контрольные суммы предопределенных исполняемых и конфигурационных файлов ПО ССПТ-2 и в случае успешной проверки выводит первые 6 символов каждой контрольных суммы, при этом контрольные суммы исполняемых файлов должны совпадать с приведенными ниже, а контрольные суммы конфигурационных файлов изменяются при

реконфигурации устройства. Контрольные суммы исполняемых файлов, выводимые при команде **system icheck** должны совпадать с контрольными суммами, указанными в паспорте на устройство.

В случае, если управляющий интерфейс является первым:

fnpsh> system icheck

FNPSH-I-30AE-Проверка целостности выполнена

kernel	095cb9...
libc.so.7	dfc575...
libkvm.so.4	802b7c...
libssl.so.5	87fb73...
login	b8bd77...
ntpdate	685b6d...
telnetd	3bacae...
openssl	ecbe3d...
libfnpcrypt.so.1	ccd528...
fnpsh	18b1fa...
fnpinfo	00739e...
fnp_authd	5bd494...
fnp_csd	00357a...
fnp_filtd	a0dd5a...
fnp_logd	5ae298...
fnp_shd	1d8575...
libfnp.so.1	3c1f7e...
fnp_had	01d172...
fnp_cryd	45a095...
fnp2_gost.key	d79b1a...
fnp2_gost.sig	fc1b1a...
ca_gost.sig	f12e67...
fnp2_key.pem	eb6f8a...
fnp2_cert.pem	e9a9c2...
ca_cert.pem	d394e0...
master.passwd	5d1d26...
fnp.cf	54a3bf...
fnp_passwd	a704b6...
net_passwd	d41d8c...
fnp_net.keys	d41d8c...
mac.cf	610322...

```
arp.cf          fb0fd6...
ip.cf           066d14...
ipx.cf          cce7a5...
ap.cf           ee2792...
vlan.cf         ec5387...
time.cf         76b973...
fnpsh>
```

В случае, если управляющий интерфейс является последним:

```
fnpsh> system icheck
FNPSH-I-30AE-Проверка целостности выполнена
kernel          095cb9...
libc.so.7       dfc575...
libkvm.so.4     802b7c...
libssl.so.5     87fb73...
login           b8bd77...
ntpdate         685b6d...
telnetd         3bacae...
openssl         ecbe3d...
libfnpcrypt.so.1 ccd528...
fnpsh           18b1fa...
fnpinfo         00739e...
fnp_authd       5bd494...
fnp_csd         00357a...
fnp_filtd       a0dd5a...
fnp_logd        5ae298...
fnp_shd         1d8575...
libfnp.so.1     3c1f7e...
fnp_had         01d172...
fnp_cryd        45a095...
fnp2_gost.key   d79b1a...
fnp2_gost.sig   fc1b1a...
ca_gost.sig     f12e67...
fnp2_key.pem    eb6f8a...
fnp2_cert.pem   e9a9c2...
ca_cert.pem     d394e0...
master.passwd   5d1d26...
```

```
fnp.cf          864465...
fnp_passwd      5cb05c...
net_passwd      d41d8c...
fnp_net.keys    d41d8c...
mac.cf          af754f...
arp.cf          3db935...
ip.cf           f8e405...
ipx.cf          8434c6...
ap.cf           ee2792...
vlan.cf         ec5387...
time.cf         76b973...
fnpsh>
```

4.6.2. Поверка аппаратного обеспечения и системных ресурсов

Для контроля работы аппаратного и программного обеспечения ПО ССПТ-2 предназначены команды **system show** и **system status**.

Команда **system show** выводит:

- тип и частоту центрального процессора;
- количество оперативной памяти;
- общее количество сетевых интерфейсов Ethernet;
- количество и имена фильтрующих интерфейсов;
- параметры управляющего интерфейса;
- версию программного обеспечения ССПТ-2;
- наличие модулей программного обеспечению ССПТ-2 и их статус (запущен или остановлен);
- параметры командного интерфейса администратора (тайм-аут неактивности и просмоторщик (режим просмотра информации) по умолчанию).

```
fnpsh>system show
Центральный процессор: Intel(R) Pentium(R) 4 CPU 3.00GHz
Оперативная память: 528220160 bytes (503M)
Всего интерфейсов: 4
Фильтрующих интерфейсов: 3: eth0,eth1,eth2
Управляющий интерфейс: отключен
```

Версия ПО ССПТ-2:
Пакетный фильтр: запущен
Сервер авторизации: запущен
Сервер проверки контрольных сумм: запущен
Сервер высокой готовности: запущен
Сервер регистрации: запущен
Командный сервер: запущен
Сервер терминального доступа: запущен
Тайм-аут неактивности FNPSH: 600 секунд
Просмоторщик по умолчанию FNPSH: внутренний (internal)
fnpsh>

Команда **system status** выводит:

- данные по использованию центрального процессора;

- данные по использованию оперативной памяти;

- данные по использованию flash-памяти.

fnpsh> system status
Использование центрального процессора:
Пользовательские процессы: 0,0%
Приоритетные процессы: 0,0%
Системные процессы: 0,0%
Прерывания: 0,0%
Простой процессора: 100,0%
Использование оперативной памяти:
Активная: 16,0M
Неактивная: 3,0M
Свободно: 203,0M
Всего: 254M
Состояние flash-памяти:
Раздел: 0
Использовано: 32M (14%)
Свободно: 201M (86%)
Всего: 240M
Раздел: 1
Использовано: 1,0K (100%)
Свободно: 0B (0%)
Всего: 1,0K
Раздел: 2
Использовано: 10K (0%)
Свободно: 13M (100%)
Всего: 14M

fnpsh>

Приведенные команды могут быть полезны при поиске источника неисправностей в случае возникновения нештатных ситуаций.

4.6.3. Установка системного времени и даты

Для изменения параметров системной даты, времени и временной зоны предназначены команды **system time set** и **system time zone**:

1) команда system time set позволяет изменить системную дату и/или время, например:

fnpsh> system time set 2006/11/13 14:32:00
FNPSH-I-3057-Системное время изменено (13.11.2006 14:32:00, MSK)
fnpsh>

2) команда system time zone позволяет изменить временную зону, например:

fnpsh> system time zon
[1] Africa
[2] America - North and South
[3] Antarctica
[4] Arctic Ocean
[5] Asia
[6] Atlantic Ocean
[7] Australia
[8] Europe
[9] Indian Ocean
[10] Pacific Ocean
Выберите континент/регион (Отмена - <Enter>): 8
[1] Aland Islands [16] Gibraltar [31] Poland
[2] Albania [17] Greece [32] Portugal
[3] Andorra [18] Hungary [33] Romania
[4] Austria [19] Ireland [34] Russian Federatio
[5] Belarus [20] Italy [35] San Marino
[6] Belgium [21] Latvia [36] Serbia and Monten
[7] Bosnia and Herzego [22] Liechtenstein [37] Slovakia
[8] Bulgaria [23] Lithuania [38] Slovenia
[9] Croatia [24] Luxembourg [39] Spain
[10] Czech Republic [25] Macedonia (The Fo [40] Sweden
[11] Denmark [26] Malta [41] Switzerland
[12] Estonia [27] Moldova [42] Turkey

[13] Finland [28] Monaco [43] Ukraine
[14] France [29] Netherlands [44] United Kingdom
[15] Germany [30] Norway [45] Vatican City Stat
Выберите страну/регион (Отмена - <Enter>): 34
[1] Moscow-01 - Kaliningrad
[2] Moscow+00 - west Russia
[3] Moscow+01 - Caspian Sea
[4] Moscow+02 - Urals
[5] Moscow+03 - west Siberia
[6] Moscow+03 - Novosibirsk
[7] Moscow+04 - Yenisei River
[8] Moscow+05 - Lake Baikal
[9] Moscow+06 - Lena River
[10] Moscow+07 - Amur River
[11] Moscow+07 - Sakhalin Island
[12] Moscow+08 - Magadan
[13] Moscow+09 - Kamchatka
[14] Moscow+10 - Bering Sea
Выберите временную зону (Отмена - <Enter>): 6
FNPSH-I-3061-Часовой пояс изменен (NOVT)

Внимание!!! Настройка временной зоны не входит в конфигурацию при ее сохранении/применении.

Для просмотра настроек системного времени используется команда system time show:

fnpsh> system time show
Настройки системного времени:
Дата: 13.11.2006, понедельник
Время: 17:35:41
Временная зона: NOVT, GMT+0600
NTP: отключено
NTP сервер: отсутствует
Регистрация сообщений NTP:отключено
Тайм-аут опроса NTP: 3600
fnpsh>

Вывод данной команды подтверждает установку временной зоны, выполненную ранее.

4.6.4. Использование протокола NTP

Программное обеспечение ССПТ-2 поддерживает функцию синхронизации системного времени по протоколу NTP (Network Time Protocol). Для того, чтобы включить функцию синхронизации времени по протоколу NTP, необходимо обеспечить наличие и доступность через управляющий интерфейс ССПТ-2 NTP-сервера, а также проделать следующие действия:

1) установить IP-адрес NTP-сервера командой **system time ntp server**:

fnpsh> system time ntp server 193.13.18.5
FNPSH-I-305C-Адрес NTP сервера изменен
fnpsh>

2) включить использование NTP-сервера командой **system time ntp enable**:

fnpsh> system time ntp enable
FNPSH-I-3059-NTP включен
fnpsh>

После проделанных операций NTP-сервер будет опрашиваться периодически для синхронизации времени. Время опроса по умолчанию – 3600 секунд. Чтобы изменить тайм-аут опроса NTP-сервера, необходимо воспользоваться командой system time ntp timeout, задав новое значение тайм-аута в секундах:

fnpsh> system time ntp timeout 86400
FNPSH-I-3060-Тайм-аут NTP изменен
fnpsh>

Тайм-аут опроса NTP сервера может быть изменен в пределах от 600 секунд (10 минут) до 86400 секунд (1 сутки) включительно.

Возможна регистрация событий, возникающих при обращении к NTP-серверу (сообщения об ошибках или успешной синхронизации), в журнале системных событий (syslog). Для включения данной опции необходимо воспользоваться командой:

fnpsh> system time ntp log enable
FNPSH-I-305E-Регистрация NTP сообщений включена
fnpsh>

Для однократной синхронизация по протоколу NTP (без включения периодической синхронизации или с последней) предназначена команда system time ntp update, например:

fnpsh> system time ntp update 193.13.18.5
FNPSH-I-305D-Системное время изменено по NTP (поправка -55.672673 sec)
fnpsh>

В качестве аргумента данная команда принимает IP-адрес NTP-сервера. Для успешного выполнения данной команды необходимо наличие и доступность NTP-сервера с указанным адресом через управляющий интерфейс ССПТ-2.

4.7. Структура и редактирование правил фильтрации

4.7.1. Структура правил фильтрации

Фильтрация сетевого трафика может осуществляться на различных уровнях сетевого взаимодействия. Каждому из уровней соответствует отдельная группа (таблица) правил фильтрации. Правила фильтрации каждой группы задают параметры полей заголовков протоколов, соответствующих данному уровню фильтрации. Таким образом, в ССПТ-2 реализован пакетный фильтр, осуществляющий фильтрацию сетевого трафика на основании данных, содержащихся в заголовках протоколов.

В ССПТ-2 имеются следующие таблицы правил фильтрации:

1) **таблица MAC-правил** – правила фильтрации на уровне кадров Ethernet. Обрабатываются кадры формата Ethernet II, IEEE 802.3 raw, IEEE 802.2-LLC и IEEE 802.2-SNAP;

2) **таблица ARP-правил** – правила фильтрации для пакетов служебных протоколов ARP и RARP;

3) **таблица временных IP-правил** – правила фильтрации для протокола IP. Данные правила анализируют ограниченное число параметров заголовка сетевого и

транспортного уровней и действуют только на удаление пакета. Временные IP-правила не сохраняются на дисковом накопителе ССПТ-2 и теряются при перезагрузке;

4) **таблица IP-правил** – правила фильтрации для протокола IP. В IP-правилах фильтрации имеются дополнительные параметры для обработки транспортных протоколов TCP и UDP, и для служебного протокола ICMP;

5) **таблица IPX-правил** – правила фильтрации для протокола IPX;

6) **таблица прикладных правил (AP-правил)** – правила фильтрации на прикладном уровне.

Кроме таблиц правил фильтрации имеются дополнительные служебные таблицы:

1) **таблица интервалов времени** – временные интервалы необходимы для организации фильтрации в заданный промежуток времени;

2) **таблица групп VLAN-ов** – группы VLAN-ов (виртуальных локальных сетей, стандарт IEEE 802.1q) необходимы для организации различных политик безопасности для разных виртуальных сетей.

В таблицах **MAC-правил, ARP-правил, IP-правил и IPX-правил** фильтрации имеется **глобальное правило**. Глобальное правило применяется в том случае, если значения полей заголовков обрабатываемого в данный момент времени пакета не удовлетворяют ни одному из существующих правил данной таблицы.

Правила фильтрации могут быть **условными** и **безусловными**. Безусловные правила фильтрации работают всегда, т.е. в течение всего времени работы ССПТ-2. Условные правила фильтрации работают только в определенные промежутки времени. Эти промежутки времени носят название **интервалов времени**, которые задаются в **таблице интервалов времени**.

Таблица интервалов времени также хранится на дисковом накопителе ССПТ-2 и загружается в оперативную память при каждом старте устройства. Может быть определено **не более 1024** интервалов времени.

Глобальные правила фильтрации всегда являются безусловными.

Правила фильтрации, за исключением глобальных, могут быть **активными** или **неактивными**. Неактивные правила не используются при обработке поступающих пакетов.

Путь прохождения пакета через фильтрующие интерфейсы ССПТ-2 в правиле фильтрации определяется с помощью **масок интерфейсов**. Существует маска **входных** интерфейсов и маска **выходных** интерфейсов. Маской входных интерфейсов определяется набор фильтрующих интерфейсов ССПТ-2, с которых ожидается поступление пакета для данного правила фильтрации. Маской **выходных** интерфейсов определяется набор интерфейсов, на которые пакет должен быть передан, если данное правило было к этому пакету применено. В любом случае, пакет никогда не будет передан на фильтрующий интерфейс, с которого он был принят. Способ использования маски выходных интерфейсов варьируется в зависимости от того, какое действие задает применяемое правило фильтрации.

Правила фильтрации задают следующие действия, которые могут быть выполнены над сетевым пакетом:

1) **передача** – передача пакета на выходные интерфейсы, определенные в правиле фильтрации. При этом пакет передается только на те фильтрующие интерфейсы, которые определены в маске выходных интерфейсов данного правила;

2) **пропуск** – передача пакета на следующий уровень обработки, если таковой имеется. Для MAC-правил следующим уровнем обработки являются ARP-, IP- или IPX-правила. Для IP-правил следующим уровнем обработки являются прикладные (AP) правила. Если для данного правила фильтрации отсутствует следующий уровень (например, для ARP-правила), пакет передается на определенные в правиле фильтрации выходные интерфейсы;

3) **удаление** – запрет прохождения пакета. Принятый пакет не будет передан ни на один из фильтрующих интерфейсов ССПТ-2.

Поскольку фильтрация пакетов в ССПТ-2 является многоуровневой, маска выходных интерфейсов MAC-уровня учитывается при обработке пакета на следующих уровнях (ARP, IP или IPX). Это означает что, если к пакету применяется

сначала MAC-правило, предписывающее передачу на интерфейс **eth0**, а затем IP-правило, предписывающее передачу на интерфейс **eth1**, то результирующая маска выходных интерфейсов окажется пустой и данный пакет не будет передан ни на одни фильтрующий интерфейс. Другими словами, если к пакету применяется регулярное MAC-правило, то пакет может быть передан только на те фильтрующие интерфейсы, которые определены в маске выходных интерфейсов этого MAC-правила, даже если на следующем уровне к пакету будет применено правило, разрешающее передачу на какие-либо другие интерфейсы.

Внимание!!! В случае нулевой маски выходных интерфейсов передача пакета запрещается полностью, и в журнал регистрации событий будет занесено соответствующее предупреждающее сообщение с указанием комбинации правил фильтрации, применение которых дало в результате пустую маску выходных интерфейсов.

Правила фильтрации однозначно идентифицируются своим номером. Номер правила представляет собой целое число в диапазоне значений от **1** до **65535**. Не допускается существование нескольких правил фильтрации с одним и тем же номером в одной и той же группе. В каждой группе может быть определено **не более 1024** правил фильтрации включая глобальное правило.

Первоначально таблицы правил фильтрации пусты, а все глобальные правила предписывают удаление сетевых пакетов. Таким образом, после первого включения, ССПТ-2 не пропускает сетевые пакеты через фильтрующие интерфейсы.

Порядок обработки пакетов в ССПТ-2 зависит от режима фильтрации, в котором находится пакетный фильтр в данное время. Режимы фильтрации, а также обработка пакетов в этих режимах описана в разделе 10.

4.7.2. Редактирование правил в таблицах

Для правил фильтрации, интервалов времени и групп VLAN определены следующие операции редактирования:

- добавление: команда **rule add <определение_правила>**;

- редактирование: команда **rule edit <определение_правила>**;

- удаление: команда **rule delete <идентификатор_правила>**;

- сохранение правил в дополнительном наборе: команда **rule save <имя_набора>**;

- загрузка правил из дополнительного набора: команда **rule load <имя_набора>**;

- просмотр правил из текущего или дополнительного набора: команда **rule show <опции_просмотра> [<имя_набора>]**.

Для команд редактирования и добавления возможны два формата задания определения правила:

- в виде **<тип_правила>:<номер_правила>:<параметр1>:<параметр2>: ..:<параметрN>**;

- в виде **<тип_правила>:<номер_правила> <параметр1>=<значение> ... <параметрN>=<значение>**.

4.7.3. Группы VLAN

Группы VLAN предназначены для объединения нескольких идентификаторов VLAN (стандарт IEEE 802.1q) в группу для последующей привязки данной группы к одному из правил фильтрации. В этом случае данное правило фильтрации будет применяться только к пакетам, содержащим один из идентификаторов VLAN, указанных в группе, и, таким образом, работать только в обозначенных в группе VLAN виртуальных локальных сетях. Это необходимо для построения собственных политик безопасности для различных виртуальных локальных сетей.

Для добавления новой группы VLAN могут использоваться следующие команды:

1) **rule add vlan:<номер>:<идентификаторы>:<комментарии>**;

2) **rule add vlan:<номер> tags=<идентификаторы> [comments=<комментарии>]**, где:

- **<номер>** - номер группы VLAN, допустимые значения: 1-65535;

- **<идентификаторы>** - список идентификаторов (значений тэгов) VLAN, допустимые значения 0-4095;

- **<комментарии>** - комментарии к группе VLAN; длина строки комментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

Пример:

```
fnpsh> rule add vlan:10:12,14,16,20-30:"Группа производство"
FNPSH-I-3008-VLAN группа добавлена (10)
fnpsh>
fnpsh> rule add vlan:20 tags=35,45,48,50-70 comments="Группа продавцов"
FNPSH-I-3008-VLAN группа добавлена (20)
fnpsh>
fnpsh> rule show type=vlan
vlan:10:12,14,16,20-30:"Группа производство"
vlan:20:35,45,48,50-70:"Группа продавцов"
fnpsh>
fnpsh> rule show type=vlan mode=detail
VLAN группа 10 - "Группа производство":
VLAN идентификаторы: 12,14,16,20-30
VLAN группа 20 - "Группа продавцов":
VLAN идентификаторы: 35,45,48,50-70
fnpsh>
fnpsh> rule show mode=detail type=vlan
VLAN группа 10 - "Группа производство+сбыт":
VLAN идентификаторы: 12,20-30,32,34
VLAN группа 20 - "Группа продавцов":
VLAN идентификаторы: 100
fnpsh>
```

Обязательными при добавлении группы VLAN в формате "**vlan:<номер>:<идентификаторы>:<комментарии>**" являются параметры *<номер>* и **<идентификаторы>**.

При добавлении группы VLAN в формате "**vlan:<номер> tags=<идентификаторы> [comments=<комментарии>]**" обязательными параметрами являются параметры **<номер>** и **tags=<идентификаторы>**.

Для редактирования существующей группы VLAN могут использоваться следующие команды:

1) **rule edit vlan:<номер>:<идентификаторы>:<комментарии>**;

2) **rule edit vlan:<номер> [tags=<идентификаторы>] [comments=<комментарии>]**,

где параметры правила аналогичны команде **rule add vlan**.

Пример:

fnpsh> rule edit vlan:10:12,20-30,32,34:"Группа производство+сбыт"
Изменить группу VLAN? (Y/N) [N]: y
FNPSH-I-300F-VLAN группа изменена (10)
fnpsh>
fnpsh>rule edit vlan:20 tags=100
Изменить группу VLAN? (Y/N) [N]: y
FNPSH-I-300F-VLAN группа изменена (20)
fnpsh>

Для удаления существующей группы VLAN может использоваться следующая команда **rule delete vlan:<номер>**, где **<номер>** - номер существующей группы VLAN.

Пример:

fnpsh> rule delete vlan:10
Удалить группу VLAN? (Y/N) [N]: y
FNPSH-I-3016-VLAN группа удалена (10)
fnpsh>

4.7.4. Интервалы времени

Интервалы времени предназначены для организации фильтрации в заданный временной диапазон. Для этого созданный интервал времени привязывается к правилу фильтрации, после чего данное правило фильтрации действует только в указанный интервал времени.

Для добавления нового интервала времени могут использоваться следующие команды:

1) rule add time:<номер>:<месяцы>:<дни_месяца>:<дни_недели> :<время>:<комментарии>

2) rule add time:<номер> months=<месяцы> mdays=<дни_месяца> wdays=<дни_недели> time=<время> comments=<комментарии>,

где:

3) **<номер>** - номер интервала времени, допустимые значения: 1-65535;

4) **<месяцы>** - список месяцев, ожидаются следующие значения:

- **any** – любой месяц (по умолчанию);

- **jan,feb,mar,apr,may,jun,jul,aug,sep,oct,nov,dec** – одно или более разделенных запятыми имен месяцев в указанных сокращениях;

5) **<дни_месяца>** - список месяцев, ожидаются следующие значения:

- **any** – любой день месяца (по умолчанию);

- **<num>[-<num>][,<num>[-<num>]]:** список дней месяца, например: 5,7,9,12-20,29;

6) **<дни_недели>** - список дней недели, ожидаются следующие значения:

- **any** – любой день недели (по умолчанию);

- **mon,tue,wed,thu,fri,sat,sun** – один или более разделенных запятыми дней недели в указанных сокращениях;

7) **<время>** - список временных интервалов, ожидаются следующие значения:

- **any** – любое время (по умолчанию);

- **<ЧЧ.ММ.СС>-<ЧЧ.ММ.СС>[,<ЧЧ.ММ.СС>-<ЧЧ.ММ.СС>]** - список интервалов времени, например: 00.00.00-09.30.00,12.30.00-17.30.59,23.00.00-23.59.59

8) **<комментарии>** - комментарии к интервалу времени; длина строки комментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

Обязательным при добавлении интервала времени в формате "**time:<номер>:<параметр1>:<параметр2>:...**" является параметр **<номер>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию. Допускается

отсутствие одного или нескольких параметров в перечне (**<параметр5>:<параметр6>:::<параметр9>**). В этом случае будут использованы значения по умолчанию для пропущенных параметров.

При добавлении интервала времени в формате "**time:<номер> <параметр1>=<значение> ... <параметрN>=<значение>**" обязательным является параметр **<номер>**. Для неуказанных в определении правила параметров принимаются значения по умолчанию.

Пример:

fnpsh> rule add time:10:jan,feb,oct:1,2,10-20:any:00.00.00-09.30.00,12.30.00-17.30.59
FNPSH-I-300D-Интервал времени добавлен (10)
fnpsh>
fnpsh> rule add time:20 months=nov,dec wdays=mon,tue,wed,thu,fri time=08.30.00-17.30.00
FNPSH-I-300D-Интервал времени добавлен (20)
fnpsh>
fnpsh> rule show type=time
time:10:jan,feb,oct:1-2,10-20:any:00.00.00-09.30.00,12.30.00-17.30.59
time:20:nov,dec:any:mon,tue,wed,thu,fri:08.30.00-17.30.00
fnpsh>
fnpsh>
fnpsh> rule show type=time mode=detail
Интервал времени 10:
Месяцы: jan,feb,oct
Дни месяца: 1-2,10-20
Интервалы времени: 00.00.00-09.30.00,12.30.00-17.30.59
Интервал времени 20:
Месяцы: nov,dec
Дни недели: mon,tue,wed,thu,fri
Интервалы времени: 08.30.00-17.30.00
fnpsh>

Для редактирования существующего интервала времени могут использоваться следующие команды:

1) **rule edit time:<номер>:<месяцы>:<дни_месяца>:<дни_недели>: <время>:<комментарии>**;

2) **rule edit time:<номер> [months=<месяцы>] [mdays=<дни_месяца>] [wdays=<дни_недели>] [time=<время>] [comments=<комментарии>]**,

где параметры аналогичны команде **rule add time**.

Пример:

fnpsh> rule edit time:10 months=any mdays=any wdays=sat,sun comments="Уборка территории"
Изменить интервал времени? (Y/N) [N]: y
FNPSH-I-3014-Интервал времени изменен (10)
fnpsh>
fnpsh> rule edit time:20:any:10-24:mon,tue,wed,thu,fri:08.30.00-18.30.00:Работаем
Изменить интервал времени? (Y/N) [N]: y
FNPSH-I-3014-Интервал времени изменен (20)
fnpsh>
fnpsh> rule show type=time time:10:any:any:sat,sun:00.00.00-09.30.00,12.30.00-17.30.59:"Уборка территории"
time:20:any:10-24:mon,tue,wed,thu,fri:08.30.00-18.30.00:Работаем
fnpsh>
fnpsh> rule show type=time mode=detail
Интервал времени 10 - "Уборка территории":
Дни недели: sat,sun
Интервалы времени: 00.00.00-09.30.00,12.30.00-17.30.59
Интервал времени 20 - Работаем:
Дни месяца: 10-24
Дни недели: mon,tue,wed,thu,fri
Интервалы времени: 08.30.00-18.30.00
fnpsh>

Для удаления существующего интервала времени используется команда **rule delete time:<номер>**, где **<номер>** - номер существующего интервала времени.

Пример:

fnpsh> rule delete time:20
Удалить интервал времени? (Y/N) [N]: y
FNPSH-I-301B-Интервал времени удален (20)
fnpsh>

4.7.5. MAC-правила фильтрации

Для фильтрации параметров канального уровня предназначены MAC-правила фильтрации, содержащиеся в таблице MAC-правил. MAC-правила фильтрации позволяют фильтровать пакеты по следующим полям заголовка канального уровня (Ethernet):

- тип фрейма Ethernet;
- MAC-адреса отправителя и получателя;
- инкапсулированный протокол;
- идентификатор VLAN.

Для добавления нового регулярного MAC-правила могут использоваться следующие команды:

1) **rule add mac:<номер>:<действие>:<регистрация>:<вход>:[<выход>:] <интервал_времени>:<источник>:<приемник>:<активность>: <комментарии>:<фреймы>: <vlans>:<протоколы>:<сигнализация>]**

2) **rule add mac:<номер> action=<действие> in=<вход> [out=<выход>] [srcmac=<источник>][dstmac=<приемник>][frame=<фрейм>][protocol=<протоколы>][vlan=<vlans>][log=<регистрация>][alarm=<сигнализация>][time= <интервал_времени>][active=<активность>] [comments=<комментарии>]**,

где:

1) **<номер>** - номер MAC-правила, допустимые значения: 1-65535;

2) **<действие>** - действие правила. Ожидаются следующие значения:

- **accept** – передача пакета на следующий уровень обработки;
- **pass** – передача пакета на выходные интерфейсы;
- **drop** – удаление пакета;

3) **<вход>** - список входных интерфейсов. Ожидаются следующие ключевые слова:

- **<имя_интерфейса>[,<имя_интерфейса>]** – список символических имен интерфейсов;
- **<номер_интерфейса>[,<номер_интерфейса>]** – список номеров интерфей-

сов (нумерация начинается с нуля);

- **<маска_интерфейсов>:** битовая маска интерфейсов (например, 01001 означает интерфейсы 0 и 3, всего пять фильтрующих интерфейсов);

4) **<выход>** - список выходных интерфейсов. Ожидаются следующие ключевые слова:

- **<имя_интерфейса>[,<имя_интерфейса>]** – список символических имен интерфейсов;

- **<номер_интерфейса>[,<номер_интерфейса>]** – список номеров интерфейсов (нумерация начинается с нуля);

- **<маска_интерфейсов>:** битовая маска интерфейсов (например, 01001 означает интерфейсы 0 и 3, всего пять фильтрующих интерфейсов);

5) **<источник>** - список MAC-адресов источника. Ожидаются значения MAC-адресов в следующем формате:

- **any** – любой MAC-адрес источника (по умолчанию);

- **<MAC-адрес>[/<MAC-маска>][,<MAC-адрес>[/<MAC-маска>]]** - список MAC-адресов и (при необходимости) масок MAC-адресов, используемых для выделения необходимого количества значащих разрядов из MAC-адреса (например, 00e07590dae0,00e0fe7895cd/ffffffff0000,00ed8c3d7a44/24);

6) **<приемник>** - список MAC-адресов приемника. Ожидаются значения MAC-адресов в следующем формате:

- **any** – любой MAC-адрес приемника (по умолчанию);

- **<MAC-адрес>[/<MAC-маска>][,<MAC-адрес>[/<MAC-маска>]]** - список MAC-адресов и (при необходимости) масок MAC-адресов, используемых для выделения необходимого количества значащих разрядов из MAC-адреса (например, 00e07590dae0,00e0fe7895cd/ffffffff0000,00ed8c3d7a44/24);

7) **<фрейм>** - типы Ethernet-фреймов. Ожидаются следующие ключевые слова:

- **any** – любой фрейм Ethernet (по умолчанию);

- **eth2** - фрейм EthernetII;

- **llc** – фрейм IEEE-802.3 с заголовком IEEE-802.2/LLC;

- **snap** - фрейм IEEE-802.3 с заголовком IEEE-802.2/SNAP;

- **raw** - фрейм IEEE-802.3;

Возможно указание списком (например, **eth2,snap,raw**)

8) **<протоколы>** - список инкапсулированных протоколов. Ожидаются следующие ключевые слова, зависящие от типа фрейма Ethernet:

- **any** – любой инкапсулированный протокол (по умолчанию);

- **<num>[-<num>][,<num>[-<num>]]** - десятичные или шестнадцатеричные значения номера протокола для фреймов EthernetII и IEEE-802.3 с заголовком IEEE-802.2/LLC. Допустимые значения для фрейма EthernetII: 1519-65535 . Параметр <протоколы> для фрейма EthernetII сравнивается с полем «Тип протокола» заголовка EthernetII обрабатываемого пакета. Допустимые значения для фрейма IEEE-802.3 с заголовком IEEE-802.2/LLC: 0-255. Параметр <протоколы> для фрейма IEEE-802.3 с заголовком IEEE-802.2/LLC сравнивается с полем SSAP заголовка IEEE-802.2/LLC обрабатываемого пакета;

- **<OUI>/<num>[-<num>][,<num>[-<num>]]** - шестизначный шестнадцатеричный код производителя (<OUI>) и список номеров протоколов (в десятичном или шестнадцатеричном виде) для фрейма IEEE-802.3 с заголовком IEEE-802.2/SNAP. Допустимые значения для <OUI>: 000000-ffffff. Допустимые значения для номеров протоколов: 0-65535. Параметр <протоколы> для IEEE-802.3 с заголовком IEEE-802.2/SNAP сравнивается с полями «OUI» и «Тип протокола» заголовка IEEE-802.2/SNAP обрабатываемого пакета;

9) **<vlans>** - параметр использования VLAN. Ожидаются следующие ключевые слова:

- **any** – любой фрейм Ethernet (с тэгом IEEE 802.1q или без него - по умолчанию);

- **yes** или **vlan** – только фреймы Ethernet с тегом IEEE 802.1q;

- **no** или **novlan** – только фреймы Ethernet без тега IEEE 802.1q;

- **<группа_vlan>** - номер группы VLAN. Правило будет действовать только

для фреймов Ethernet, содержащих указанные в данной группе номера тэгов VLAN;

10) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **yes** или **pkt**, или **log**, или **logpkt** – регистрировать пакет, обработанный данным правилом;

- **no** или **nolog** – не регистрировать пакет, обработанный данным правилом (поумолчанию);

11) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного пакета;

12) **<интервал_времени>** - номер интервала времени, привязанного к данному правилу. Значение 0 означает безусловное, т.е. всегда активное правило (по умолчанию);

13) **<активность>** - активность данного правила. Ожидаются следующие ключевые слова:

- **yes** или **active** – правило активно (по умолчанию);

- **no** или **noactive** – правило неактивно;

14) **<комментарии>** - комментарии к MAC-правилу. Длина строки комментария до 31символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

Обязательными при добавлении MAC-правила в формате **"mac:<номер>:<параметр1>: <параметр2>:..."** являются параметры **<номер>**, **<действие>**, **<регистрация>**, **<вход>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию. Допускается отсутствие одного или нескольких параметров в перечне **(<параметр5>:<параметр6>:::<параметр9>**). В этом случае будут использованы значения по умолчанию для пропущенных параметров.

Обязательными при добавлении MAC-правила в формате "**mac:<номер> <параметр1>= <значение>...<параметрN>=<значение>**" являются параметры **<номер>**, **action=<действие>** и **in=<вход>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию. Для правила, предписывающего удаление пакета, значения выходных интерфейсов не учитывается.

Пример:

fnpsh> rule add mac:10:accept:nolog:1:0,2:0:00ed8c3d7a44/24,
00e07590dae0:00e0fe7895cd/32:active::eth2:any:0x4300,0x127e:noalarm
FNPSH-I-3009-MAC правило добавлено (10)
fnpsh>
fnpsh> rule add mac:20 action=drop in=eth2 srcmac=000c011345b5
dstmac=0c003418da4b,000c45bdc57a frame=snap protocol=0x001c4d/0x34,0x56
alarm=yes vlan=no
FNPSH-I-3009-MAC правило добавлено (20)
fnpsh>
fnpsh> rule show type=mac
mac:0:accept:nolog
mac:10:accept:nolog:1:0,2:0:00ed8c3d7a44/24,00e07590dae0:00e0fe7895cd/32:
active::eth2:any:0x4300,0x127e:noalarm
mac:20:drop:nolog:2:0,1:0:000c011345b5:0c003418da4b,000c45bdc57a:active
::snap:any:0x001c4d/0x34,0x56:alarm
fnpsh>
fnpsh> rule show type=mac mode=detail
MAC правило 0:
Действие: accept (передача на следующий уровень обработки)
Регистрация пакета: отключено
MAC правило 10:
Действие: accept (передача на следующий уровень обработки)
Входные интерфейсы: eth1
Выходные интерфейсы: eth0,eth2
MAC-адреса источника: 00ed8c3d7a44/24,00e07590dae0
MAC-адреса приемника: 00e0fe7895cd/32
Фреймы Ethernet: eth2
Инкапсулированные протоколы: 0x4300,0x127e
MAC правило 20:
Действие: drop (удаление)
Входные интерфейсы: eth2
MAC-адреса источника: 000c011345b5
MAC-адреса приемника: 0c003418da4b,000c45bdc57a
Фреймы Ethernet: snap

Инкапсулированные протоколы: 0x001c4d/0x34,0x56
Сигнализация: включено
fnpsh>

Для редактирования существующего MAC правила могут использоваться следующие команды:

1) **rule edit mac:<номер>:<действие>:<регистрация>:<вход>:[<выход>:<интервал_времени>:<источник>:<приемник>:<активность>:<комментарии>:<фреймы>:<vlans>:<протоколы>:<сигнализация>]**

2) **rule edit mac:<номер> [action=<действие>] [in=<вход>] [out=<выход>] [srcmac=<источник>][dstmac=<приемник>][frame=<фрейм>][protocol=<протоколы>] [vlan=<vlans>] [log=<регистрация>] [alarm=<сигнализация>] [time= <интервал_времени>] [active=<активность>] [comments=<комментарии>]**,

где **<номер>** - номер MAC-правила. Допустимые значения: 0-65535. Нулевое MAC-правило является глобальным MAC-правилом. Остальные параметры MAC-правила аналогичны параметрам команды rule add mac.

Для глобального MAC-правила определены только два параметра: **<действие>** и **<регистрация>**. Глобальное MAC-правило не может быть удалено.

Пример:

fnpsh> rule edit mac:10:pass:log:1:0:0:00e07590dae0:00e0fe7895cd/32
Изменить MAC правило? (Y/N) [N]: y
FNPSH-I-3010-MAC правило изменено (10)
fnpsh>
fnpsh> rule edit mac:20 in=eth1 vlan=no comments="Удаляем с eth1"
Изменить MAC правило? (Y/N) [N]: y
FNPSH-I-3010-MAC правило изменено (20)
fnpsh>
fnpsh> rule edit mac:0 log=yes
Изменить MAC правило? (Y/N) [N]: y
FNPSH-I-3010-MAC правило изменено (0)
fnpsh> rule show type=mac
mac:0:accept:logpkt
mac:10:pass:logpkt:1:0:0:00e07590dae0:00e0fe7895cd/32:active::any:any:any:noalarm
mac:20:drop:nolog:1::0:000c011345b5:0c003418da4b,000c45bdc57a:active:"Удаляем с eth1":snap:novlan:0x001c4d/0x34,0x56:alarm

fnpsh>
fnpsh> rule show type=mac mode=detail
MAC правило 0:
Действие: accept (передача на следующий уровень обработки)
Регистрация пакета: включено
MAC правило 10:
Действие: pass (передача на выходные интерфейсы)
Входные интерфейсы: eth1
Выходные интерфейсы: eth0
MAC-адреса источника: 00e07590dae0
MAC-адреса приемника: 00e0fe7895cd/32
Регистрация пакета: включено
MAC правило 20 - "Удаляем с eth1":
Действие: drop (удаление)
Входные интерфейсы: eth1
MAC-адреса источника: 000c011345b5
MAC-адреса приемника: 0c003418da4b,000c45bdc57a
Фреймы Ethernet: snap
Инкапсулированные протоколы: 0x001c4d/0x34,0x56
VLAN: нет (пакеты без тэга VLAN)
Сигнализация: включено
fnpsh>

Для удаления регулярного MAC-правила используется команда **rule delete mac:<номер>**, где **<номер>** - номер существующего MAC-правила;

Пример:

fnpsh> rule delete mac:10
Удалить MAC правило? (Y/N) [N]: y
FNPSH-I-3017-MAC правило удалено (10)
fnpsh>

4.7.6. ARP-правила фильтрации

Для фильтрации параметров протоколов ARP и RARP предназначены ARP-правила фильтрации, содержащиеся в таблице ARP-правил. ARP-правила фильтрации позволяют фильтровать пакеты по следующим полям заголовков ARP/RARP:

- MAC-адреса отправителя и получателя;

- IP-адреса отправителя и получателя;

- тип сообщения;

- идентификатор VLAN.

Для добавления нового регулярного ARP-правила могут использоваться следующие команды:

1) **rule add arp:<номер>:<действие>:<регистрация>:<вход>:[<выход>:**

<интервал_времени>:<mac_источник>:<ip_источник>:<mac_приемник>:<ip_приемник>:<arp_сообщение>:<активность>:<комментарии>:<vlans>:<сигнализация>]

2) **rule add arp:<номер> action=<действие> in=<вход> [out=<выход>] [srcmac=<mac_источник>] [srcip=<ip_источник>] [dstmac=<mac_приемник>]**

[dstip=<ip_приемник>] [type=<arp_сообщение>] [vlan=<vlans>] [log=<регистрация>] [alarm=<сигнализация>] [time=<интервал времени>] [active=<активность>] [comments=<комментарии>],

где:

1) **<номер>** - номер ARP-правила, допустимые значения: 1-65535;

2) **<действие>** - действие правила. Ожидаются следующие значения:

- **accept** или **pass** – передача пакета на выходные интерфейсы;

- **drop** – удаление пакета;

3) **<вход>** - список входных интерфейсов. Ожидаются следующие ключевые слова:

- **<имя_интерфейса>[,<имя_интерфейса>]** – список символических имен интерфейсов;

- **<номер_интерфейса>[,<номер_интерфейса>]** – список номеров интерфейсов (нумерация начинается с нуля);

- **<маска_интерфейсов>:** битовая маска интерфейсов (например, 01001 означает интерфейсы 0 и 3, всего пять фильтрующих интерфейсов)

4) **<выход>** - список выходных интерфейсов. Ожидаются следующие ключевые слова:

- **<имя_интерфейса>[,<имя_интерфейса>]** – список символических имен интерфейсов;

- **<номер_интерфейса>[,<номер_интерфейса>]** – список номеров интерфейсов (нумерация начинается с нуля);

- **<маска_интерфейсов>:** битовая маска интерфейсов (например, 01001 означает интерфейсы 0 и 3, всего пять фильтрующих интерфейсов);

5) **<mac_источник>** - список MAC-адресов источника ARP-пакета. Ожидаются значения MAC-адресов в следующем формате:

- **any** – любой MAC-адрес источника (по умолчанию);

- **<MAC-адрес>[/<MAC-маска>][,<MAC-адрес>[/<MAC-маска>]]** - список MAC- адресов и (при необходимости) масок MAC-адресов, используемых для выделения необходимого количества значащих разрядов из MAC-адреса (например, 00e07590dae0,00e0fe7895cd/ffffffff0000,00ed8c3d7a44/24);

6) **<ip_источник>** - список IP-адресов источника ARP-пакета. Ожидаются значения IP-адресов в следующем формате:

- **any** – любой IP-адрес источника (по умолчанию);

- **<IP-address>{[-<IP-address>]|[/netmask]}[,<IP-address>{[-<IP-address>]|[/netmask]}]** – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);

7) **<mac_приемник>** - список MAC-адресов приемника ARP-пакета. Ожидаются значения MAC-адресов в следующем формате:

- **any** – любой MAC-адрес приемника (по умолчанию);

- **<MAC-адрес>[/<MAC-маска>][,<MAC-адрес>[/<MAC-маска>]]** - список MAC- адресов и (при необходимости) масок MAC-адресов, используемых для выделения необходимого количества значащих разрядов из MAC-адреса (например, 00e07590dae0,00e0fe7895cd/ffffffff0000,00ed8c3d7a44/24);

8) **<ip_приемник>** - список IP-адресов приемника ARP-пакета. Ожидаются значения IP-адресов в следующем формате:

- **any** – любой IP-адрес приемника (по умолчанию);

- **<IP-address>{[-<IP-address>]|[/netmask]}[,<IP-address>{[-<IP-address>]|[/netmask]}]** – список IP-адресов (например, 192.168.10.1,192.168.10.10-

192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);

9) **<arp_сообщение>** - типы ARP-сообщения. Ожидаются следующие ключевые слова:

- **any** – любой тип ARP-сообщения (по умолчанию);

- **arp-request** - ARP-запрос;

- **arp-reply** – ARP-ответ;

- **rarp-request** - RARP-запрос;

- **rarp-reply** – RARP-ответ;

Возможно указание списком (например, **arp-request,arp-reply**)

10) **<vlans>** - параметр использования VLAN. Ожидаются следующие ключевые слова:

- **any** – любой фрейм Ethernet (с тэгом IEEE 802.1q или без него - по умолчанию);

- **yes** или **vlan** – только фреймы Ethernet с тегом IEEE 802.1q;

- **no** или **novlan** – только фреймы Ethernet без тега IEEE 802.1q;

- **<группа_vlan>** - номер группы VLAN. Правило будет действовать только для фреймов Ethernet, содержащих указанные в данной группе номера тэгов VLAN;

11) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **yes** или **pkt**, или **log**, или **logpkt** – регистрировать пакет, обработанный данным правилом;

- **no** или **nolog** – не регистрировать пакет, обработанный данным правилом (поумолчанию);

12) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного пакета;

13) **<интервал_времени>** - номер интервала времени, привязанного к дан-

ному правилу. Значение 0 означает безусловное, т.е. всегда активное правило (по умолчанию);

14) **<активность>** - активность данного правила. Ожидаются следующие ключевые слова:

- **yes** или **active** – правило активно (по умолчанию);

- **no** или **noactive** – правило неактивно;

15) **<комментарии>** - комментарии к данному ARP-правилу. Длина строки комментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

Обязательными при добавлении ARP-правила в формате "**arp:<номер>:<параметр1>: <параметр2>:...**" являются параметры **<номер>**, **<действие>**, **<регистрация>**, **<вход>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию. Допускается отсутствие одного или нескольких параметров в перечне **(<параметр5>:<параметр6>:::<параметр9>**). В этом случае будут использованы значения по умолчанию для пропущенных параметров.

Обязательными при добавлении ARP-правила в формате "**arp:<номер> <параметр1>= <значение>...<параметрN>=<значение>**" являются параметры **<номер>**, **action=<действие>** и **in=<вход>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию.

Для правила, предписывающего удаление пакета, значения выходных интерфейсов не учитывается.

Пример:

fnpsh> rule add arp:5:accept:log:0:1:0:00e07590dae0,00e0fe7895cd/ffffffff0000:192.168.10.2,192.168.10.16/255.255.255.248:ffffffffffff:192.168.10.254:arp-request::"Запрос к маршрутизатору"::noalarm
FNPSH-I-300A-ARP правило добавлено (5)
fnpsh>
fnpsh> rule add arp:15 action=drop log=pkt in=0 dstip=192.168.10.130 type=arp-reply comments=Запрет alarm=yes
FNPSH-I-300A-ARP правило добавлено (15)
fnpsh>

fnpsh> rule show type=arp
arp:0:pass:nolog
arp:5:accept:logpkt:0:1:0:00e07590dae0,00e0fe7895cd/32:192.168.10.2,192.168.10.16/29:ffffffffffff:192.168.10.254:arp-request:active:"Запрос маршрутизатору":any:noalarm
arp:15:drop:logpkt:0::0:any:any:any:192.168.10.130:arp-reply:active:Запрет:any:alarm
fnpsh>
fnpsh> rule show type=arp mode=detail
ARP правило 0:
Действие: pass (передача на выходные интерфейсы)
Регистрация пакета: отключено
ARP правило 5 - "Запрос маршрутизатору":
Действие: accept (передача на выходные интерфейсы)
Входные интерфейсы: eth0
Выходные интерфейсы: eth1
MAC-адреса источника: 00e07590dae0,00e0fe7895cd/32
IP-адреса источника: 192.168.10.2,192.168.10.16/29
MAC-адреса приемника: ffffffffffff
IP-адреса приемника: 192.168.10.254
ARP-сообщение: arp-request
Регистрация пакета: включено
ARP правило 15 - Запрет:
Действие: drop (удаление)
Входные интерфейсы: eth0
IP-адреса приемника: 192.168.10.130
ARP-сообщение: arp-reply
Регистрация пакета: включено; сигнализация: включено
fnpsh>

Для редактирования существующего ARP-правила могут использоваться следующие команды:

1) **rule edit arp:<номер>:<действие>:<регистрация>:<вход>:[<выход>:<интервал_времени>:<mac_источник>:<ip_источник>:<mac_приемник>:<ip_приемник>:<arp_сообщение>:<активность>:<комментарии>:<vlans>:<сигнализация>]**

2) **rule edit arp:<номер> [action=<действие>] [in=<вход>] [out=<выход>] [srcmac=<mac_источник>] [srcip=<ip_источник>] [dstmac=<mac_приемник>] [dstip=<ip_приемник>] [type=<arp_сообщение>] [vlan=<vlans>] [log= <pe-**

гистрация>] [alarm=<сигнализация>] [time=<интервал_времени>] [active=<активность>] [comments=<комментарии>],

где: **<номер>** - номер ARP-правила. Допустимые значения: 0-65535. Нулевое ARP-правило является глобальным ARP-правилом. Остальные параметры ARP-правила аналогичны параметрам команды **rule add arp**.

Для глобального ARP-правила определены только два параметра: **<действие>** и **<регистрация>**.

Пример:

fnpsh> rule edit arp:5:accept:nolog:0:1:0:00c0de16e933:any:any:any:arp-request,arp-reply:active::novlan:
Изменить ARP правило? (Y/N) [N]: y
FNPSH-I-3011-ARP правило изменено (5)
fnpsh>
fnpsh> rule edit arp:15 dstip=192.168.10.140 log=no alarm=no
Изменить ARP правило? (Y/N) [N]: y
FNPSH-I-3011-ARP правило изменено (15)
fnpsh>
fnpsh> rule show type=arp
arp:0:pass:nolog
arp:5:accept:nolog:0:1:0:00c0de16e933:any:any:any:arp-request,arp-reply:active::novlan:noalarm
arp:15:drop:nolog:0::0:any:any:any:192.168.10.140:arp-reply:active:Запрет:any:noalarm
fnpsh>
fnpsh> rule edit arp:0 log=yes
Изменить ARP правило? (Y/N) [N]: y
FNPSH-I-3011-ARP правило изменено (0)
fnpsh>
fnpsh> rule show type=arp mode=detail
ARP правило 0:
Действие: pass (передача на выходные интерфейсы)
Регистрация пакета: включено
ARP правило 5:
Действие: accept (передача на выходные интерфейсы)
Входные интерфейсы: eth0
Выходные интерфейсы: eth1
MAC-адреса источника: 00c0de16e933
ARP-сообщение: arp-request,arp-reply
VLAN: нет (пакеты без тэга VLAN)

ARP правило 15 - Запрет:
Действие: drop (удаление)
Входные интерфейсы: eth0
IP-адреса приемника: 192.168.10.140
ARP-сообщение: arp-reply
fnpsh>

Для удаления существующего ARP-правила используется команда **rule delete arp:<номер>**, где **<номер>** - номер существующего ARP-правила;

Пример:

fnpsh> rule delete arp:15
Удалить ARP правило? (Y/N) [N]: y
FNPSH-I-3018-ARP правило удалено (15)
fnpsh>

Глобальное ARP-правило не может быть удалено.

4.7.7. Временные IP-правила фильтрации

Временные IP-правила используются в основном для блокировки сетевых атак в реальном режиме времени, действую только на удаление и предназначены для фильтрации по основным полям заголовков IP, TCP и UDP:

- IP-адреса отправителя и получателя;
- протокол транспортного уровня;
- порты отправителя и получателя.

Для добавления нового временного IP-правила могут использоваться следующие команды:

1) **rule add iptmp:<номер>:<регистрация>:<вход>:<время_жизни>: <протокол>:<ip_источник>:<порт_источник>:<ip_приемник>: <порт_ приемник> [:<комментарии>:<сигнализация>]**

2) **rule add iptmp:<номер> in=<вход> srcip=<ip_источник> [srcport=<порт_источник>] [dstip=<ip_приемник>] [dstport=<порт_приемник>] [protocol=<протокол>] [log=<регистрация>] [alarm=<сигнализация>] [time=<время_жизни>] [comments=<комментарии>]**,

где:

1) **<номер>** - номер временного IP-правила. Допустимые значения: 1-65535;

2) **<вход>** - список входных интерфейсов. Ожидаются следующие ключевые слова:

- **<имя_интерфейса>[,<имя_интерфейса>]** – список символических имен интерфейсов;

- **<номер_интерфейса>[,<номер_интерфейса>]** – список номеров интерфейсов (нумерация начинается с нуля);

- **<маска_интерфейсов>:** битовая маска интерфейсов (например, 01001 означает интерфейсы 0 и 3, всего пять фильтрующих интерфейсов);

3) **<ip_источник>** - список IP-адресов источника пакета. Ожидаются значения IP-адресов в следующем формате:

- **any** – любой IP-адрес источника (по умолчанию);

- **<IP-address>{[-<IP-address>]|[/netmask]}[,<IP-address>{[-<IP-address>]|[/netmask]}]** – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);

4) **<порт_источник>** - список TCP- или UDP- портов источника. Ожидаются значения в следующем формате:

- **any** – любой порт источника (по умолчанию);

- **<num>[-<num>][,<num>[-<num>]]**- список портов источника (например, 22-25,110,80);

5) **<ip_приемник>** - список IP-адресов приемника пакета. Ожидаются значения IP-адресов в следующем формате:

- **any** – любой IP-адрес приемника (по умолчанию);

- <**IP-address>{[-<IP-address>]|[/netmask]}[,<IP-address>{[-<IP-address>]|[/netmask]}]** – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);

6) **<порт_приемника>** - список TCP- или UDP- портов приемника. Ожидаются значения в следующем формате:

- **any** – любой порт приемника (по умолчанию);

- **<num>[-<num>][,<num>[-<num>]]**- список портов приемника (например, 22-25,110,80);

7) **<протокол>** - проткол транспортного уровня. Ожидаются следующие ключевые слова:

- **any** – любой протокол (по умолчанию);

- **<name>[-<name>][,<name>[-<name>]]** - список имен протоколов (например, icmp,tcp- udp);

- **<num>[-<num>][,<num>[-<num>]]** - список номеров протоколов в десятичном виде (например, 1,10-13);

8) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **yes** или **pkt**, или **log**, или **logpkt** – регистрировать пакет, обработанный данным правилом;

- **no** или **nolog** – не регистрировать пакет, обработанный данным правилом (поумолчанию);

9) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного пакета;

10) **<время_жизни>** - время жизни данного правила в секундах. Допустимые значения: 60-31536000. Значение по умолчанию: 3600;

11) **<комментарии>** - комментарии к данному правилу. Длина строки комментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

Обязательными при добавлении временного IP-правила в формате "**iptmp:<номер>:<параметр1>:<параметр2>:...**" являются все параметры, кроме параметров **<комментарии>** и **<сигнализация>**. Допускается отсутствие одного

или нескольких параметров в перечне (**<параметр5>:<параметр6>::: <параметр9>**). В этом случае будут использованы значения по умолчанию для пропущенных параметров.

Обязательными при добавлении временного IP-правила в формате "**iptmp:<номер> <параметр1>=<значение> ... <параметрN>=<значение>**" являются параметры **<номер>**, **in=<вход>** и один из параметров **srcip=<ip_источник>**, **srcport=<порт_источник>**, **dstip=<ip_приемник>** или **dstport=<порт_приемник>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию.

Глобального правила в таблице временных IP-правил нет.

Пример:

fnpsh> rule add iptmp:10:log:eth0:7200:tcp:193.86.10.13:any:any:25:"Атака на smtp-сервер"
FNPSH-I-3055-Временное IP правило добавлено (10)
fnpsh>
fnpsh> rule add iptmp:20 in=eth1 dstip=192.168.18.34 dstport=53 protocol=udp alarm=yes
FNPSH-I-3055-Временное IP правило добавлено (20)
fnpsh>
fnpsh> rule show type=iptmp iptmp:10:logpkt:0:7200:tcp:193.86.10.13:any:any:25:"Атака на smtp-сервер":noalarm:iptmp:20:nolog:1:3600:udp:any:any:192.168.18.34:53::alarm
fnpsh>
fnpsh> rule show type=iptmp mode=detail
Временное IP правило 10 - "Атака на smtp-сервер":
Входные интерфейсы: eth0
Инкапсулированные протоколы: tcp
IP-адреса источника: 193.86.10.13
Порты приемника: 25
Время жизни: 6948 сек.
Регистрация пакета: включено
Временное IP правило 20:
Входные интерфейсы: eth1
Инкапсулированные протоколы: udp
IP-адреса приемника: 192.168.18.34
Порты приемника: 53
Время жизни: 3455 сек.
Сигнализация: включено

fnpsh>

При выводе временных IP-правил в детальном режиме в поле «Время жизни» показывается количество секунд до удаления данного правила из таблицы временных IP-правил.

Для редактирования существующего временного IP-правила могут использоваться следующие команды:

1) **rule edit iptmp:<номер>:<регистрация>:<вход>:<время_жизни>: <протокол>:<ip_истоник>:<порт_источник>:<ip_приемник>: <порт_приемник> [:<комментарии> :<сигнализация>]**

2) **rule edit iptmp:<номер> in=<вход> srcip=<ip_источник> [srcport=<порт_источник>] [dstip=<ip_приемник>] [dstport=<порт_ приемник>] [protocol=<протокол>] [log=<регистрация>] [alarm= <сигнализация>] [time=<время _жизни>] [comments=<комментарии>],**

где **<номер>** - номер существующего временного IP-правила.

Остальные параметры временного IP-правила аналогичны параметрам команды **rule add iptmp**.

Пример:

fnpsh> rule edit iptmp:10:nolog:0:86400:tcp:193.86.10.13:any:192.168.10.25:25:"Атака на smtp-сервер"
Изменить временное IP правило? (Y/N) [N]: y
FNPSH-I-3056-Временное IP правило изменено (10)
fnpsh>
fnpsh> rule edit iptmp:20 protocol=tcp,udp time=86400 comments="Продлеваем время правила"
Изменить временное IP правило? (Y/N) [N]: y
FNPSH-I-3056-Временное IP правило изменено (20)
fnpsh>
fnpsh> rule show type=iptmp
iptmp:10:nolog:0:86400:tcp:193.86.10.13:any:192.168.10.25:25:"Атака на smtp-сервер":noalarm
iptmp:20:nolog:1:86400:tcp,udp:any:any:192.168.18.34:53:"Продлеваем время правила":alarm
fnpsh>
fnpsh> rule show type=iptmp mode=detail
Временное IP правило 10 - "Атака на smtp-сервер":

Входные интерфейсы: eth0
Инкапсулированные протоколы: tcp
IP-адреса источника: 193.86.10.13
IP-адреса приемника: 192.168.10.25
Порты приемника: 25
Время жизни: 86174 сек.
Временное IP правило 20 - "Продлеваем время правила":
Входные интерфейсы: eth1
Инкапсулированные протоколы: tcp,udp
IP-адреса приемника: 192.168.18.34
Порты приемника: 53
Время жизни: 86376 сек.
Сигнализация: включено
fnpsh>

Для удаления существующего временного IP-правила используется следующая команда **rule delete iptmp:<номер>**, где **<номер>** - номер существующего временного IP-правила;

Пример:

fnpsh> rule delete iptmp:10
Удалить временное IP правило? (Y/N) [N]: y
FNPSH-I-3067-Временное IP правило удалено (10)
fnpsh>

4.7.8. IP-правила фильтрации

IP-правила предназначены для фильтрации пакетов по следующим полям заголовков протоколов IP, а также TCP, UDP и ICMP:

- протокол транспортного уровня;
- IP-адреса отправителя и получателя;
- порты отправителя и получателя (для протоколов TCP и UDP);
- тип и код сообщения (для протокола ICMP);
- поле «Старшинство» заголовка IP-пакета;
- флаги TOS заголовка IP-пакета;
- флаги фрагментации и смещения фрагмента заголовка IP-пакета;
- поле «Длина» заголовка IP-пакета;

- поле TTL заголовка IP-пакета;

- идентификатор VLAN.

Для добавления нового IP-правила могут использоваться следующие команды:

1) **rule add ip:<номер>:<действие>:<регистрация>:<вход>:[<выход>:<интервал_времени>:<протокол>:<ip_источник>:<порт_источник>:<ip_ приемник>:<порт_приемник>:<старшинство>:<флаги_TOS>: <фрагментация>:<длина>:<диапазон_ttl>:<тип_код_icmp>:<активность>:<комментарии>:<vlans>:<создание_сессии>:<тайм-аут_сессии>:<прикладные_правила>: <сигнализация>]**

где **<тип_код_icmp>:**

{any|<icmp_type>[/{any}|{<icmp_code_range>|<icmp_code>}[,{<icmp_code_range>|<icmp_code>}]…}

где **<icmp_code_range>:**

<начальное значение_код_icmp>-<конечное значение_код_icmp>

Описание:

- для любых значений кодов/типов ICMP указывается ключевое слово «any»;

- элементы списка кодов/типов ICMP разделяются символом «вертикальная черта» (|);

- элемент списка состоит из:

  - одиночного числового (десятичного) значения кода ICMP;

  - списка значений типов ICMP, разделенных символом запятой (,), или ключевого слова «any»;

  - элементом списка типов ICMP может быть:

    - одиночное числовое (десятичное) значение типа ICMP;

    - диапазон числовых (десятичных) значений типов ICMP;

Примеры:

- **any –** все, что угодно;

- **2/any –** ICMP тип 2 с любым кодом;

- **2/3,4|3/1-3,5 –** тип 2 с кодом 3 либо 4 или тип 3 с кодом с 1 по 3 либо 5.

2) **rule add ip:<номер> action=<действие> in=<вход> [out=<вход>] [srcip=<ip_источник>] [srcport=<порт_источник>] [dstip=<ip_приемник>] [dstport=<порт_приемник>] [protocol=<протокол>] [icmp=<тип_код_icmp>]**

[preced=<старшинство>] [tos=<флаги_TOS>] [frag=<фрагментация>][len =<длина>] [ttl=<диапазон_ttl>] [vlan=<vlans>] [time=<интервал_времени>] [session= <создание_сессии>] [timeout=<тайм-аут_сессии>][apr=<прикладные_ правила>] [alarm=<сигнализация>] [active=<активность>] [log=<регистрация>] [comments =<комментарии>],

где:

1) **<номер>** - номер IP-правила. Допустимые значения: 1-65535;

2) **<действие>** - действие правила. Ожидаются следующие значения:

- **accept** – передача пакета на следующий уровень обработки;

- **pass** – передача пакета на выходные интерфейсы;

- **drop** – удаление пакета;

3) **<вход>** - список входных интерфейсов. Ожидаются следующие ключевые слова:

- **<имя_интерфейса>[,<имя_интерфейса>]** – список символических имен интерфейсов;

- **<номер_интерфейса>[,<номер_интерфейса>]** – список номеров интерфейсов (нумерация начинается с нуля);

- **<маска_интерфейсов>:** битовая маска интерфейсов (например, 01001 означает интерфейсы 0 и 3, всего пять фильтрующих интерфейсов);

4) **<выход>** - список выходных интерфейсов. Ожидаются следующие ключевые слова:

- **<имя_интерфейса>[,<имя_интерфейса>]** – список символических имен интерфейсов;

- **<номер_интерфейса>[,<номер_интерфейса>]** – список номеров интерфейсов (нумерация начинается с нуля);

- **<маска_интерфейсов>:** битовая маска интерфейсов (например, 01001 означает интерфейсы 0 и 3, всего пять фильтрующих интерфейсов);

5) **<ip_источник>** - список IP-адресов источника пакета. Ожидаются значения IP-адресов в следующем формате:

- **any** – любой IP-адрес источника (по умолчанию);

- **<IP-address>{[-<IP-address>]|[/netmask]}[,<IP-address>{[-<IP-address>]|[/netmask]}]** – список IP-адресов. В зависимости от типа перечисления можно вбить разное количество записей:

- перечисление IP-адресов через запятую – 16 записей (пример: 192.168.1.1, 192.168.2.2 и т.д.);
- перечисление IP-адресов с заменой одного IP-адреса на диапазон – 15 записей (пример: 192.168.1.1, 192.168.2.2-192.168.2.10, 192.168.3.1 и т.д.);
- перечисление диапазонов IP-адресов – 8 записей (пример: 192.168.1.1-192.168.1.10, 192.168.2.1-192.168.2.15 и т.д.);

6) **<порт_источник>** - список TCP- или UDP- портов источника. Ожидаются значения в следующем формате:

- **any** – любой порт источника (по умолчанию);

- **<num>[-<num>][,<num>[-<num>]]**- список портов источника (например, 22-25,110,80);

7) **<ip_приемник>** - список IP-адресов приемника пакета. Ожидаются значенияIP-адресов в следующем формате:

- **any** – любой IP-адрес приемника (по умолчанию);

- **<IP-address>{[-<IP-address>]|[/netmask]}[,<IP-address>{[-<IP-address>]|[/netmask]}]** – список IP-адресов В зависимости от типа перечисления можно вбить разное количество записей:

- перечисление IP-адресов через запятую – 16 записей (пример: 192.168.1.1, 192.168.2.2 и т.д.);
- перечисление IP-адресов с заменой одного IP-адреса на диапазон – 15 записей (пример: 192.168.1.1, 192.168.2.2-192.168.2.10, 192.168.3.1 и т.д.);

- перечисление диапазонов IP-адресов – 8 записей (пример: 192.168.1.1-192.168.1.10, 192.168.2.1-192.168.2.15 и т.д.);

8) **<порт_приемник>** - список TCP- или UDP- портов приемника. Ожидаются значения в следующем формате:

- **any** – любой порт приемника (по умолчанию);

- **<num>[-<num>][,<num>[-<num>]]**- список портов приемника (например, 22-25,110,80)

9) **<протокол>** - проткол транспортного уровня. Ожидаются следующие ключевые слова:

- **any** – любой протокол (по умолчанию);

- **<name>[-<name>][,<name>[-<name>]]** - список имен протоколов (например, icmp,tcp- udp);

- **<num>[-<num>][,<num>[-<num>]]** - список номеров протоколов в десятичном виде (например, 1,10-13);

10) **<тип_код_icmp>** - тип и код ICMP-сообщения. Ожидаются следующие ключевые слова:

- **any** - любой тип и код ICMP-сообщения (по умолчанию);

- **<icmp_type_code>[|<icmp_type_code>]…**:

где **<icmp_type_code>: {any|<icmp_type>[/{any}|{<icmp_code_range>|<icmp_code>}[,{<icmp_code_range>|<icmp_code>}]…}** – список типов и кодов ICMP-сообщения (например: any, 2/any, 2/3,4|3/1-3,5));

11) **<старшинство>** - значение подполя «Старшинство» поля TOS заголовка IP-пакета. Ожидаются следующие ключевые слова:

- **any** - любое значение подполя «Старшинство» (по умолчанию);

- **netctrl: network control**, значение подполя: 111;

- **inctrl: internetwork control**, значение подполя: 110;

- **critic: CRITIC/ECP**, значение подполя: 101;

- **flasho: flash override**, значение подполя: 100;

- **flash: flash**, значение подполя: 011;

- **immed: immediatly**, значение подполя: 010;

- **prior: priority**, значение подполя: 001;

- **rout: routine**, значение подполя: 000.Возможно указание списком (например: **immed,prior,rout**);

12) **<флаги_TOS>** - значение битов TOS поля TOS заголовка IP-пакета. Ожидаются следующие ключевые слова:

- **any** -любое значение битов TOS (по умолчанию);

- **delay_set или delay_clr или delay_any** - бит delay соответственно установлен, сброшен или в любом состоянии;

- **throu_set** или **throu_clr** или **throu_any** - бит throughput соответственно установлен, сброшен или в любом состоянии;

- **relia_set** или **relia_clr** или **relia_any** - бит reliability соответственно установлен, сброшен или в любом состоянии;

- **cost_set** или **cost_clr** или **cost_any** - бит cost соответственно установлен, сброшен или в любом состоянии;

- **ecn_notect** или **ecn_ect** или **ecn_ce** или **ecn_ectce** или **ecn_any** - подполе ECN имеет значение 00 (notect), 01 или 10 (ect), 11 (ce), 01 or 10 or 11 (ectce), любое соответственно;

13) **<фрагментация>** - использование фрагментации принятым пакетом. Ожидаются следующие ключевые слова:

- **any** - правило применяется как к фрагментированным, так и к нефрагментированным пакетам (по умолчанию);

- **yes** или **frag_only** - правило применяется только к фрагментированным пакетам;

- **no** или **frag_not** - правило применяется только к нефрагментированным пакетам;

14) **<длина>** - максимальная допустимая длина IP-пакета. Ожидаются следующие ключевые слова или значения:

- **any** - любая длина IP-пакета (по умолчанию);

- **<num>** - значение максимальной допустимой длины IP-пакета в байтах. Допустимые значения: 0-65535;

15) **<диапазон_ttl>** - допустимый диапазон значений поля TTL заголовка IP-пакета. Ожидаются следующие ключевые слова или значения:

- **any** - любое значение поля TTL (по умолчанию);

- **<num>-<num>** - диапазон допустимых значений поля TTL. Допустимые значения: 0-255;

16) **<vlans>** - параметр использования VLAN. Ожидаются следующие ключевые слова:

- **any** – любой фрейм Ethernet (с тэгом IEEE 802.1q или без него - по умолчанию);

- **yes** или **vlan** – только фреймы Ethernet с тегом IEEE 802.1q;

- **no** или **novlan** – только фреймы Ethernet без тега IEEE 802.1q;

- **<группа_vlan>** - номер группы VLAN. Правило будет действовать только для фреймов Ethernet, содержащих указанные в данной группе номера тэгов VLAN;

17) **<интервал_времени>** - номер интервала времени, привязанного к данному правилу. Значение 0 означает безусловное, т.е. всегда активное правило (по умолчанию).

18) **<создание_сессии>** - параметр создания сессии на основе пакетов, обработанных данным правилом. Ожидаются следующие ключевые слова:

- **default** или **defses** - использовать параметр «Создание сессий для IP-правил по умолчанию» (команда "session ip") (по умолчанию);

- **yes** или **ses** - создавать сессии по пакетам, обработанным данным правилом;

- **no** или **noses** - не создавать сессии по пакетам, обработанным данным правилом;

19) **<тайм-аут_сессии>** - тайм-аут неактивности для сессий, созданных по пакетам,обработанным данным правилом(для состояния ESTABLISHED). Ожидаются следующие ключевые слова или значения:

- **default** или **deftout** - использовать значения по умолчанию для тайм-аутов

сессий (команда "session timeout") (по умолчанию);

- **<num>** - значение тайм-аута в секундах. Значение 0 (ноль) означает бесконечный тайм-аут, т.е. такая сессия может быть удалена только после ее корректного завершения;

20) **<прикладные_правила>** - список прикладных правил, привязанных к данному IP-правилу. Все пакеты в сессиях, созданных по данному IP-правилу, будут обрабатываться прикладными правилами из данного списка. Ожидаются следующие ключевые слова или значения:

- **no** или **noapr** - пакеты не будут обрабатываться на прикладном уровне (по умолчанию);

- **<num>[-<num>][,<num>[-<num>]]** - список прикладных правил. Данные правила должны быть уже определены в таблице прикладных правил (например: 10,20,30-50,80);

21) **<активность>** - активность данного правила. Ожидаются следующие ключевые слова:

- **yes** или **active** – правило активно (по умолчанию);

- **no** или **noactive** – правило неактивно;

22) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **nolog** – не регистрировать пакет и сессии, обработанные по данному правилу (по умолчанию);

- **yes** или **log**, или **logpkt, logses** – регистрировать пакеты и сессии, обработанные по данному правилу;

- **pkt** или **logpkt** – регистрировать пакеты, обработанные по данному правилу;

- **ses** или **logses** – регистрировать сессии, обработанные по данному правилу;

23) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом.Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного

пакета;

24) **<комментарии>** - комментарии к данному правилу. Длина строки комментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

Обязательными при добавлении IP-правила в формате "**ip:<номер>:<параметр1>: <параметр2>:...**" являются параметры **<номер>**, **<действие>**, **<регистрация>**, **<вход>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию. Допускается отсутствие одного или нескольких параметров в перечне (**<параметр5>:<параметр6>::: <параметр9>**). В этом случае будут использованы значения по умолчанию для пропущенных параметров.

Обязательными при добавлении IP-правила в формате "**ip:<номер> <параметр1>= <значение>...<параметрN>=<значение>**" являются параметры **<номер>**, **action=<действие>** и **in=<вход>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию.

Для правила, предписывающего удаление пакета, значения выходных интерфейсов не учитывается.

Пример:

fnpsh> rule add ip:20:accept:log:0:1:0:icmp:194.85.19.3,194.85.19.5:any:any:any:any:any:::0/0,8/0:active:"ICMP ping":any:ses:deftout:noapr
FNPSH-I-300B-IP правило добавлено (20)
fnpsh>
fnpsh> rule add ip:30 action=drop in=eth2 protocol=tcp,udp srcip=193.18.234.0/24,193.18.224.128/27 ttl=0-30 timeout=15
FNPSH-I-300B-IP правило добавлено (30)
fnpsh>
fnpsh> rule show type=ip
ip:0:accept:nolog
ip:20:accept:logpkt,logses:0:1:0:icmp:194.85.19.3,194.85.19.5:any:any:any:any:any:any:any:any:0/0,8/0:active:"ICMP ping":any:ses:deftout:noapr:noalarm
ip:30:drop:nolog:2::0:tcp,udp:193.18.234.0/24,193.18.224.128/27:any:any:any:any:any:any:any:0-30:any:active::any:defses:15:noapr:noalarm
fnpsh>
fnpsh> rule show type=ip mode=detail

IP правило 0:
Действие: accept (передача на следующий уровень обработки)
Регистрация пакетов: отключено; регистрация сессий: отключено
IP правило 20 - "ICMP ping":
Действие: accept (передача на следующий уровень обработки)
Входные интерфейсы: eth0
Выходные интерфейсы: eth1
Инкапсулированные протоколы: icmp
IP-адреса источника: 194.85.19.3,194.85.19.5
ICMP тип/код: 0/0,8/0
Сессии: создаются; тайм-аут неактивности: по умолчанию
Регистрация пакета: включено; регистрация сессий: включено
IP правило 30:
Действие: drop (удаление)
Входные интерфейсы: eth2
Инкапсулированные протоколы: tcp,udp
IP-адреса источника: 193.18.234.0/24,193.18.224.128/27
Значения TTL: 0-30
Сессии: создаются по умолчанию; тайм-аут неактивности: 15 сек.
fnpsh>

Для редактирования существующего IP-правила могут использоваться следующие команды:

1) **rule edit ip:<номер>:<действие>:<регистрация>:<вход>:[<выход>:<интервал_времени>:<протокол>:<ip_источник>:<порт_источник>:<ip_ приемник>:<порт_приемник>:<старшинство>:<флаги_TOS>:<фрагментация>:<длина>:<диапазон_ttl>:<тип_код_icmp>:<активность>:<комментарии>:<vlans>: <создание_сессии>: <тайм-аут_сессии>:<прикладные_правила>: <сигнализация>]**

2) **rule edit ip:<номер> [action=<действие>] [in=<вход>] [out=<вход>] [srcip=<ip_источник>] [srcport=<порт_источник>] [dstip=<ip_приемник>] [dstport=<порт_приемник>] [protocol=<протокол>] [icmp=<тип_код_icmp>] [preced=<старшинство>] [tos=<флаги_TOS>] [frag=<фрагментация>] [len=<длина>] [ttl=<диапазон_ttl>] [vlan=<vlans>] [time=<интервал_времени>] [session=<создание_сессии>] [timeout=<тайм-аут_сессии>] [apr=<прикладные_правила>] [alarm=<сигнализация>] [active=<активность>] [log= <регистра-**

ция>] [comments=<комментарии>], где **<номер>** - номер существующего IP-правила. Остальные параметры IP-правила аналогичны параметрам команды **rule edit ip**.

Пример:

fnpsh> rule edit ip:20:accept:logpkt:0:1:0:tcp,udp:194.85.19.3,194.85.19.5:any:any:any:any:any:any:any:any:active::any:noses:deftout:noapr:alarm
Изменить IP правило? (Y/N) [N]: y
FNPSH-I-3012-IP правило изменено (20)
fnpsh>
fnpsh> rule edit ip:30 action=pass ttl=any dstport=23
Изменить IP правило? (Y/N) [N]: y
FNPSH-I-3012-IP правило изменено (30)
fnpsh>
fnpsh> rule edit ip:0 action=drop log=pkt
Изменить IP правило? (Y/N) [N]: y
FNPSH-I-3012-IP правило изменено (0)
fnpsh>
fnpsh> rule show type=ip
ip:0:drop:logpkt
ip:20:accept:logpkt:0:1:0:tcp,udp:194.85.19.3,194.85.19.5:any:any:any:any:any:any:any:any:active::any:noses:deftout:noapr:alarm
ip:30:pass:nolog:2:0,1:0:tcp,udp:193.18.234.0/24,193.18.224.128/27:any:any:23:any:any:any:any:any:any:active::any:defses:15:noapr:noalarm
fnpsh>
fnpsh> rule show type=ip mode=detail
IP правило 0:
Действие: drop (удаление)
Регистрация пакетов: включено; регистрация сессий: отключено
IP правило 20:
Действие: accept (передача на следующий уровень обработки)
Входные интерфейсы: eth0
Выходные интерфейсы: eth1
Инкапсулированные протоколы: tcp,udp
IP-адреса источника: 194.85.19.3,194.85.19.5
Сессии: не создаются; тайм-аут неактивности: по умолчанию
Регистрация пакета: включено; сигнализация: включено
IP правило 30:
Действие: pass (передача на выходные интерфейсы)
Входные интерфейсы: eth2
Выходные интерфейсы: eth0,eth1
Инкапсулированные протоколы: tcp,udp

IP-адреса источника: 193.18.234.0/24,193.18.224.128/27
Порты приемника: 23
Сессии: создаются по умолчанию; тайм-аут неактивности: 15 сек.
fnpsh>

Для удаления существующего IP-правила используется команда **rule delete ip:<номер>**, где **<номер>** - номер существующего IP-правила;

Пример:

fnpsh> rule delete ip:20
Удалить IP правило? (Y/N) [N]: y
FNPSH-I-3019-IP правило удалено (20)
fnpsh>
Глобальное IP-правило не может быть удалено.

4.7.9. IPX-правила фильтрации

IPX-правила предназначены для фильтрации пакетов по следующим полям заголовка протокола IPX:

- адреса сети отправителя и получателя;
- адреса хостов отправителя и получателя;
- сокеты отправителя и получателя;
- тип пакета;
- идентификатор VLAN.

Для добавления нового IPX-правила могут использоваться следующие команды:

1) **rule add ipx:<номер>:<действие>:<регистрация>:<вход>:[<выход>:<интервал_времени>:<сети_источника>/<хосты_источника>:<сокеты_источника>:<сети_приемника>/<хосты_приемника>:<сокеты_ приемника>:<тип_пакета>:<активность>:<комментарии>:<vlans>:<сигнализация>]**

2) **rule add ipx:<номер> action=<действие> in=<вход> [out=<вход>] [srcnet=<сети_источника>] [srchost=<хосты_источника>] [srcsock=<сокеты_источника>] [dstnet=<сети_приемника>][dsthost=<хосты_приемника>] [dstsock=<сокеты_приемника>][packet=<тип_пакета>] [vlan=<vlans>] [time=<интервал_времени>] [alarm=<сигнализация>] [active=<активность>][log=**

<регистрация>] [comments=<комментарии>],

где:

1) **<номер>** - номер IPX-правила. Допустимые значения: 1-65535;

2) **<действие>** - действие правила. Ожидаются следующие значения:

- **accept** или **pass**– передача пакета на выходные интерфейсы;

- **drop** – удаление пакета;

3) **<вход>** - список входных интерфейсов. Ожидаются следующие ключевые слова:

- **<имя_интерфейса>[,<имя_интерфейса>]** – список символических имен интерфейсов;

- **<номер_интерфейса>[,<номер_интерфейса>]** – список номеров интерфейсов (нумерация начинается с нуля);

- **<маска_интерфейсов>** - битовая маска интерфейсов (например, 01001 означает интерфейсы 0 и 3, всего пять фильтрующих интерфейсов);

4) **<выход>** - список выходных интерфейсов. Ожидаются следующие ключевые слова:

- **<имя_интерфейса>[,<имя_интерфейса>]** – список символических имен интерфейсов;

- **<номер_интерфейса>[,<номер_интерфейса>]** – список номеров интерфейсов (нумерация начинается с нуля);

- **<маска_интерфейсов>** - битовая маска интерфейсов (например, 01001 означает интерфейсы 0 и 3, всего пять фильтрующих интерфейсов);

5) **<сети_источника>** - диапазон сетей - источников пакета. Ожидаются значения сетей в следующем формате:

- **any** – любой адрес сети источника (по умолчанию);

- <**net**>**[-<net>]** - одиночное значение или диапазон IPX-сетей источника в шестнадцатеричном виде (например: (0f00abcd-a150b250);

6) **<хосты_источника>** - список хостов - источников пакета. Ожидаются значения хостов в следующем формате:

- **any** – любой адрес хоста источника (по умолчанию);

- **<host>[,<host>]** - список хостов – источников пакета в шестнадцатеричном виде (например: 00b0459db456,00b0458acce);

7) **<сокеты_источника>** - список сокетов источника. Ожидаются следующие ключевые слова и значения:

- **any** – любой сокет источника (по умолчанию);

- **ncp** - Netware NCP Core Protocol;

- **sap** - Netware SAP Service Advertising;

- **rip** - Netware RIP Routing Information;

- **netbios** - Netware Netbios;

- **diag** - Netware Diagnostics;

- **ser: <num>** - шестнадцатеричное значение номера сокета. Допускается указание списка сокетов (например, rip,diag,0x4590);

8) **<сети_приемника>** - диапазон сетей - приемников пакета. Ожидаются значения сетей в следующем формате:

- **any** – любой адрес сети приемника (по умолчанию);

- **<net>[-<net>]** - одиночное значение или диапазон IPX-сетей приемника в шестнадцатеричном виде (например: (0150b250-0f00abcd);

9) **<хосты_приемника>** - список хостов – приемников пакета. Ожидаются значения хостов в следующем формате:

- **any** – любой адрес хоста приемника (по умолчанию);

- **<host>[,<host>]** - список хостов – приемников пакета в шестнадцатеричном виде (например: 00b0459db456,00b0458acce);

10) **<сокеты_приемника>** - список сокетов примника. Ожидаются следующие ключевые слова и значения:

- **any** – любой сокет приемника (по умолчанию);

- **ncp** - Netware NCP Core Protocol;

- **sap** - Netware SAP Service Advertising;

- **rip** - Netware RIP Routing Information;

- **netbios** - Netware Netbios;

- **diag** - Netware Diagnostics;

- **ser:<num>** - шестнадцатеричное значение номера сокета. Допускается указание списка сокетов (например, rip,diag,0x4590);

11) **<тип_пакета>** - тип IPX-пакета. Ожидаются следующие ключевые слова:

- **any** – любой тип IPX-пакета (по умолчанию);

- **hello** – пакет Hello;

- **rip** – пакет протокола RIP (Routing Information Protocol);

- **echo** – пакет Echo;

- **error** - пакет Error;

- **sap** – пакет NetWare 386 или SAP;

- **spp** – пакет протокола SPP (Sequenced Packet Protocol);

- **netware** - пакет NetWare 286;

- **<num>** - шестнадцатеричное значение номера протокола. Допускается указание списка протоколов (например: **hello,error,1d18**);

12) **<vlans>** - параметр использования VLAN. Ожидаются следующие ключевые слова:

- **any** – любой фрейм Ethernet (с тэгом IEEE 802.1q или без него - по умолчанию);

- **yes** или **vlan** – только фреймы Ethernet с тегом IEEE 802.1q;

- **no** или **novlan** – только фреймы Ethernet без тега IEEE 802.1q;

- **<группа_vlan>** - номер группы VLAN. Правило будет действовать только для фреймов Ethernet, содержащих указанные в данной группе номера тэгов VLAN;

13) **<интервал_времени>** - номер интервала времени, привязанного к данному правилу. Значение 0 означает безусловное, т.е. всегда активное правило (по умолчанию);

14) **<активность>** - активность данного правила. Ожидаются следующие ключевые слова:

- **yes** или **active** – правило активно (по умолчанию);

- **no** или **noactive** – правило неактивно;

15) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **yes** или **pkt**, или **log**, или **logpkt** – регистрировать пакет, обработанный данным правилом;

- **no** или **nolog** – не регистрировать пакет, обработанный данным правилом (поумолчанию);

16) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного пакета;

17) **<комментарии>** - комментарии к данному правилу. Длина строки комментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

Обязательными при добавлении IPX-правила в формате "**ipx:<номер>:<параметр1>: <параметр2>:...**" являются параметры **<номер>**, **<действие>**, **<регистрация>**, **<вход>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию. Допускается отсутствие одного или нескольких параметров в перечне (**<параметр5>:<параметр6>::: <параметр9>**). В этом случае будут использованы значения по умолчанию для пропущенных параметров.

Обязательными при добавлении IPX-правила в формате "**ipx:<номер> <параметр1>= <значение>...<параметрN>=<значение>**" являются параметры **<номер>**, **action=<действие>** и **in=<вход>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию.

Для правила, предписывающего удаление пакета, значения выходных интерфейсов не учитываются.

Пример:

fnpsh> rule add ipx:20:accept:log:eth1:eth0:0:0x1010-0x1020/000d0e135fee,000d0 e48d1d2:ncp,sap:0x1030/any:any:hello,rip::Пропустить:novlan:
FNPSH-I-300C-IPX правило добавлено (20)
fnpsh>
fnpsh> rule add ipx:30 action=drop in=eth2 dstnet=1f00 dsthost=0d0e1478ff11,0d0e14acbb17 vlan=yes log=yes alarm=yes
FNPSH-I-300C-IPX правило добавлено (30)
fnpsh>
fnpsh> rule show type=ipx
ipx:0:accept:nolog
ipx:20:accept:logpkt:1:0:0:1010-1020/000d0e135fee,000d0e48d1d2:ncp,sap:1030/any:any:hello,rip:active:Пропустить:novlan:noalarm
ipx:30:drop:logpkt:2::0:any:any:1f00/0d0e1478ff11,0d0e14acbb17:any:any:active::vlan:alarm
fnpsh>
fnpsh> rule show type=ipx mode=detail
IPX правило 0:
Действие: accept (передача на выходные интерфейсы)
Регистрация пакета: отключено
IPX правило 20 - Пропустить:
Действие: accept (передача на выходные интерфейсы)
Входные интерфейсы: eth1
Выходные интерфейсы: eth0
Сети/хосты источника: 1010-1020/000d0e135fee,000d0e48d1d2
Сокеты источника: ncp,sap
Сети/хосты приемника: 1030/any
Тип пакета: hello,rip
VLAN: нет (пакеты без тэга VLAN)
Регистрация пакета: включено
IPX правило 30:
Действие: drop (удаление)
Входные интерфейсы: eth2
Сети/хосты приемника: 1f00/0d0e1478ff11,0d0e14acbb17
VLAN: да (пакеты с тэгом VLAN)
Регистрация пакета: включено; сигнализация: включено
fnpsh>

Для редактирования существующего IPX-правила могут использоваться следующие команды:

1) **rule edit ipx:<номер>:<действие>:<регистрация>:<вход>:[<выход>:<интервал_времени>:<сети_источника>/<хосты_источника>:<сокеты_ источника>:<сети_приемника>/<хосты_приемника>:<сокеты_приемника>:<тип_пакета>:<активность>:<комментарии>:<vlans>:<сигнализация>]**

2) **rule edit ipx:<номер> [action=<действие>] [in=<вход>] [out=<вход>] [srcnet=<сети_источника>] [srchost=<хосты_источника>] [srcsock=<сокеты_ источника>] [dstnet=<сети_приемника>] [dsthost=<хосты_ приемника>][dstsock=<сокеты_приемника>][packet=<тип_пакета>] [vlan=<vlans>] [time=<интервал_времени>] [alarm=<сигнализация>] [active=<активность>] [log=<регистрация>] [comments=<комментарии>]**, где - **<номер>** - номер IPX-правила. Допустимые значения: 0-65535;

Остальные параметры IPX-правила аналогичны параметрам команды rule add ipx.

Пример:

fnpsh> rule edit ipx:20:accept:nolog:eth1:eth0:0:0x1010-0x1023/any:ncp,sap,
0x1f15:0x1030/any:any:any:::novlan:alarm
Изменить IPX правило? (Y/N) [N]: y
FNPSH-I-3013-IPX правило изменено (20)
fnpsh>
fnpsh> rule edit ipx:30 srcnet=1 srchost=00c012be5f1a alarm=no
Изменить IPX правило? (Y/N) [N]: y
FNPSH-I-3013-IPX правило изменено (30)
fnpsh>
fnpsh> rule edit ipx:0 action=drop
Изменить IPX правило? (Y/N) [N]: y
FNPSH-I-3013-IPX правило изменено (0)
fnpsh>
fnpsh> rule show type=ipx
ipx:0:drop:nolog
ipx:20:accept:nolog:1:0:0:1010-1023/any:ncp,sap,1f15:1030/any:any:
any:active::novlan:alarm
ipx:30:drop:logpkt:2::0:1/00c012be5f1a:any:1f00/0d0e1478ff11,0d0e14acbb17:
any:any:active::vlan:noalarm
fnpsh>

fnpsh> rule show type=ipx mode=detail
IPX правило 0:
Действие: drop (удаление)
Регистрация пакета: отключено
IPX правило 20:
Действие: accept (передача на выходные интерфейсы)
Входные интерфейсы: eth1
Выходные интерфейсы: eth0
Сети/хосты источника: 1010-1023/any
Сокеты источника: ncp,sap,1f15
Сети/хосты приемника: 1030/any
VLAN: нет (пакеты без тэга VLAN)
Сигнализация: включено
IPX правило 30:
Действие: drop (удаление)
Входные интерфейсы: eth2
Сети/хосты источника: 1/00c012be5f1a
Сети/хосты приемника: 1f00/0d0e1478ff11,0d0e14acbb17
VLAN: да (пакеты с тэгом VLAN)
Регистрация пакета: включено
fnpsh>

Для удаления существующего IPX-правила используется команда rule delete ipx:<номер>, где <номер> - номер существующего IPX-правила.

Пример:

fnpsh> rule delete ipx:20
Удалить IPX правило? (Y/N) [N]: y
FNPSH-I-301A-IPX правило удалено (20)
fnpsh>
Глобальное IPX-правило не может быть удалено.

4.7.10. Правила фильтрации прикладного уровня

Прикладные правила предназначены для фильтрации пакетов по данным прикладного уровня. Параметры прикладного правила зависят от прикладного протокола, для фильтрации которого предназначено данное правило. Прикладные протоколы различаются следующим образом:

- протокол HTTP (HyperText Transfer Protocol, протокол передачи гипертекстовой информации);

- протокол SMTP (Simple Mail Transfer Protocl, простой протокол передачи почты);

- протокол FTP (File Transfer Protocol, протокол передачи файлов);

- сервисы SQL (протоколы распределенных систем управления базами данных);

- все остальные прикладные протоколы.

Для любых текстовых данных, используемых в качестве параметров прикладного правила (например, имя WEB-сайта или произвольная строка поиска), используются следующие специальные символы:

1) "*" (символ «звездочка»)- любая комбинация символов (например: *.ru относится ко всем именам сайтов в домене ru);

2) "_" (символ «подчеркивание») - пробел (например: Content-Type:_text/html означает строку поиска Content-Type: text/htm);

3) "^" - начало строки прикладных данных (например: ^200_Ok относится к строке 200 Ok, расположенной в начале прикладных данных);

4) "$" - конец строки прикладных данных (например: $end_of_text относится к строке end_of_text, расположенной в конце прикладных данных);

5) "," или "|" - логическое «или» (например: www.ccc.ru,www.bbb.ru будет относиться и к имени сайта www.ccc.ru , и к имени сайта www.bbb.ru);

6) "\" - символ экранирования, т.е. символ, указывающий на отсутствие необходимости рассматривать следующий за ним символ, как специальный (например, **abc_abc@domain.ru** будет удовлетворять строке **abc_abc@domain.ru**, т.е. символ "_" не будет рассматриваться как специальный символ)

Обязательными при добавлении прикладного правила в формате "**ap:<номер>: <параметр1>:<параметр2>:...**" являются параметры **<номер>**, **<действие>**, **<регистрация>** и **<протокол>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию. Допускается отсутствие одно-

го или нескольких параметров в перечне (**<параметр5>:<параметр6>::: <параметр9>**). В этом случае будут использованы значения по умолчанию для пропущенных параметров.

Обязательными при добавлении прикладного правила в формате "**ap:<номер> <параметр1>= <значение>...<параметрN>=<значение>**" являются параметры **<номер>**, **action=<действие>** и **protocol=<протокол>**. Для остальных параметров в случае их отсутствия принимаются значения по умолчанию.

Команды добавления и редактирования прикладных правил в зависимости от прикладного протокола даны ниже.

Для удаления существующего прикладного правила используется команда **rule delete ap:<номер>**, где **<номер>** - номер существующего прикладного правила;

Пример:

fnpsh> rule delete ap:20
Удалить AP правило? (Y/N) [N]: y
FNPSH-I-301A-AP правило удалено (20)
fnpsh>

Глобального правила в таблице прикладных правил не предусмотрено. Если пакет при обработке в таблице прикладных правил не удовлетворяет ни одному правилу, такой пакет пропускается на выходные интерфейсы, определенные ранее на MAC- и IP-уровне.

Прикладное правило применяются к пакету только в том случае, если все параметры правила соответствуют данным пакета (или сессии, к которой принадлежит данный пакет).

4.7.11. Правила фильтрации протокола HTTP

Для добавления нового прикладного правила для фильтрации данных протокола HTTP могут использоваться следующие команды:

1) **rule add ap:<номер>:<действие>:<регистрация>:http[:host=**

<имя_сервера>& method=<http_метод>&file=<имя_файла>&data= <текстовые_данные>&begin=<начало_поиска_двоичных_данных>&olv=<двоичные_данные>: <регистр>:<направление>:<активность>:<комментарии>: <сигнализация>]

2) **rule add ap:<номер> action=<действие> protocol=http [host= <имя_сервера>] [method=<http_метод>] [file=<имя_файла>] [data= <текстовые_данные>] [begin=<начало_поиска_двоичных_данных>] [olv=<двоичные_данные>][case=<регистр>] [dir=<направление>] [alarm=<сигнализация>] [active=<активность>] [log=<регистрация>] [comments=<комментарии>]**,

где:

1) **<номер>** - номер прикладного правила. Допустимые значения: 1-65535;

2) **<действие>** - действие правила. Ожидаются следующие значения:

- **accept** или **pass**– передача пакета на выходные интерфейсы;

- **drop** – удаление пакета и сессии, к которой принадлежит данный пакет;

3) **<имя_сервера>** - имена WEB-сайтов. Ожидаются следующие ключевые слова и значения:

- **any** – любой WEB-сайт (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<name>[,<name>]** - список имен или фрагментов имен WEB-сайтов (например www.abc.com,*.fee.ru);

4) **<http_метод>** - идентификаторы методов запроса к HTTP-серверу. Ожидаются следующие ключевые слова:

- **get** – метод GET;

- **put** – метод PUT;

- **post** – метод POST;

- **head** - метод HEAD;

- **delete** – метод DELETE.

Допускается указание идентификаторов метода списком (например **get,post**);

5) **<имя_файла>** - имена файлов, запрашиваемых у WEB-сайта. Ожидаются

следующие ключевые слова и значения:

- **any** – любой файл (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<name>[,<name>]** - список имен или фрагментов имен файлов (например index.html,*.pdf,instuction.*);

6) **<текстовые_данные>** - любая последовательность печатных символов. Ожидаются следующие ключевые слова и значения:

- **any** – любая текстовая последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<symbols>[,<symbols>]** - список символьных последовательностей (например Content-Type:_text/html,^HTTP/1.1_200_OK);

7) **<двоичные_данные>** - последовательность двоичных данных по указанному смещению. Ожидаются следующие ключевые слова и значения:

- **any** – любая двоичная последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<смещение>/<длина>/<значение>** - двоичная последовательность в шестнадцатеричном виде <значение>, длина которой в байтах составляет <длина> и смещение относительно начала прикладных данных в байтах составляет <смещение> (например: 12/3/0xac16d3, т.е. будет произведен поиск двоичных данных 0xac16d3, длиной 3 байта по смещению 12 байт от начала прикладных данных пакета). Параметр <смещение> может принимать значение any, в этом случае указанные двоичные данные ищутся на всей длине прикладных данных пакета;

8) **<начало_поиска_двоичных_данных>** - указывает точку отсчета смещения для поиска <двоичных_данных>. Ожидаются следующие ключевые слова:

- **header** – поиск будет производиться от начала заголовка HTTP (по умолчанию);

- **body** – поиск будет производиться от начала тела HTTP-сообщения (заголовок не учитывается);

9) **<регистр>** - регистр символов в строках поиска. Ожидаются следующие

ключевые слова:

- **any** – регистр не учитывается (по умолчанию);

- **upper** – только символы в верхнем регистре;

- **lower** – только символы в нижнем регистре;

- **sensitive –** символы в заданных регистрах;

10) **<направление>** - направление потока, в котором производится поиск. Ожидаются следующие ключевые слова:

- **any** – правило применяется к обоим потокам – от клиента к серверу и от сервера к клиенту (по умолчанию);

- **from-server** - правило применяется только к потоку от сервера к клиенту;

- **from-client** -правило применяется только к потоку от клиента к серверу;

11) **<активность>** - активность данного правила. Ожидаются следующие ключевые слова:

- **yes** или **active** – правило активно (по умолчанию);

- **no** или **noactive** – правило неактивно;

12) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **nolog** – не регистрировать пакеты и сессии, обработанные по данному правилу (по умолчанию);

- **yes** или **log,** или **logpkt, logses** – регистрировать пакеты и сессии, обработанные по данному правилу;

- **pkt** или **logpkt** – регистрировать пакеты, обработанные по данному правилу;

- **ses** или **logses** – регистрировать сессии, обработанные по данному правилу;

13) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом.

Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного пакета;

14) **<комментарии>** - комментарии к данному правилу. Длина строки комментария до 31символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

Пример:

fnpsh> rule add ap:10:drop:nolog:http:host=www.aaa.ru,www.bbb.ru,*.msk.ru:
any: from-client:active:"Запрет сайтов":noalarm
FNPSH-I-300E-AP правило добавлено (10)
fnpsh>

Прикладное правило номер 10 будет блокировать доступ к сайтам www.aaa.ru, www.bbb.ru и сайтам из домена msk.ru

fnpsh> rule add ap:20:pass:logses:http:host=www.pics.ru&file=*/pictures/*:any:
:active:"Разрешение просмотра":noalarm
FNPSH-I-300E-AP правило добавлено (20)
fnpsh>

Прикладное правило номер 20 разрешает запрос файлов из каталога /pictures/ сайта www.pics.ru

fnpsh> rule add ap:30 action=drop protocol=http begin=body olv=0/3/0x3b16df
FNPSH-I-300E-AP правило добавлено (30)
fnpsh>

Прикладное правило номер 30 запрещает пересылку пакета и удаляет сессию в случае, если будут обнаружены данные 0x3b16df по смещению 0 байт относительно начала тела HTTP-сообщения.

Внимание!!! Если предполагается фильтрация только по параметру **«host»**, то рекомендуется устанавливать параметр направления в значение **«от клиента – from-client»** для того, чтобы ускорить обработку пакетов в межсетевом экране.

fnpsh> rule show type=ap
ap:10:drop:nolog:http:host=www.aaa.ru,www.bbb.ru,*.msk.ru:any:from-
client:acti ve:"Запрет сайтов":noalarm
ap:20:pass:logses:http:host=www.pics.ru&file=*/pictures/*:any:any:active:

"Разрешение просмотра":noalarm
ap:30:drop:nolog:http:begin=body&olv=0/3/0x3b16df:any:any:active::noalarm
fnpsh>
fnpsh> rule show type=ap mode=detail
Прикладное правило 10 - "Запрет сайтов":
Действие: drop (удаление пакета и сессии)
Прикладной протокол: http
WEB-сервера: www.aaa.ru,www.bbb.ru,*.msk.ru
Направление поиска: от клиента к серверу
Прикладное правило 20 - "Разрешение просмотра":
Действие: pass (передача на выходные интерфейсы)
Прикладной протокол: http
WEB-сервера: www.pics.ru
Имена файлов: */pictures/*
Регистрация сессий: включено
Прикладное правило 30:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: http
Двоичные данные: смещение 0, длина 3, значение 0x3b16df
fnpsh>

Для редактирования существующего прикладного правила для фильтрации данных протокола HTTP могут использоваться следующие команды:

1) **rule edit ap:<номер>:<действие>:<регистрация>:http[:host=<имя_сервера>&method=<http_метод>&file=<имя_файла>&data=<текстовые_данные>&begin=<начало_поиска_двоичных_данных>&olv=<двоичные_ данные>: <регистр>: <направление>:<активность>:<комментарии>: <сигнализация>]**

2) **rule edit ap:<номер> [action=<действие>] [host=<имя_сервера>] [method=<http_метод>] [file=<имя_файла>] [data=<текстовые_данные>] [begin=<начало_поиска_двоичных_данных>] [olv=<двоичные_данные>] [case=<регистр>] [dir=<направление>] [alarm=<сигнализация>] [active= <активность>] [log=<регистрация>] [comments=<комментарии>]**,

где: **<номер>** - номер прикладного правила. Допустимые значения: 1-65535;

Остальные параметры прикладного правила для фильтрации данных протокола HTTP аналогичны параметрам команды **rule add ap**, описанной выше в этом

разделе. При редактировании прикладного правила в формате "**ap:<номер> <параметр1>= <значение>...<параметрN>=<значение>**" не допускается изменять параметр идентификатора прикладного протокола.

Пример:

fnpsh> rule edit ap:30:drop:nolog:http:begin=body&olv=0/3/0x3b16df:::::alarm
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (30)
fnpsh>

У прикладного правила номер 30 изменили значение параметра сигнализации

fnpsh> rule edit ap:10 host=www.aaa.ru
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (10)
fnpsh>

У прикладного правила номер 10 изменили список имен сайтов.

fnpsh> rule edit ap:20 file=any
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (20)
fnpsh>

У прикладного правила номер 20 удалили параметр file из списка параметров.

fnpsh> rule show type=ap
ap:10:drop:nolog:http:host=www.aaa.ru:any:from-client:active:"Запрет сайтов": noalarm
ap:20:pass:logses:http:host=www.pics.ru:any:any:active:"Разрешение просмотра": noalarm
ap:30:drop:nolog:http:begin=body&olv=0/3/0x3b16df:any:any:active::alarm
fnpsh>
fnpsh> rule show viewer=no mode=detail type=ap
Прикладное правило 10 - "Запрет сайтов":
Действие: drop (удаление пакета и сессии)
Прикладной протокол: http
WEB-сервера: www.aaa.ru
Направление поиска: от клиента к серверу
Прикладное правило 20 - "Разрешение просмотра":
Действие: pass (передача на выходные интерфейсы)
Прикладной протокол: http
WEB-сервера: www.pics.ru
Регистрация сессий: включено

Прикладное правило 30:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: http
Двоичные данные: смещение 0, длина 3, значение 0x3b16df
Сигнализация: включено
fnpsh>

4.7.12. Правила фильтрации протокола SMTP

Для добавления нового прикладного правила для фильтрации данных протокола SMTP могут использоваться следующие команды:

1) **rule add ap:<номер>:<действие>:<регистрация>:smtp[:from= <отправители>& to=<получатели>&data=<текстовые_данные>&olv=<двоичные_данные>: <регистр>:<направление>:<активность>:<комментарии>: <сигнализация>]**

2) **rule add ap:<номер> action=<действие> protocol=smtp [from=<отправители>] [to=<получатели>] [data=<текстовые_данные>] [olv=<двоичные_данные>][case=<регистр>] [dir=<направление>] [alarm= <сигнализация>] [active=<активность>] [log=<регистрация>] [comments= <комментарии>]**,

где:

1) **<номер>** - номер прикладного правила. Допустимые значения: 1-65535;

2) **<действие>** - действие правила. Ожидаются следующие значения:

- **accept** или **pass**– передача пакета на выходные интерфейсы;

- **drop** – удаление пакета и сессии, к которой принадлежит данный пакет;

3) **<отправители>** - почтовые адреса отправителей. Ожидаются следующие ключевые слова и значения:

- **any** – любой e-mail адрес (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<email>[,<email>]** - список email адресов или фрагментов адресов отправителей (например: abc@fee.ru,*@hotmail.com)

4) **<получатели>** - почтовые адреса получателей. Ожидаются следующие ключевые слова и значения:

- **any** – любой e-mail адрес (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<email>[,<email>]** - список email адресов или фрагментов адресов олучателей (например: abc@fee.ru,*@hotmail.com);

5) **<текстовые_данные>** - последовательность печатных символов. Ожидаются следующие ключевые слова и значения:

- **any** – любая текстовая последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<symbols>[,<symbols>]:** список текстовых последовательностей (например Content-Type:_text/html,^HTTP/1.1_200_OK);

6) **<двоичные_данные>** - последовательность двоичных данных по указанному смещению. Ожидаются следующие ключевые слова и значения:

- **any** – любая двоичная последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<смещение>/<длина>/<значение>** - двоичная последовательность в шестнадцатеричном виде <значение>, длина которой в байтах составляет <длина> и смещение относительно начала прикладных данных в байтах составляет <смещение> (например: 12/3/0xac16d3, т.е. будет произведен поиск двоичных данных 0xac16d3, длиной 3 байта по смещению 12 байт от начала прикладных данных пакета). Параметр <смещение> может принимать значение **any**, в этом случае указанные двоичные данные ищутся на всей длине прикладных данных пакета;

7) **<регистр>** - регистр символов в строках поиска. Ожидаются следующие ключевые слова:

- **any** – регистр не учитывается (по умолчанию);

- **upper** – только символы в верхнем регистре;

- **lower** – только символы в нижнем регистре;

- **sensitive –** символы в заданных регистрах;

8) **<направление>** - направление потока, в котором производится поиск. Ожидаются следующие ключевые слова:

- **any** – правило применяется к обоим потокам – от клиента к серверу и от сервера к клиенту (по умолчанию);

- **from-server:** правило применяется только к потоку от сервера к клиенту;

- **from-client:** правило применяется только к потоку от клиента к серверу;

9) **<активность>** - активность данного правила. Ожидаются следующие ключевые слова:

- **yes** или **active** – правило активно (по умолчанию);

- **no** или **noactive** – правило неактивно;

10) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **nolog** – не регистрировать пакеты и сессии, обработанные по данному правилу (по умолчанию);

- **yes** или **log,** или **logpkt, logses** – регистрировать пакеты и сессии, обработанные по данному правилу;

- **pkt** или **logpkt** – регистрировать пакеты, обработанные по данному правилу;

- **ses** или **logses** – регистрировать сессии, обработанные по данному правилу;

11) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом.Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного пакета;

12) **<комментарии>** - комментарии к данному правилу. Длина строки комментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

В силу особенностей протокола SMTP и его обработки ПО ССПТ-2 для фильтрации почтовых сообщений не может быть построено политики «все, что не разрешено, запрещено».

Пример:

fnpsh> rule add ap:10:drop:nolog:smtp:to=abc@fee.ru:any:from-client:active:
"Запрет получателя":noalarm
FNPSH-I-300E-AP правило добавлено (10)
fnpsh>

Прикладное правило номер 10 будет блокировать отправку почты на адрес abc@fee.ru.

fnpsh> rule add ap:20 action=accept protocol=smtp from=andrey@corporate.ru, valily@corporate.ru alarm=yes
FNPSH-I-300E-AP правило добавлено (20)
fnpsh>

Прикладное правило номер 20 разрешает отправку почты с адресов andrey@corporate.ru и valily@corporate.ru

fnpsh> rule add ap:30 action=drop protocol=smtp
data=Last_week_security_report alarm=yes
FNPSH-I-300E-AP правило добавлено (30)
fnpsh>

Прикладное правило номер 30 запрещает отправку почтового сообщения, в котором встречается строка «Last week security report».

fnpsh> rule show type=ap
ap:10:drop:nolog:smtp:to=abc@fee.ru:any:from-client:active:"Запрет получателя" :noalarm
ap:20:accept:nolog:smtp:from=andrey@corporate.ru,valily@corporate.ru:any:any:active::alarm
ap:30:drop:nolog:smtp:data=Last_week_security_report:any:any:active::alarm
fnpsh>
fnpsh> rule show type=ap mode=detail Прикладное правило 10 - "Запрет получателя":
Действие: drop (удаление пакета и сессии)
Прикладной протокол: smtp
Email адреса получателей: abc@fee.ru
Направление поиска: от клиента к серверу
Прикладное правило 20:
Действие: accept (передача на выходные интерфейсы)
Прикладной протокол: smtp
Email адреса отправителей: andrey@corporate.ru,valily@corporate.ru
Сигнализация: включено

Прикладное правило 30:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: smtp
Текстовые данные: Last_week_security_report
Сигнализация: включено
fnpsh>

Для редактирования существующего прикладного правила для фильтрации данных протокола SMTP могут использоваться следующие команды:

1) **rule edit ap:<номер>:<действие>:<регистрация>:smtp[:from =<отправители>& to=<получатели>&data=<текстовые_данные>&olv= <двоичные_данные>: <регистр>:<направление>:<активность>:<комментарии>: <сигнализация>]**

2) **rule edit ap:<номер> action=<действие> [from=<отправители>] [to=<получатели>] [data=<текстовые_данные>] [olv=<двоичные_данные>] [case=<регистр>] [dir=<направление>] [alarm=<сигнализация>] [active= <активность>] [log=<регистрация>] [comments=<комментарии>]**,

где **<номер>** - номер прикладного правила. Допустимые значения: 1-65535;

Остальные параметры прикладного правила для фильтрации данных протокола SMTP аналогичны параметрам команды **rule add ap**, описанной выше в этом разделе. При редактировании прикладного правила в формате "**ap:<номер> <параметр1>=<значение>... <параметрN>=<значение>**" не допускается изменять параметр идентификатора прикладного протокола.

Пример:

fnpsh> rule edit ap:10:drop:log:smtp:to=abc@fee.ru,def@fee.ru:any:from-client: active:"Запрет получателя":noalarm
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (10)
fnpsh>

У прикладного правила номер 10 изменили список отправителей и параметр регистрации.

fnpsh> rule edit ap:20 to=*@corporate.ru
Изменить прикладное правило? (Y/N) [N]: y

FNPSH-I-3015-AP правило изменено (20)
fnpsh>

У прикладного правила номер 20 добавили получателя почтового сообщения.

fnpsh> rule edit ap:30 data=any
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (30)
fnpsh>

У прикладного правила номер 30 удалили параметр data из списка параметров. После этого данное правило применяется к любому пакету SMTP-протокола.

fnpsh>ruleshow type=ap ap:10:drop:logpkt,logses:smtp:to=abc@fee.ru,def@fee.ru:any:from-client:active:"Запрет получателя":noalarm
ap:20:accept:nolog:smtp:from=andrey@corporate.ru,valily@corporate.ru&to=*@corporate.ru:any:any:active::alarm
ap:30:drop:nolog:smtp::any:any:active::alarm
fnpsh>
fnpsh> rule show viewer=no type=ap mode=detail
Прикладное правило 10 - "Запрет получателя":
Действие: drop (удаление пакета и сессии)
Прикладной протокол: smtp
Email адреса получателей: abc@fee.ru,def@fee.ru
Направление поиска: от клиента к серверу
Регистрация пакета: включено; регистрация сессий: включено
Прикладное правило 20:
Действие: accept (передача на выходные интерфейсы)
Прикладной протокол: smtp
Email адреса отправителей: andrey@corporate.ru,valily@corporate.ru
Email адреса получателей: *@corporate.ru
Сигнализация: включено
Прикладное правило 30:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: smtp
Сигнализация: включено
fnpsh>

4.7.13. Правила фильтрации протокола FTP

Для добавления нового прикладного правила для фильтрации данных протокола FTP могут использоваться следующие команды:

1) **rule add ap:<номер>:<действие>:<регистрация>:ftp[:cmd= <команды>& file=<имя_файла>&user=<имя_пользователя>&pass=<пароль>&data= <текстовые_данные>&olv=<двоичные_данные>: <регистр>:<направление>: <активность>:<комментарии>:<сигнализация>]**

2) **rule add ap:<номер> action=<действие> protocol=ftp [cmd=<команды>] [file=<имя_файла>] [user=<имя_пользователя>] [pass=<пароль>] [data= <текстовые_данные>] [olv=<двоичные_данные>][case=<регистр>] [dir= <направление>] [alarm=<сигнализация>] [active=<активность>] [log=<регистрация>] [comments=<комментарии>]**,

где:

1) **<номер>** - номер прикладного правила. Допустимые значения: 1-65535;

2) **<действие>** - действие правила. Ожидаются следующие значения:

- **accept** или **pass** – передача пакета на выходные интерфейсы;

- **drop** – удаление пакета и сессии, к которой принадлежит данный пакет;

3) **<команды>** - команды клиента протокола FTP. Ожидаются следующие ключевые слова:

- **any** – любая команда (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **put** - команда пересылки файла на FTP-сервер;

- **get** - команда пересылки файла с FTP-сервера;

- **list** - команда вывода содержимого каталога FTP-сервера;

Возможно задание параметра списком (например: **get,list**);

4) **<имя_файла>** - имена файлов, передаваемых между FTP-клиентом и FTP-сервером. Ожидаются следующие ключевые слова и значения:

- **any** – любой файл (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<name>[,<name>]** - список имен или фрагментов имен файлов (например **document1.doc,*.zip,crack.***);

5) **<имя_пользователя>** - имена пользователей, предъявляемые при доступе

к FTP-серверу. Ожидаются следующие ключевые слова и значения:

- **any** – любое имя пользователя (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<name>[,<name>]** - список имен или фрагментов имен пользователей (например **andr,swb,anonymous,Alexander***)

6) **<пароль>** - пароли пользователей, предъявляемые при доступе к FTP-серверу. Ожидаются следующие ключевые слова и значения:

- **any** – любой пароль (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<password>[,<password>]** - список паролей или фрагментов паролей (например **qwerty, *arm**)

7) **<текстовые_данные>** - последовательность печатных символов. Ожидаются следующие ключевые слова и значения:

- **any** – любая текстовая последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<symbols>[,<symbols>]:** список текстовых последовательностей (например **Content-Type:_text/html,^HTTP/1.1_200_OK**);

8) **<двоичные_данные>** - последовательность двоичных данных по указанному смещению. Ожидаются следующие ключевые слова и значения:

- **any** – любая двоичная последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<смещение>/<длина>/<значение>** - двоичная последовательность в шестнадцатеричном виде <значение>, длина которой в байтах составляет <длина> и смещение относительно начала прикладных данных в байтах составляет <смещение> (например: 12/3/0xac16d3, т.е. будет произведен поиск двоичных данных 0xac16d3, длиной 3 байта по смещению 12 байт от начала прикладных данных пакета). Параметр <смещение> может принимать значение any, в этом случае указанные двоичные данные ищутся на всей длине прикладных данных пакета;

9) **<регистр>** - регистр символов в строках поиска. Ожидаются следующие

ключевые слова:

- **any** – регистр не учитывается (по умолчанию);

- **upper** – только символы в верхнем регистре;

- **lower** – только символы в нижнем регистре;

- **sensitive –** символы в заданных регистрах;

10) **<направление>** - направление потока, в котором производится поиск. Ожидаются следующие ключевые слова:

- **any** – правило применяется к обоим потокам – от клиента к серверу и от сервера к клиенту (по умолчанию);

- **from-server:** правило применяется только к потоку от сервера к клиенту;

- **from-client:** правило применяется только к потоку от клиента к серверу;

11) **<активность>** - активность данного правила. Ожидаются следующие ключевые слова:

- **yes** или а**ctive** – правило активно (по умолчанию);

- **no** или **noactive** – правило неактивно;

12) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **nolog** – не регистрировать пакеты и сессии, обработанные по данному правилу (по умолчанию);

- **yes** или **log,** или **logpkt, logses** – регистрировать пакеты и сессии, обработанные по данному правилу;

- **pkt** или **logpkt** – регистрировать пакеты, обработанные по данному правилу;

- **ses** или **logses** – регистрировать сессии, обработанные по данному правилу;

13) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного пакета;

14) **<комментарии>** - комментарии к данному правилу. Длина строки ком-

ментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

В силу особенностей протокола FTP и его обработки ПО ССПТ-2 для фильтрации данных этого протокола не может быть построено политики «все, что не разрешено, запрещено».

Пример:

fnpsh> rule add ap:10:drop:log:ftp:user=andr&file=*.zip:any:any:active:"Запрет скачивания файла":noalarm
FNPSH-I-300E-AP правило добавлено (10)
fnpsh>

Прикладное правило номер 10 блокирует запросы на получение файлов с расширением zip для пользователя andr.

fnpsh> rule add ap:20 action=drop protocol=ftp cmd=put
FNPSH-I-300E-AP правило добавлено (20)
fnpsh>

Прикладное правило номер 20 блокирует попытки передать файлы на FTP-сервер.

fnpsh> rule add ap:30 action=accept protocol=ftp user=anonymous pass=qweqwerty
FNPSH-I-300E-AP правило добавлено (30)
fnpsh>

Прикладное правило номер 30 разрешает доступ к FTP-серверу пользователя anonymous с паролем qweqwerty.

fnpsh> rule show type=ap
ap:10:drop:logpkt,logses:ftp:user=andr&file=*.zip:any:any:active:"Запрет скачивания файла":noalarm
ap:20:drop:nolog:ftp:cmd=put:any:any:active::noalarm
ap:30:accept:nolog:ftp:user=anonymous&pass=qweqwerty:any:any:active:
:noalarm
fnpsh>
fnpsh> rule show viewer=no type=ap mode=detail
Прикладное правило 10 - "Запрет скачивания файла":
Действие: drop (удаление пакета и сессии)
Прикладной протокол: ftp
Имена файлов: *.zip

Пользователи FTP: andr
Регистрация пакета: включено; регистрация сессий: включено
Прикладное правило 20:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: ftp
Команды FTP: put
Прикладное правило 30:
Действие: accept (передача на выходные интерфейсы)
Прикладной протокол: ftp
Пользователи FTP: anonymous
Пароли пользователей FTP: qweqwerty
fnpsh>

Для редактирования существующего прикладного правила для фильтрации данных протокола FTP могут использоваться следующие команды:

1) **rule edit ap:<номер>:<действие>:<регистрация>:ftp[:cmd=<команды> &file=<имя_файла>&user=<имя_пользователя>&pass=<пароль>& data= <текстовые_данные>&olv=<двоичные_данные>: <регистр>:<направление>: <активность>:<комментарии>:<сигнализация>]**

2) **rule edit ap:<номер> action=<действие> protocol=ftp [cmd=<команды>] [file=<имя_файла>] [user=<имя_пользователя>] [pass=<пароль>] [data= <текстовые_данные>] [olv=<двоичные_данные>] [case=<регистр>] [dir=<направление>] [alarm=<сигнализация>] [active=<активность>] [log=<регистрация>] [comments=<комментарии>]**,

где: **<номер>** - номер существующего прикладного правила. Допустимые значения: 1-65535;

Остальные параметры прикладного правила для фильтрации данных протокола FTP аналогичны параметрам команды **rule add ap**, описанной выше в этом разделе. При редактировании прикладного правила в формате "**ap:<номер> <параметр1>=<значение>... <параметрN>=<значение>**" не допускается изменять параметр идентификатора прикладного протокола.

Пример:

fnpsh> rule edit ap:10:drop:nolog:ftp:file=*.zip:any:any:active:"Запрет скачивания файла":noalarm

Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (10)
fnpsh>

У прикладного правила номер 10 изменили параметр регистрации и удалили идентификатор пользователя.

fnpsh> rule edit ap:20 cmd=any user=anonymous
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (20)
fnpsh>

У прикладного правила номер 20 удалили параметр cmd из списка параметров и добавили параметр user.

fnpsh> rule show type=ap
ap:10:drop:nolog:ftp:file=*.zip:any:any:active:"Запрет скачивания файла":
noala rm
ap:20:drop:nolog:ftp:user=anonymous:any:any:active::noalarm
ap:30:accept:nolog:ftp:user=anonymous&pass=qweqwerty:any:any:active::
noalarm
fnpsh>
fnpsh> rule show type=ap mode=detail
Прикладное правило 10 - "Запрет скачивания файла":
Действие: drop (удаление пакета и сессии)
Прикладной протокол: ftp
Имена файлов: *.zip
Прикладное правило 20:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: ftp
Пользователи FTP: anonymous
Прикладное правило 30:
Действие: accept (передача на выходные интерфейсы)
Прикладной протокол: ftp
Пользователи FTP: anonymous
Пароли пользователей FTP: qweqwerty
fnpsh>

4.7.14. Правила фильтрации сервисов SQL

Под сервисами SQL далее понимается протоколы взаимодействия следующих приложений:

1) Oracle SQL*NET (идентификатор сервиса: sql*net);

2) Microsoft SQL server (идентификатор сервиса: ms-sql-s);

3) Microsoft SQL monitor (идентификатор сервиса: ms-sql-m);

4) Watcom SQL (идентификатор сервиса: watcom-sql);

5) PostgreSQL (идентификатор сервиса: postgresql).

Для добавления нового прикладного правила для фильтрации данных сервисов SQL могут использоваться следующие команды:

1) **rule add ap:<номер>:<действие>:<регистрация>:<sql_сервис>[:query=<sql_запрос>&data=<текстовые_данные>&olv=<двоичные_данные>:<регистр>:<направление>:<активность>:<комментарии>:<сигнализация>]**

2) **rule add ap:<номер> action=<действие> protocol=<sql_сервис> [query=<sql_запрос>] [data=<текстовые_данные>] [olv=<двоичные_данные>] [case=<регистр>] [dir=<направление>] [alarm=<сигнализация>] [active= <активность>] [log= <регистрация>] [comments=<комментарии>]**,

где:

1) **<номер>** - номер прикладного правила. Допустимые значения: 1-65535;

2) **<действие>** - действие правила. Ожидаются следующие значения:

accept или **pass** – передача пакета на выходные интерфейсы;

drop – удаление пакета и сессии, к которой принадлежит данный пакет;

3) **<sql_сервис>** - идентификатор SQL-сервиса. Ожидаются следующие ключевые слова:

- **sql** – любой сервис SQL из перечисленных выше;
- **sql*net** – сервис Oracle SQL*NET;
- **ms-sql-s** – сервис Microsoft SQL server;
- **ms-sql-m** – сервис Microsoft SQL monitor;
- **watcom-sql** – сервис Watcom SQL;
- **postgresql** – сервис PostgreSQL;

4) **<sql_запрос>** - SQL-запрос или его фрагмент. Ожидаются следующие ключевые слова и значения:

- **any** – любой запрос (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<запрос>[,<запрос>]** - SQL-запрос или его фрагмент (например **update_table_set_cl_id=*,select_*_from_table**). В данном примере заэкранирован знак подчеркивания в имени параметра cl_id и знак «*» в запросе select для того, чтобы ПО ССПТ-2 не воспринимало данные символы в качестве специальных);

5) **<текстовые_данные>** - последовательность печатных символов. Ожидаются следующие ключевые слова и значения:

- **any** – любая текстовая последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<symbols>[,<symbols>]:** список текстовых последовательностей (например **John_Smith,Oleg_Popov**);

6) **<двоичные_данные>** - последовательность двоичных данных по указанному смещению. Ожидаются следующие ключевые слова и значения:

- **any** – любая двоичная последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<смещение>/<длина>/<значение>** - двоичная последовательность в шестнадцатеричном виде <значение>, длина которой в байтах составляет <длина> и смещение относительно начала прикладных данных в байтах составляет <смещение> (например: 12/3/0xac16d3, т.е. будет произведен поиск двоичных данных 0xac16d3, длиной 3 байта по смещению 12 байт от начала прикладных данных пакета). Параметр <смещение> может принимать значение any, в этом случае указанные двоичные данные ищутся на всей длине прикладных данных пакета;

7) **<регистр>** - регистр символов в строках поиска. Ожидаются следующие ключевые слова:

- **any** – регистр не учитывается (по умолчанию);

- **upper** – только символы в верхнем регистре;

- **lower** – только символы в нижнем регистре;

- **sensitive –** символы в заданных регистрах;

8) **<направление>** - направление потока, в котором производится поиск. Ожидаются следующие ключевые слова:

- **any** – правило применяется к обоим потокам – от клиента к серверу и от сервера к клиенту (по умолчанию);

- **from-server:** правило применяется только к потоку от сервера к клиенту;

- **from-client:** правило применяется только к потоку от клиента к серверу;

9) **<активность>** - активность данного правила. Ожидаются следующие ключевые слова:

- **yes** или **active** – правило активно (по умолчанию);

- **no** или **noactive** – правило неактивно;

10) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **nolog** – не регистрировать пакеты и сессии, обработанные по данному правилу (по умолчанию);

- **yes** или **log,** или **logpkt, logses** – регистрировать пакеты и сессии, обработанные по данному правилу;

- **pkt** или **logpkt** – регистрировать пакеты, обработанные по данному правилу;

- **ses** или **logses** – регистрировать сессии, обработанные по данному правилу;

11) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом.Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного пакета;

2) **<комментарии>** - комментарии к данному правилу. Длина строки комментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

В силу особенностей сервисов SQL и их обработки ПО ССПТ-2 для фильтрации данных таких протоколов не может быть построено политики «все, что не разрешено, запрещено».

Пример:

fnpsh> rule add ap:10:drop:nolog:sql:query=update_table_set_cl_id=*:lower:
from-client:active::noalarm
FNPSH-I-300E-AP правило добавлено (10)
fnpsh>

Прикладное правило номер 10 блокирует SQL-запрос любого SQL-сервиса на модификацию поля cl_id таблицы table.

fnpsh> rule add ap:20 action=accept protocol=sql*net query=select_*_from
_tabl e
FNPSH-I-300E-AP правило добавлено (20)
fnpsh>

Прикладное правило номер 20 разрешает сервису Oracle SQL*NET выполнять запрос select * from_table.

fnpsh> rule show type=ap
ap:10:drop:nolog:sql:query=update_table_set_cl_id=*:lower:from-client:active:
:noalarm
ap:20:accept:nolog:sql*net:query=select_*_from_table:any:any:active::noalarm
fnpsh>
fnpsh> rule show type=ap mode=detail
Прикладное правило 10:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: sql
SQL запрос: update_table_set_cl_id=*
Регистр символов: нижний
Направление поиска: от клиента к серверу
Прикладное правило 20:
Действие: accept (передача на выходные интерфейсы)
Прикладной протокол: sql*net
SQL запрос: select_*_from_table
fnpsh>

Для редактирования существующего прикладного правила для фильтрации данных сервисом SQL могут использоваться следующие команды:

1) **rule edit ap:<номер>:<действие>:<регистрация>:<sql_сервис>**

[:query=<sql_запрос>&data=<текстовые_данные>&olv=<двоичные_данные>:<регистр>:<направление>:<активность>:<комментарии>: <сигнализа-

ция>]

2) **rule edit ap:<номер> action=<действие> protocol=<sql_сервис> [query=<sql_запрос>] [data=<текстовые_данные>] [olv=<двоичные_данные>] [case=<регистр>] [dir=<направление>] [alarm=<сигнализация>] [active=<активность>] [log=<регистрация>] [comments=<комментарии>]**,

где: **<номер>** - номер существующего прикладного правила. Допустимые значения: 1-65535;

Остальные параметры прикладного правила для фильтрации данных сервисов SQL аналогичны параметрам команды **rule add ap**, описанной выше в этом разделе. При редактировании прикладного правила в формате "**ap:<номер> <параметр1>=<значение>... <параметрN>=<значение>**" не допускается изменять параметр идентификатора прикладного протокола.

Пример:

fnpsh> rule edit ap:20:accept:logses:sql*net:query=select_*_from_table2:any:
from-client:active::noalarm
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (20)
fnpsh>

У прикладного правила номер 20 изменили параметр регистрации, имя таблицы в SQL-запросе и ограничил направление поиска только потоком от клиента.

fnpsh> rule edit ap:10 query=update_table_set_cl_id=*,update_*
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (10)
fnpsh>

У прикладного правила номер 10 в строку SQL-запроса добавили запрос на изменение таблицы table2.

fnpsh> rule show type=ap
ap:10:drop:nolog:sql:query=update_table_set_cl_id=*,update_table2*:lower:from
client:active::noalarm
ap:20:accept:logses:sql*net:query=select_*_from_table2:any:from-client:active
::noalarm
fnpsh>
fnpsh> rule show viewer=no type=ap mode=detail

Прикладное правило 10:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: sql
SQL запрос: update_table_set_cl_id=*,update_table2*
Регистр символов: нижний
Направление поиска: от клиента к серверу
Прикладное правило 20:
Действие: accept (передача на выходные интерфейсы)
Прикладной протокол: sql*net
SQL запрос: select_*_from_table2
Направление поиска: от клиента к серверу
Регистрация сессий: включено
fnpsh>

4.7.15. Правила фильтрации других прикладных протоколов

Для добавления нового прикладного правила для фильтрации прикладных протоколов, отличных от HTTP, SMTP, FTP и сервисов SQL могут использоваться следующие команды:

1) **rule add ap:<номер>:<действие>:<регистрация>:<протокол>[data=<текстовые_данные>&olv=<двоичные_данные>:<регистр>:<направление>:<активность>:<комментарии>:<сигнализация>]**

2) **rule add ap:<номер> action=<действие> protocol=<протокол> [data=<текстовые_данные>] [olv=<двоичные_данные>] [case=<регистр>] [dir=<направление>] [alarm=<сигнализация>] [active=<активность>] [log= <регистрация>] [comments=<комментарии>]**,

где:

1) **<номер>** - номер прикладного правила. Допустимые значения: 1-65535;

2) **<действие>** - действие правила. Ожидаются следующие значения:

- **accept** или **pass** – передача пакета на выходные интерфейсы;

- **drop** – удаление пакета и сессии, к которой принадлежит данный пакет;

3) **<протокол>** - идентификатор прикладного протокола. Ожидаются следующие ключевые слова и значения:

- **<name>** – имя прикладного протокола (в семействе ОС UNIX см. файл

/etc/services, в семействе ОС Windows см. файл C:\Windows\System32\drivers\etc\services; например: pop3);

- **<num>** – номер прикладного протокола, соответствующий номеру порта для данного протокола. Соответствие между именами и номерами прикладных протоколов содержится в файле services (в семействе ОС UNIX см. файл /etc/services, в семействе ОС Windows см. файл C:\Windows\System32\drivers\etc\services; например: pop3);

4) **<текстовые_данные>** - последовательность печатных символов. Ожидаются следующие ключевые слова и значения:

- **any** – любая текстовая последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<symbols>[,<symbols>]:** список текстовых последовательностей (например John_Smith,Oleg_Popov);

5) **<двоичные_данные>** - последовательность двоичных данных по указанному смещению. Ожидаются следующие ключевые слова и значения:

- **any** – любая двоичная последовательность (по умолчанию). Используется для удаления данного параметра из списка параметров;

- **<смещение>/<длина>/<значение>** - двоичная последовательность в шестнадцатеричном виде <значение>, длина которой в байтах составляет <длина> и смещение относительно начала прикладных данных в байтах составляет <смещение> (например: 12/3/0xac16d3, т.е. будет произведен поиск двоичных данных 0xac16d3, длиной 3 байта по смещению 12 байт от начала прикладных данных пакета). Параметр <смещение> может принимать значение any, в этом случае указанные двоичные данные ищутся на всей длине прикладных данных пакета;

6) **<регистр>** - регистр символов в строках поиска. Ожидаются следующие ключевые слова:

- **any** – регистр не учитывается (по умолчанию);

- **upper** – только символы в верхнем регистре;

- **lower** – только символы в нижнем регистре;

- **sensitive –** символы в заданных регистрах;

7) **<направление>** - направление потока, в котором производится поиск. Ожидаются следующие ключевые слова:

- **any** – правило применяется к обоим потокам – от клиента к серверу и от сервера к клиенту (по умолчанию);

- **from-server:** правило применяется только к потоку от сервера к клиенту;

- **from-client:** правило применяется только к потоку от клиента к серверу;

8) **<активность>** - активность данного правила. Ожидаются следующие ключевые слова:

- **yes** или **active** – правило активно (по умолчанию);

- **no** или **noactive** – правило неактивно;

9) **<регистрация>** - параметр регистрации для пакета, обработанного данным правилом. Ожидаются следующие ключевые слова:

- **no** или **nolog** – не регистрировать пакеты и сессии, обработанные по данному правилу (по умолчанию);

- **yes** или **log,** или **logpkt, logses** – регистрировать пакеты и сессии, обработанные по данному правилу;

- **pkt** или **logpkt** – регистрировать пакеты, обработанные по данному правилу;

- **ses** или **logses** – регистрировать сессии, обработанные по данному правилу;

10) **<сигнализация>** - параметр сигнализации для пакета, обработанного данным правилом.Ожидаются следующие ключевые слова:

- **no** или **noalarm** – не посылать сообщение сигнализации (по умолчанию);

- **yes** или **alarm** – послать сообщение сигнализации о прохождении данного пакета;

11) **<комментарии>** - комментарии к данному правилу. Длина строки комментария до 31 символа. Комментарии с пробелами и/или двоеточиями должны заключаться в двойные кавычки.

Пример:

fnpsh> rule add ap:10:drop:log:tftp:data=update.zip:any:from

-client:active:"Блокировка обновлений":noalarm
FNPSH-I-300E-AP правило добавлено (10)
fnpsh>

Прикладное правило номер 10 блокирует передачу файла update.zip по протоколу TFTP.

fnpsh> rule add ap:20 action=drop protocol=domain
olv=any/11/0x777777046d61696 c027275 dir=from-client
fnpsh>

Прикладное правило номер 20 отправку на DNS-сервер запрос IP-адреса по имени www.mail.ru.

fnpsh> rule show type=ap
ap:10:drop:logpkt,logses:tftp:data=update.zip:any:from-client:active:"Блокировка обновлений":noalarm
ap:20:drop:nolog:domain:olv=any/11/0x777777046d61696c027275:any:from-client:active::noalarm
fnpsh>
fnpsh> rule show type=ap mode=detail
Прикладное правило 10 - "Блокировка обновлений":
Действие: drop (удаление пакета и сессии)
Прикладной протокол: tftp
Текстовые данные: update.zip
Направление поиска: от клиента к серверу
Регистрация пакета: включено; регистрация сессий: включено
Прикладное правило 20:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: domain
Двоичные данные: смещение any, длина 11, значение 0x777777046d61696c027275
Направление поиска: от клиента к серверу
fnpsh>

Для редактирования существующего прикладного правила для фильтрации данных сервисом SQL могут использоваться следующие команды:

1) **rule edit ap:<номер>:<действие>:<регистрация>:<sql_сервис>[:query=<sql_запрос>&data=<текстовые_данные>&olv=<двоичные_данные>:<регистр>:<направление>:<активность>:<комментарии>:<сигнализация>]**

2) **rule edit ap:<номер> action=<действие> protocol=<sql_сервис> [query=**

<sql_запрос>] [data=<текстовые_данные>] [olv=<двоичные_данные>] [case=<регистр>] [dir=<направление>] [alarm=<сигнализация>] [active=<активность>] [log=<регистрация>] [comments=<комментарии>],

где: **<номер>** - номер существующего прикладного правила. Допустимые значения: 1-65535;

Остальные параметры прикладного правила для фильтрации данных сервисов SQL аналогичны параметрам команды **rule add ap**, описанной выше в этом разделе. При редактировании прикладного правила в формате "**ap:<номер> <параметр1>=<значение>... <параметрN>=<значение>**" не допускается изменять параметр идентификатора прикладного протокола.

Пример:

fnpsh> rule edit ap:20:accept:logses:sql*net:query=select_*_from_table2:any:from-client:active::noalarm
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (20)
fnpsh>

У прикладного правила номер 20 изменили параметр регистрации, имя таблицы в SQL-запросе и ограничил направление поиска только потоком от клиента.

fnpsh> rule edit ap:10 query=update_table_set_cl_id=*,update_*
Изменить прикладное правило? (Y/N) [N]: y
FNPSH-I-3015-AP правило изменено (10)
fnpsh>

У прикладного правила номер 10 в строку SQL-запроса добавили запрос на изменение таблицы table2.

fnpsh> rule show type=ap
ap:10:drop:nolog:sql:query=update_table_set_cl_id=*,update_table2*:lower:fro-client:active::noalarm
ap:20:accept:logses:sql*net:query=select_*_from_table2:any:from-client:active::noalarm
fnpsh>
fnpsh> rule show viewer=no type=ap mode=detail
Прикладное правило 10:
Действие: drop (удаление пакета и сессии)
Прикладной протокол: sql

SQL запрос: update_table_set_cl_id=*,update_table2*
Регистр символов: нижний
Направление поиска: от клиента к серверу
Прикладное правило 20:
Действие: accept (передача на выходные интерфейсы)
Прикладной протокол: sql*net
SQL запрос: select_*_from_table2
Направление поиска: от клиента к серверу
Регистрация сессий: включено
fnpsh>

4.7.16. Работа с правилами фильтрации

Кроме команд редактирования имеются команды, облегчающие работу с правилами фильтрации. Это команды:

- просмотра правил;

- копирования правил;

- изменения номера (перемещения) правил;

- просмотра статистики правил.

Для просмотра правил фильтрации, интервалов времени и групп VLAN предназначена команда **rule show**:

fnpsh> rule show viewer=no
mac:0:accept:nolog
arp:0:accept:nolog
ip:0:accept:nolog
ip:2:accept:nolog:0:1,2:0:any:any:any:any:any:any:any:any:any:any:any:active:"
sdf sd":any:defses:deftout:noapr:noalarm
ap:10:accept:nolog:http::any:any:active::noalarm
ap:20:accept:nolog:ftp::any:any:active::noalarm
ap:30:accept:nolog:sql::any:any:active::noalarm
ap:40:accept:nolog:pop3::any:any:active::noalarm
ipx:0:accept:nolog
fnpsh>

По умолчанию правила фильтрации отображаются во внутреннем просмотрщике командного интерфейса администратора. В приведенном выше примере отображение в просмотрщике было отключено (опция viewer=no). Имеется воз-

можность просмотра правил только заданного типа (опция type=<тип_правила>), правил из заданного диапазона номеров (опция rnum=<диапазон>), а также другие опции (полный список опций команд см. в приложении Справочник команд).

Для копирования правил фильтрации, интервалов времени и групп VLAN в пределах таблицы предназначена команда **rule copy**:

fnpsh> rule copy ip 2 10
FNPSH-I-3093-IP правило скопировано
fnpsh> rule show viewer=no
mac:0:accept:nolog
arp:0:accept:nolog
ip:0:accept:nolog
ip:2:accept:nolog:0:1,2:0:any:any:any:any:any:any:any:any:any:any:any:active:"w
sdf sd":any:defses:deftout:noapr:noalarm
ip:10:accept:nolog:0:1,2:0:any:any:any:any:any:any:any:any:any:any:any:active:"
wsdf sd":any:defses:deftout:noapr:noalarm
ap:10:accept:nolog:http::any:any:active::noalarm
ap:20:accept:nolog:ftp::any:any:active::noalarm
ap:30:accept:nolog:sql::any:any:active::noalarm
ap:40:accept:nolog:pop3::any:any:active::noalarm
ipx:0:accept:nolog
fnpsh>
В данном примере IP правило 2 было скопировано в IP правило 10.

Для изменения номера (перемещения) правил фильтрации, интервалов времени и групп VALN в пределах таблицы предназначена команда **rule move**:

fnpsh> rule move ap 40 140
FNPSH-I-309C-AP правило перемещено
fnpsh>
fnpsh> rule show viewer=no
mac:0:accept:nolog
arp:0:accept:nolog
ip:0:accept:nolog
ip:2:accept:nolog:0:1,2:0:any:any:any:any:any:any:any:any:any:any:any:active:"w
sdf sd":any:defses:deftout:noapr:noalarm
ip:10:accept:nolog:0:1,2:0:any:any:any:any:any:any:any:any:any:any:any:active:"
wsdf sd":any:defses:deftout:noapr:noalarm
ap:10:accept:nolog:http::any:any:active::noalarm

ap:20:accept:nolog:ftp::any:any:active::noalarm
ap:30:accept:nolog:sql::any:any:active::noalarm
ap:140:accept:nolog:pop3::any:any:active::noalarm
ipx:0:accept:nolog
fnpsh>

В данном примере у прикладного правила 40 был изменен номер на 140.

Для просмотра статистики использования текущего набора правил фильтрации предназначена команда **rule stats show**:

fnpsh> rule stats show viewer=no

Правила	Последнее изменение	Пакеты	Байты
mac:0	21.11.2006, 12:09:32	255	16K
arp:0	21.11.2006, 12:09:36	160	2904
ip:0	21.11.2006, 12:09:40	12	432
ip:2	21.11.2006, 11:25:19	31	3828
ip:10	21.11.2006, 11:39:24	0	0
ap:10	21.11.2006, 11:29:43	0	0
ap:20	21.11.2006, 11:29:51	0	0
ap:30	21.11.2006, 11:29:58	0	0
ap:140	21.11.2006, 11:41:58	0	0
ipx:0	21.11.2006, 11:25:19	21	1023

fnpsh>

По умолчанию статистика использования правил фильтрации отображаются во внутреннем просмотрщике командного интерфейса администратора. В приведенном выше примере отображение в просмотрщике было отключено (опция viewer=no). Имеется возможность просмотра статистики правил только заданного типа (опция type=<тип_правила>), правил определенного действия (опция action=<действие>), а также другие опции. Количество пакетов, обработанное каждым правилом фактически является счетчиком срабатываний данного правила фильтрации. Количество байт для правил фильтрации является счетчиком полезной нагрузки, обработанной каждым правилом.

Для очистки статистики использования правил фильтрации предназначена команда **rule stats clear**:

fnpsh> rule stats clear
Очистить статистику использования правил? (Y/N) [N]: y
FNPSH-I-30AA-Статистика правил очищена
fnpsh>
fnpsh> rule stats show viewer=no

Правила	Последнее изменение	Пакеты	Байты
mac:0	21.11.2006, 12:09:32	0	0
arp:0	21.11.2006, 12:09:36	0	0
ip:0	21.11.2006, 12:09:40	0	0
ip:2	21.11.2006, 11:25:19	0	0
ip:10	21.11.2006, 11:39:24	0	0
ap:10	21.11.2006, 11:29:43	0	0
ap:20	21.11.2006, 11:29:51	0	0
ap:30	21.11.2006, 11:29:58	0	0
ap:140	21.11.2006, 11:41:58	0	0
ipx:0	21.11.2006, 11:25:19	0	0

fnpsh>

Внимание!!! При изменении правил фильтрации необходимо перезапустить фильтр.

4.7.17. Дополнительные наборы правил

ПО ССПТ-2 имеет возможность работы с дополнительными наборами правил фильтрации, сохраненными на файловой системе ССПТ-2. Над дополнительными наборами командный интерфейс администратора позволяет выполнять следующие действия:

- сохранение текущего набора правил фильтрации в дополнительном наборе;
- просмотр списка имеющихся дополнительных наборов правил;
- загрузка сохраненного дополнительного набора в текущий набор;
- просмотр правил в указанном дополнительном наборе правил;
- удаление дополнительного набора правил фильтрации.
- восстановление предыдущего набора правил;
- загрузка правил по умолчанию.

Для сохранения текущего набора правил фильтрации в дополнительном

наборе предназначена команда **rule save <имя_набора>**:

fnpsh> rule save my_rules
FNPSH-I-301F-Дополнительный набор правил сохранен
fnpsh>

В приведенном примере примере текущий набор правил фильтрации сохранен в дополнительном наборе под именем my_rules.

Для просмотра списка имеющихся дополнительных наборов правил предназначена команда **rule list**:

fnpsh> rule list
Список дополнительных наборов правил:
Имя Время создания
ap_http 19.10.2006 17:41:47 (MSD)
apl_rules 17.02.2006 11:22:18 (MSK)
current 03.07.2006 13:13:45 (MSD)
default_accept 13.11.2006 13:05:53 (MSK)
default_drop 13.11.2006 13:05:53 (MSK)
ftp_rule 16.08.2006 15:28:46 (MSD)
my_rules 21.11.2006 12:51:50 (MSK)
rules 18.09.2006 11:46:37 (MSD)
Всего: 8 Свободно: 0
fnpsh>

Возможно сохранение до восьми дополнительных наборов правил фильтрации. По умолчанию имеется два предустановленных дополнительных набора правил фильтрации:

1) default_accept: все глобальные правила настроены на пропуск пакетов без регистрации;

2) default_drop: все глобальные правила настроены на удаление пакетов без регистрации.

Для просмотра правил в дополнительном наборе предназначена команда **rule show <имя_набора>**:

fnpsh> rule show default_accept
mac:0:accept:nolog

arp:0:accept:nolog
ip:0:accept:nolog
ipx:0:accept:nolog
fnpsh>

В приведенном выше примере осуществлен просмотр предустановленного дополнительного набора правил default_accept.

Для загрузки правил из дополнительного набора предназначена команда **rule load <имя_набора>**:

fnpsh> rule load default_accept
Загрузить дополнительный набор правил (режим управления сессиями)?
(Y/N)[N]: y
FNPSH-I-304A-Таблица сессий очищена
FNPSH-I-301E-Дополнительный набор правил загружен
fnpsh>

В приведенном выше примере загружен дополнительный набор правил default_accept. При выполнении данной команды в режиме управления сессиями и в режиме трансляции сетевых адресов производится очистка таблицы сессий.

Для удаления дополнительного набора правил фильтрации с файловой системы ССПТ-2 предназначена команда **rule remove <имя_набора>**:

fnpsh> rule remove my_rules
Удалить дополнительный набор правил? (Y/N) [N]: y
FNPSH-I-3020-Дополнительный набор правил удален
fnpsh>

При редактировании правил фильтрации на файловой системе ССПТ-2 автоматически сохраняется так называемый предыдущий набор правил, т.е. набор правил по состоянию на момент до редактирования. Для восстановления предыдущего набора правил в качестве текущего предназначена команда **rule rollback**:

fnpsh> rule rollback
Восстановить предыдущий набор правил (режим управления сессиями)?
(Y/N) [N]: y
FNPSH-I-304A-Таблица сессий очищена

FNPSH-I-3021-Предыдущее состояние текущего набора правил восстановлено
fnpsh>

При выполнении данной команды в режиме управления сессиями и в режиме трансляции сетевых адресов производится очистка таблицы сессий.

Для загрузки правил по умолчанию (все глобальные правила настроены на удаление пакетов без регистрации) предназначена команда rule default:

fnpsh> rule default
Установить правила по умолчанию (удаление всех пакетов)? (Y/N) [N]: y
FNPSH-I-304A-Таблица сессий очищена
FNPSH-I-30A0-Установлены правила по умолчанию
fnpsh>

При выполнении данной команды в режиме управления сессиями и в режиме трансляции сетевых адресов производится очистка таблицы сессий.

5. АДМИНИСТРИРОВАНИЕ ССПТ-2 – РЕГИСТРАЦИЯ

5.1. Общие положения

Подсистема регистрации предназначена для ведения журналов регистрации, в которых фиксируются различные события, возникающие при работе ССПТ-2. Различают следующие журналы регистрации:

1) журнал регистрации событий;

2) журнал регистрации трафика;

3) журнал регистрации системных сообщений.

Объем журнала регистрации событий и журнал регистрации пакетов – до 6000 записей каждый. При заполненном журнале регистрации добавление новых записей происходит путем замещения самой старой записи в журнале.

Архивные копии журналов регистрации могут быть сохранены на удаленном FTP сервере для их последующего анализа. Сохранение журналов регистрации на удаленном сервере хранения дает возможность подробного ретроспективного анализа сетевого трафика, а также функционирования ССПТ-2 по их различным показателям на практически неограниченном интервале времени.

Журнал регистрации системных сообщений предназначен для регистрации информации о следующих событиях:

1) события, связанные с работой управляющей операционной системы ССПТ-2;

2) события, возникающие при работе ПО ССПТ-2, и информация о которых может в тносительно короткое время заполнить журнал регистрации событий;

3) события, связанные с получением пакетов с определенными параметрами (механизм сигнализации)

Информация об этих событиях кроме регистрации в журнале системных сообщений может передаваться в режиме реального времени (по мере возникновения событий) на удаленный SYSLOG-сервер для оперативной обработки и анализа.

Для просмотра настроек подсистемы регистрации при использовании интерфейса командной строки предусмотрена команда **log show**:

fnpsh> log show
Регистрация пакетов: отключено
Регистрация ошибочных пакетов в сессиях: отключено
Регистрация ошибочных пакетов в NAT: отключено
Регистрация синхронизации по NTP: отключено
Выгрузка журналов регистрации по FTP: отключено
FTP-сервер: отсутствует
Путь на FTP-сервере: отсутствует
Имя пользователя на FTP-сервере: отсутствует
Выгрузка системных сообщений по SYSLOG: отключено
SYSLOG-сервер: отсутствует
fnpsh>

В выводе данной команды представлена следующая информация:

- состояние параметра регистрации пакетов;

- состояние параметра регистрации пакетов, отброшенных механизмом управления сессиями (некорректных для данного контекста сессии);

- состояние параметра регистрации пакетов, отброшенных механизмом трансляции сетевых адресов (например, пакетов, не предназначенных для передачи на внутренний интерфейс);

- состояние параметра регистрации сообщений о синхронизации времени по протоколу NTP. Данные сообщения регистрируются в журнале системных сообщений;

- состояние параметра выгрузки журналов регистрации на FTP-сервер, а также настройки FTP-сервера;

- состояние параметра выгрузки системных сообщений на SYSLOG-сервер, а также настройки SYSLOG-сервера.

5.2. Журнал регистрации событий

Событие представляет собой изменение состояния, параметров настроек или режима функционирования программного обеспечения ССПТ-2, произошедших в

результате действий администратора, либо в результате возникновения ошибок в работе ССПТ-2. События разделяются на следующие категории:

1) сообщения – предназначены для информирования администратора о событиях, не нарушающих нормальную работу программного обеспечения ССПТ-2;

2) предупреждения – предназначены для информирования администратора о событиях, не нарушающих нормального функционирования программного обеспечения ССПТ-2, однако являющихся нестандартными или некорректными с точки зрения логики работы ССПТ-2;

3) ошибки - предназначены для информирования администратора о событиях, нарушающих нормальную работу программного обеспечения ССПТ-2 и требующих специальных действий по их обработки. В случае частого появления сообщений об ошибках необходимо обращаться за консультациями к предприятию-изготовителю или к его региональным представителям.

Просмотр журнала регистрации событий осуществляется командой log event show, которая отображает журнал регистрации событий во внутреннем просмотрщике командного интерфейса администратора ССПТ-2 (см. рисунок 5.1).

Каждая запись в журнале регистрации событий состоит из следующих полей:

- порядковый номер записи;

- время добавления записи в журнал регистрации событий;

- код события – описание события – уточнение – привилегии пользователей (имя пользователя, IP-адрес управляющего компьютера).

Код события представляет собой конструкцию вида S-XXXX, где S – категория события (I – информационное сообщений, W – предупреждение, E – ошибка), XXXX – шестнадцатеричный номер события данной категории.

Регистрируются следующие события:

1) **информационные сообщения** – предназначены для информирования администратора о событиях, не нарушающих нормальную работу программного обеспечения ССПТ-2:

- 0x1001 - Останов устройства;

- 0x1002 - Перезагрузка устройства;
- 0x1003 - Запуск пакетного фильтра;
- 0x1004 - Останов пакетного фильтра;
- 0x1005 - Перезапуск пакетного фильтра;
- 0x1006 - Проверка целостности программного обеспечения;
- 0x1007 – Включение WEB-интерфейса;
- 0x1008 – Отключение WEB-интерфейса;
- 0x100f - Установка правила в значения по умолчанию;
- 0x1010 - Добавление правила фильтрации;
- 0x1011 - Изменение правила фильтрации;
- 0x1012 - Удаление правила фильтрации;
- 0x1013 - Загрузка дополнительного набора правил;
- 0x1014 - Сохранение дополнительного набора правил;
- 0x1015 - Удаление дополнительного набора правил;
- 0x1016 - Откат к предыдущему состоянию набора правил;
- 0x1017 - Копирование MAC-правила;
- 0x1018 - Перенос MAC-правила;
- 0x1019 - Копирование ARP-правила;
- 0x101a - Перенос ARP-правила;
- 0x101b - Копирование IP-правила;
- 0x101c - Перенос IP-правила;
- 0x101d - Копирование IPX-правила;
- 0x101e - Перенос IPX-правила;
- 0x101f - Копирование IPTMP-правила;
- 0x1020 - Очистка текущей регистрации пакетов;
- 0x1021 - Выгрузка файлов регистрации на FTP-сервер;
- 0x1022 - Очистка текущей регистрации сессий;
- 0x1023 - Включение выгрузки системных сообщений на SYSLOG-сервер;
- 0x1024 - Отключение выгрузки системных сообщений на SYSLOG-сервер;

- 0x1025 - IP-адрес SYSLOG сервера изменен;
- 0x1026 - Дополнительный набор правил загружен с удаленного хоста;
- 0x1027 - Дополнительная конфигурация загружена с удаленного хоста;
- 0x1029 - Перенос IPTMP-правила;
- 0x102a - Копирование интервала времени;
- 0x102b - Перенос интервала времени;
- 0x102c - Копирование AP-праила;
- 0x102d - Перенос AP-правила;
- 0x102e - Перенос группы VLAN;
- 0x102f - Сброс статистики в правилах;
- 0x1030 - Изменение конфигурации ССПТ-2;
- 0x1031 - Включение регистрации пакетов;
- 0x1032 - Изменение системного времени;
- 0x1033 - Настройка выгрузки файлов регистрации на FTP-сервер;
- 0x1034 - Включение режима управления сессиями;
- 0x1036 - Изменение настроек зеркалирования интерфейсов;
- 0x1037 - Изменение настроек тайм-аутов сессий;
- 0x1039 - Установка IP-адреса управляющего интерфейса;
- 0x103a - Удаление IP-адреса управляющего интерфейса;
- 0x103b - Отключение фильтрующего интерфейса;
- 0x103c - Включение фильтрующего интерфейса;
- 0x103d - Изменение скорости передачи фильтрующего интерфейса;
- 0x103e - Изменение режима передачи фильтрующего интерфейса;
- 0x103f - Переименование фильтрующего интерфейса;
- 0x1040 - Установка маршрута по умолчанию;
- 0x1041 - Удаление маршрута по умолчанию;
- 0x1042 - Добавление новой записи в список доступа;
- 0x1043 - Удаление записи из списка доступа;
- 0x1044 - Очистка списка доступа;

- 0x1045 - Включение маршрута по умолчанию;
- 0x1046 - Отключение маршрута по умолчанию;
- 0x1047 - Включение зеркалирования интерфейсов;
- 0x1048 - Отключение зеркалирования интерфейсов;
- 0x1049 - Включение выгрузки на FTP-сервер;
- 0x104a - Отключение выгрузки на FTP-сервер;
- 0x104b - Сброс настроек выгрузки на FTP-сервер;
- 0x104c - Отключение режима управления сессиями;
- 0x104d - Включение регистрации пакетов, отброшенных механизмом управления сессиями;
- 0x104e - Отключение регистрации пакетов, отброшенных механизмом управления сессиями;
- 0x104f - Включение фильтрации на прикладном уровне;
- 0x1050 - Отключение фильтрации на прикладном уровне;
- 0x1051 - Включение создания сессий по умолчанию для IP-правил;
- 0x1052 - Отключение создания сессий по умолчанию для IP-правил;
- 0x1053 - Изменение тайм-аутов для TCP;
- 0x1054 - Изменение тайм-аутов для UDP;
- 0x1055 - Изменение тайм-аутов для ICMP;
- 0x1056 - Изменение тайм-аутов для других протоколов;
- 0x1057 - Изменение размера таблицы сессий;
- 0x1058 - Очистка таблицы сессий;
- 0x1059 - Удаление сессии;
- 0x105a - Установка тайм-аутов в значения по умолчанию;
- 0x105b - Сброс настроек зеркалирования интерфейсов;
- 0x105c - Сохранение текущей конфигурации;
- 0x105d - Сохранение дополнительной конфигурации;
- 0x105e - Удаление дополнительной конфигурации;
- 0x105f - Загрузка дополнительной конфигурации;

- 0x1060 - Загрузка конфигурации по умолчанию;
- 0x1061 - Отключение управляющего интерфейса;
- 0x1062 - Включение управляющего интерфейса;
- 0x1063 - Изменение режима передачи управляющего интерфейса;
- 0x1064 - Изменение скорости передачи управляющего интерфейса;
- 0x1065 - Изменение системной даты;
- 0x1066 - Включение синхронизации по NTP;
- 0x1067 - Отключение синхронизации по NTP;
- 0x1068 - Сброс настроек синхронизации по NTP;
- 0x1069 - Установка IP-адреса NTP-сервера;
- 0x106a - Синхронизация по NTP выполнена;
- 0x106b - Изменение настроек синхронизации по NTP;
- 0x106c - Включение регистрации событий NTP-синхронизации;
- 0x106d - Отключение регистрации событий NTP-синхронизации;
- 0x106e - Изменение периода NTP-синхронизации;
- 0x106f - Изменение часового пояса;
- 0x1070 - Отключение регистрации пакетов;
- 0x1071 - Включение сигнализации обнаружения flood-атак;
- 0x1072 - Отключение сигнализации обнаружения flood-атак;
- 0x1073 - Включение режима обнаружения flood-атак;
- 0x1074 - Отключение режима обнаружения flood-атак;
- 0x1075 - Изменение порогового значения обнаружения flood-атаки;
- 0x1076 - Включение регистрации flood-атак;
- 0x1077 - Отключение регистрации flood-атак;
- 0x1078 - Изменение комментария временного IP-правила для заблокированной flood-атаки;
- 0x1079 - Изменение времени жизни временного IP-правила для заблокированной flood-атаки;
- 0x1100 - Вход пользователя;

- 0x1101 - Выход пользователя;
- 0x1102 - Добавление пользователя;
- 0x1103 - Удаление пользователя;
- 0x1104 - Изменение пароля пользователя;
- 0x1105 - Изменение привилегий пользователя;
- 0x1106 - Отключение пользователя;
- 0x1107 - Включение пользователя;
- 0x1108 - Изменение пароля системного пользователя;
- 0x1109 – Аутентификация сетевого пользователя;
- 0x1200 - Включение NAT;
- 0x1201 - Отключение NAT;
- 0x1202 - Установка диапазона портов NAT;
- 0x1203 - Установка внешнего адреса NAT;
- 0x1204 - Удаление внешнего адреса NAT;
- 0x1205 - Установка маршрута по умолчанию NAT;
- 0x1207 - Установка внутреннего адреса NAT;
- 0x1208 - Удаление внутреннего адреса NAT;
- 0x1209 - Включение регистрации NAT;
- 0x120a - Отключение регистрации NAT;
- 0x120b - Установка внешнего MAC-адреса NAT;
- 0x120c - Удаление внешнего MAC-адреса NAT;
- 0x120d - Добавление записи в ARP-таблицу NAT;
- 0x120e - Удаление записи из ARP-таблицы NAT;
- 0x120f - Очистка ARP-таблицы NAT;
- 0x1210 - Добавление записи в таблицу переадресации NAT;
- 0x1211 - Удаление записи из таблицы переадресации NAT;
- 0x1212 - Очистка таблицы переадресации NAT;
- 0x1213 - Включение переадресации NAT из DMZ;
- 0x1214 - Отключение переадресации NAT из DMZ;

- 0x1215 - Включение переадресации NAT с внешнего интерфейса;
- 0x1216 - Отключение переадресации NAT с внешнего интерфейса;
- 0x1217 - Включение аутентификации пользователей ;
- 0x1218 - Отключение аутентификации пользователей ;
- 0x1219 - Добавление сетевого пользователя;
- 0x121a - Удаление сетевого пользователя;
- 0x121b - Включение сетевого пользователя;
- 0x121c - Отключение сетевого пользователя;
- 0x121d – Прерывание работы сетевого пользователя;
- 0x121e – Смена пароля сетевого пользователя;
- 0x121f – Изменение тайм-аута неактивности сетевых пользователей;
- 0x1220 – Изменение параметров сетевого пользователя;
- 0x1221 – Добавление записи в файл ключей аутентификации;
- 0x1222 – Удаление записи из файла ключей аутентификации;
- 0x1223 – Обновление записи в файле ключей аутентификации;
- 0x1300 - Изменение режима резервирования;
- 0x1301 - Включение резервирования;
- 0x1302 - Отключение резервирования;
- 0x1303 - Изменение смежного резервного устройства;
- 0x1304 - Установка параметров резервирования в значения по умолчанию;
- 0x1305 - Включение синхронизации сессий;
- 0x1306 - Отключение синхронизации сессий;
- 0x1309 - Включение синхронизации правил;
- 0x130a - Отключение синхронизации правил;
- 0x130c - Синхронизация правил инициирована;
- 0x130d - Изменение тайм-аута неактивности для командного интерфейса;
- 0x130e - Изменение скорости передачи при резервировании;
- 0x130f - Изменение режима передачи при резервировании;
- 0x1310 - Синхронизация конфигурации инициирована;

- 0x1311 - Синхронизация правил завершена;
- 0x1312 - Синхронизация конфигурации выполнена;
- 0x1400 - Использование RADIUS включено;
- 0x1401 - Использование RADIUS отключено;
- 0x1402 - Тайм-аут ожидания ответа от RADIUS-сервера изменен;
- 0x1403 - Количество обращений к RADIUS серверу изменено;
- 0x1404 - Конфигурация RADIUS сервера изменена;

2) **предупреждения** – предназначены для информирования администратора о событиях, не нарушающих нормального функционирования программного обеспечения ССПТ-2, однако являющихся нестандартными или некорректными с точки зрения логики работы ССПТ-2:

- 0x2001 - Принят свой собственный кадр Ethernet;
- 0x2002 - Принят неподдерживаемый кадр Ethernet;
- 0x2003 - Недостаточно привилегий для выполнения операции;
- 0x2004 - Набор выходных интерфейсов пустой;
- 0x2005 - Неверная регистрация пользователя;
- 0x2006 - Выход незарегистрированного пользователя;
- 0x2007 - Flood-атака обнаружена и заблокирована;
- 0x2008 - Сервер высокой готовности изменил состояние устройства;
- 0x2009 - Доступ запрещен в соответствии со списком доступа;
- 0x200a - Пакет вне окна приемника;
- 0x200b - Повторный пакет;
- 0x200c - Неверная регистрация пользователя через RADIUS;
- 0x200d - Изменение режима резервирования - перевыборы;
- 0x200e - Изменение режима резервирования - отказ смежного устройства;
- 0x200f - Синхронизация правил не завершена;
- 0x2010 - Синхронизация конфигурации не завершена;
- 0x2011 - Отказ в аутентификации сетевого пользователя;

3) **ошибки** - предназначены для информирования администратора о событи-

ях, нарушающих нормальную работу программного обеспечения ССПТ-2 и требующих специальных действий по их обработки.

В свою очередь, сообщения об ошибках подразделяются на:

1) Общесистемные ошибки:

- 0x3001 - Ошибка ввода/вывода на интерфейс;
- 0x3002 - Ошибка операционной системы;
- 0x3003 - Ошибка в файле конфигурации ССПТ;
- 0x3004 - Ошибка выгрузки файлов регистрации на FTP-сервер;
- 0x3005 - Нарушена целостность программного обеспечения ССПТ;

2) ошибки, обнаруженные при обработке пакетов:

- 0x3006 - Сессия не добавлена - некорректный набор флагов;
- 0x3007 - Сессия не добавлена - таблица переполнена;
- 0x3008 - Сессия не добавлена - ошибка распределения памяти;
- 0x3009 - Сессия не добавлена - неверный номер правила;
- 0x300a - Контекст сессии - неверный входной интерфейс;
- 0x300b - Контекст сессии - не установлен флаг ACK;
- 0x300c - Контекст сессии - неверный набор флагов;
- 0x300d - Контекст сессии - неверный номер последовательности;
- 0x300e - Контекст сессии - неверный номер подтверждения;
- 0x300f - Контекст сессии - неизвестное состояние;
- 0x3100 - NAT - ARP-таблица заполнена;
- 0x3101 - NAT - не найден соответствующий ARP-запрос;
- 0x3102 - NAT - неизвестный тип ARP-сообщения;
- 0x3103 - NAT - неверный IP-адрес источника;
- 0x3104 - NAT - неверный IP-адрес приемника;
- 0x3105 - NAT - внутренний пакет;
- 0x3106 - NAT - нет свободных портов;
- 0x3107 - NAT - таблица обратных потоков заполнена;
- 0x3108 - NAT - недопустимое ICMP-сообщение;

- 0x3109 - NAT - недопустимый протокол;
- 0x310a - NAT - сессия не создана по пакету;
- 0x310b - NAT - неверный пакет с внешнего интерфейса;
- 0x310c - NAT - не найдена соответствующая сессия;
- 0x310d - NAT - не найдена соответствующая запись в ARP-таблице;
- 0x310e - Неверная длина заголовка IP-пакета;
- 0x310f - Некорректный фрагментированный IP-пакет;
- 0x3110 - NAT - фрагментированный пакет;
- 0x3111 - Некорректная длина IP-пакета;
- 0x3112 - Пакет не аутентифицирован.

Журнал регистрации событий

```
                          Журнал регистрации событий
  1| 22.11.2006 14:05:38, MSK | I-1100-Вход пользователя - Командный интерфейс;
  2| 22.11.2006 14:05:26, MSK | W-2005-Неверная регистрация пользователя - Кома
  3| 22.11.2006 14:05:22, MSK | I-1101-Выход пользователя - Командный интерфейс
  4| 22.11.2006 14:04:54, MSK | I-1100-Вход пользователя - Командный интерфейс;
  5| 22.11.2006 14:04:48, MSK | I-1101-Выход пользователя - Командный интерфейс
  6| 22.11.2006 14:03:42, MSK | I-1100-Вход пользователя - Командный интерфейс;
  7| 22.11.2006 14:03:38, MSK | I-1101-Выход пользователя - Командный интерфейс
  8| 22.11.2006 14:02:34, MSK | I-1100-Вход пользователя - Командный интерфейс;
  9| 22.11.2006 14:02:31, MSK | I-1101-Выход пользователя - Командный интерфейс
 10| 22.11.2006 13:52:51, MSK | I-1100-Вход пользователя - Командный интерфейс;
 11| 22.11.2006 13:52:48, MSK | I-1101-Выход пользователя - Командный интерфейс
 12| 22.11.2006 13:52:46, MSK | I-1100-Вход пользователя - Командный интерфейс;
 13| 22.11.2006 13:48:24, MSK | I-1003-Запуск пакетного фильтра - запуск систем
 14| 22.11.2006 13:42:02, MSK | I-1100-Вход пользователя - Командный интерфейс;
 15| 22.11.2006 13:37:53, MSK | E-3005-Нарушена целостность программного обеспе
 16| 22.11.2006 13:35:38, MSK | I-1101-Выход пользователя - Командный интерфейс
 17| 22.11.2006 13:23:13, MSK | I-1100-Вход пользователя - Командный интерфейс;
 18| 22.11.2006 13:23:09, MSK | I-1101-Выход пользователя - Командный интерфейс
 19| 22.11.2006 13:22:32, MSK | I-1100-Вход пользователя - Командный интерфейс;
 20| 22.11.2006 13:07:53, MSK | E-3005-Нарушена целостность программного обеспе
 21| 22.11.2006 13:07:16, MSK | I-1101-Выход пользователя - Командный интерфейс
 22| 22.11.2006 12:54:54, MSK | I-1100-Вход пользователя - Командный интерфейс;
 23| 22.11.2006 11:56:31, MSK | I-1101-Выход пользователя - Командный интерфейс
Строки: 1-23 из 5517          Столбцы: 1-80    H - справка  Q, F10 - выход
```

Рисунок 5.1

Возможна выборка из журнала регистрации событий по категориям и по времени добавления информации о событии.

5.3. Журнал регистрации трафика

Под регистрацией трафика в ССПТ-2 понимается регистрация информации двух видов:

1) регистрация пакетов;

2) регистрация сессий.

5.3.1. Регистрация пакетов

Регистрация пакета происходит при выполнении следующих условий:

1) включен параметр регистрации пакетов подсистемы регистрации;

2) хотя бы одно из правил, которым был обработан пакет, предписывает регистрацию пакета. При обработке в ССПТ-2 пакет проходит несколько уровней фильтрации и, соответственно, таблиц фильтрации (например, IP-пакет может быть последовательно обработан тремя правилами фильтрации: MAC-правилом, IP-правилом и прикладным правилом). Если хотя бы одно из этих правил предписывает регистрацию, пакет будет зарегистрирован.

При использовании интерфейса командной строки включение параметра регистрации пакетов подсистемы регистрации производится командой **log packet enable**:

fnpsh> log packet enable
FNPSH-I-3063-Регистрация пакетов включена
fnpsh>

Включение регистрации пакета в правиле фильтрации производится в соответствии с синтаксисом определения правила фильтрации.

Просмотр пакетов в журнале регистрации трафика осуществляется командой log packet show, которая отображает зарегистрированные пакеты во внутреннем просмотрщике командного интерфейса администратора ССПТ-2 (рис. 5.2).

Каждая строка в журнале регистрации трафика в этом случае представляет собой базовую информацию по отдельному пакету:

- время регистрации;

- действие, произведенное над пакетом;
- цепочка правил, которыми был обработан данный пакет;
- входной и выходные интерфейсы;
- протоколы;
- адреса отправителя и получателя.

При нажатии клавиши «Enter» становится доступной детальная информация о пакете, представленная в соответствии с уровнями обработки:

- общая информация;
- заголовок уровня Ethernet;
- заголовок протоколов ARP/RARP;
- заголовок протокола IP;
- заголовок протокола TCP;
- заголовок протокола UDP;
- заголовок протокола ICMP;
- заголовок протокола IPX;
- данные прикладного уровня.

Журнал регистрации трафика – зарегистрированные пакеты

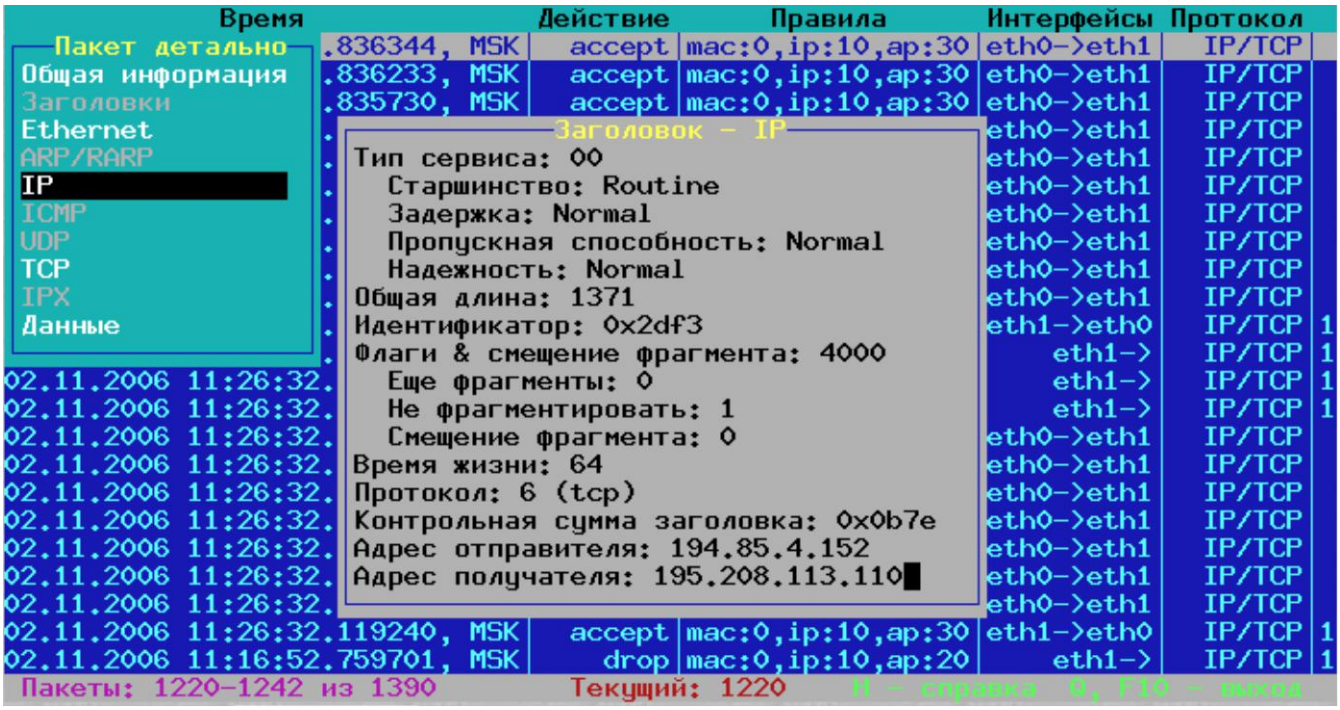

Рисунок 5.2

Возможна выборка информации о пакетах из журнала регистрации трафика по следующим параметрам:

- действие, произведенное над пакетом;
- входной и выходные интерфейсы;
- правило, которым обработан данный пакет;
- тип Ethernet фрейма;
- тип инкапсулированного протокола;
- идентификатор сессии, к которой принадлежал данный пакет;
- MAC-адреса отправителя и получателя пакета;
- IP-адреса отправителя и получателя пакета;
- порты отправителя и получателя пакета;
- время регистрации пакета.

При использовании командного интерфейса для удаления из журнала реги-

страции трафика информации о всех зарегистрированных пакетах предназначена команда **log packet clear**:

fnpsh> log packet clear
Очистить журнал регистрации пакетов? (Y/N) [N]: y
FNPSH-I-3066-Регистрация пакетов очищена
fnpsh>

При удалении из журнала регистрации трафика информации о зарегистрированных пакетах информация о зарегистрированных сессиях сохраняется.

5.3.2. Регистрация сессий

Регистрация сессий производится независимо от параметра регистрации пакетов подсистемы регистрации и происходит при выполнении следующих условий:

1) ССПТ-2 работает в режиме управления сессиями или в режиме трансляции сетевых адресов;

2) IP-правило или прикладное правило, которыми был обработан хотя бы один пакет из сессии, предписывает регистрацию сессии.

Включение регистрации сессии в IP-правиле или прикладном правиле фильтрации производится в соответствии с синтаксисом определения данного правила.

При использовании интерфейса командной строки просмотр сессий в журнале регистрации трафика осуществляется командой **log session show**, которая отображает информацию о зарегистрированных сессиях во внутреннем просмотрщике командного интерфейса администратора ССПТ-2 (см. рисунок 5.3).

Журнал регистрации трафика – зарегистрированные сессии

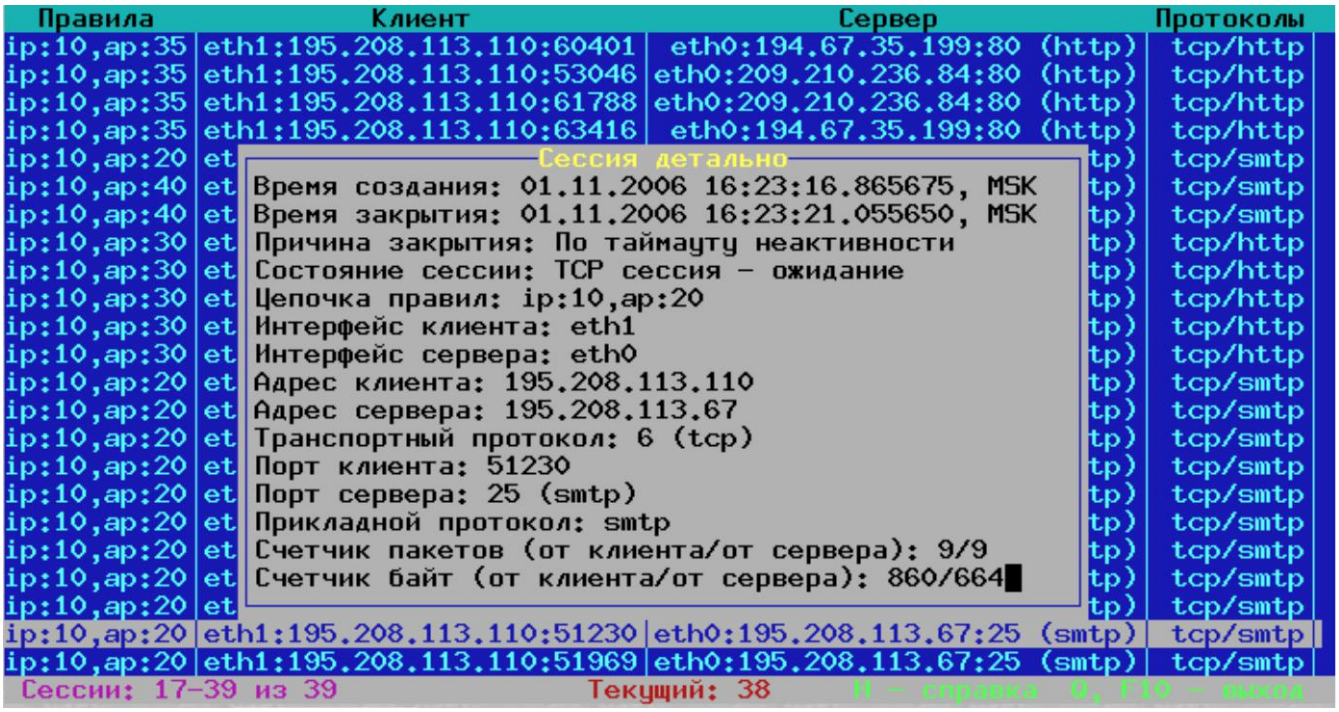

Рисунок 5.3

Каждая строка в журнале регистрации трафика в этом случае представляет собой базовую информацию по отдельной сессии:

- время начала сессии;
- действие, произведенное над пакетом;
- цепочка правил, которыми были обработаны пакеты данной сессии на IP- и прикладном уровне;
- входной и выходные интерфейсы;
- информация о клиенте сессии: интерфейс, IP-адрес, порт;
- информация о сервере сессии: интерфейс, IP-адрес, порт;
- транспортный и прикладной протокол сессии.

При нажатии клавиши **«Enter»** становится доступной следующая детальная информация о сессии:

- время создания сессии;
- время закрытия сессии;

- причина закрытия сессии;
- состояние сессии в момент закрытия;
- цепочка правил, которыми были обработаны пакеты данной сессии на IP- и прикладном уровне;
- интерфейсы клиента и сервера;
- IP-адреса клиента и сервера;
- порты клиента и сервера;
- транспортный и прикладной протокол сессии.
- счетчики пакетов и байт данной сессии;

Возможна выборка информации о сессиях из журнала регистрации трафика по следующим параметрам:

- интерфейсы клиента и сервера;
- IP-адреса клиента и сервера сессии;
- порты клиента и сервера сессии;
- транспортный и прикладной протоколы сессии;
- время начала и окончания сессии;
- номер сессии.

При использовании интерфейса командной строки для удаления из журнала регистрации трафика информации о всех зарегистрированных пакетах предназначена команда **log session clear**:

fnpsh> log session clear
Очистить журнал регистрации сессий? (Y/N) [N]: y
FNPSH-I-30a9-Регистрация сессий очищена
fnpsh>

При удалении из журнала регистрации трафика информации о зарегистрированных сессиях информация о зарегистрированных пакетах сохраняется.

5.4. Журнал регистрации системных сообщений

Журнал регистрации системных сообщений (рис.5.4) предназначен для регистрации сообщений о событиях, связанных с работой управляющей операционной системы ССПТ-2, а также событий, которые могут привести к быстрому заполнению журнала регистрации событий ССПТ-2. К таким событиям относятся:

- события, связанные с запуском и остановом подсистем (серверов) программного обеспечения ССПТ-2;
- события, связанные с ошибками чтения/записи из/на системные устройства;
- события, связанные с функционированием ПО ССПТ-2 при невозможности записать информацию с журнал регистрации событий ССПТ-2;
- синхронизация времени по протоколу NTP;
- выгрузка журналов регистрации на FTP сервер;
- сигнализационные сообщения о получении пакета с заданными параметрами (настраивается путем установки соответствующего флага в правиле фильтрации);
- сигнализационные сообщения об обнаружение и блокировка flood-атаки (настраивается путем установки соответствующего флага в настройках механизма блокировки flood-атаки, группа команд session flood)

ПО ССПТ-2 обеспечивает регистрацию запуска программ и порождения процессов (заданий, задач), относящихся к программной части ССПТ-2. В журнале регистрации системных сообщений регистрируются запуски и другие события, связанные с реализацией инициированных процессов и работой следующих программ:

- Программа «Пакетный фильтр» fnp_filtd;
- Программа «Командный интерпретатор» fnpsh;
- Программа «Командный сервер» fnp_shd;
- Программа «Сервер терминального доступа» fnp_cryd;
- Программа «Сервер регистрации» fnp_logd;
- Программа «Сервер авторизации» fnp_authd;
- Программа «Сервер высокой готовности» fnp_had;

- Программа «Сервер проверки контрольных сумм» fnp_csd;
- Программа инициализации ПО ССПТ-2 fnpsign;
- Программа выгрузки файлов регистрации на FTP сервер logftp.

В параметрах регистрации указываются:

- дата и время регистрируемого события;
- наименование ПО ССПТ-2 (fnp);
- код процесса;
- имя программного модуля
- описание события.

При использовании интерфейса командной строки просмотр журнала регистрации системных сообщений осуществляется командой **log syslog show**, которая отображает информацию во внутреннем просмотрщике командного интерфейса администратора ССПТ-2.

Журнал регистрации системных сообщений

```
 11:56:19            Журнал регистрации системных сообщений        03.07.2012
Jun 23 04:46:41 camel fnp[6124]: sm_add_session: Finding next free session id; 1
Jun 23 16:29:53 camel fnp[6124]: sm_add_session: Finding next free session id; 1
Jun 24 05:22:40 camel fnp[6124]: sm_add_session: Finding next free session id; 1
Jun 24 16:20:12 camel fnp[6124]: sm_add_session: Finding next free session id; 1
Jun 25 04:47:12 camel fnp[6124]: sm_add_session: Finding next free session id; 1
Jun 25 15:38:16 camel fnp[6124]: sm_add_session: Finding next free session id; 1
Jun 25 18:45:56 camel fnp[6124]: fnp_filtd: Пакетный фильтр заканчивает работу (
Jun 25 18:45:56 camel fnp[6119]: fnp_had: Сервер высокой готовности заканчивает
Jun 25 18:45:56 camel fnp[6114]: fnp_cryd: Терминальный сервер заканчивает работ
Jun 25 18:45:56 camel fnp[6109]: fnp_shd Командный сервер заканчивает работу (SI
Jun 25 18:45:56 camel fnp[6104]: fnp_authd: Сервер авторизации заканчивает работ
Jun 25 18:45:56 camel fnp[6099]: fnp_csd: Сервер проверки контрольных сумм закан
Jun 25 18:45:56 camel fnp[6094]: fnp_logd: Сервер регистрации заканчивает работу
Jun 25 18:46:00 camel fnp[26612]: fnpsign: Найдено Ethernet-интерфейсов: 4
Jun 25 18:46:00 camel fnp[26612]: fnpsign: fxp0 - 00:0e:0c:63:8f:16
Jun 25 18:46:00 camel fnp[26612]: fnpsign: fxp1 - 00:0e:0c:63:88:bc
Jun 25 18:46:00 camel fnp[26612]: fnpsign: fxp2 - 00:03:47:3b:68:19
Jun 25 18:46:00 camel fnp[26612]: fnpsign: fxp3 - 00:03:47:3b:68:1a
Jun 25 18:46:00 camel fnp[26612]: fnpsign: Конфигурационный файл ССПТ инициализи
Jun 25 18:46:00 camel fnp[26612]: fnpsign: Файл паролей инициализирован
Jun 25 18:46:00 camel fnp[26612]: fnpsign: Файл сетевых паролей инициализирован
Jun 25 18:46:00 camel fnp[26612]: fnpsign: Файл ключей аутентификации инициализи
 Строки: 1-22 из 355            Столбцы: 1-80    H - справка  Q, F10 - выход
```

Рисунок 5.4

Записи журнала регистрации системных сообщений могут передаваться в режиме реального времени (по мере появления сообщений) на удаленный SYSLOG-сервер для оперативной обработки и анализа.

При регистрации системных сообщений на удаленном SYSLOG - сервере в параметрах регистрации указаны:

- дата и время регистрируемого события;
- IP-адрес управляющего Ethernet - интерфейса ССПТ-2;
- код процесса;
- имя программного модуля
- описание события.

5.5. Выгрузка журналов на FTP сервер

При использовании интерфейса командной строки для настройки выгрузки журналов регистрации событий и трафика на удаленный FTP сервер для их последующего анализа необходимо настроить IP-адрес FTP сервера, каталог на FTP сервере, в который будет производится запись журналов, имя пользователя и пароль для получения доступа к FTP серверу. Данные параметры настраиваются командой log export ftp set, указав в качестве аргументов IP-адрес FTP сервера, путь на FTP сервере, имя пользователя и пароль:

fnpsh> log export ftp set 195.208.113.148 /incoming/ sspt_log
FTP пароль: *******
FTP пароль повторно: *******
FNPSH-I-3037-Параметры выгрузки журналов регистрации по FTP определены
fnpsh>

При использовании интерфейса командной строки для включения выгрузки журналов регистрации событий и трафика на удаленный FTP сервер необходимо воспользоваться командой log export ftp enable:

fnpsh> log export ftp enable
FNPSH-I-3036-Выгрузка журналов регистрации по FTP включена

fnpsh>
fnpsh> log show
Регистрация пакетов: включено
Регистрация ошибочных пакетов в сессиях: отключено
Регистрация ошибочных пакетов в NAT: отключено
Регистрация синхронизации по NTP: включено
Выгрузка журналов регистрации по FTP: включено
FTP-сервер: 195.208.113.148
Путь на FTP-сервере: /incoming/
Имя пользователя на FTP-сервере: sspt_log
Выгрузка системных сообщений по SYSLOG: отключено
SYSLOG-сервер: отсутствует
fnpsh>

При включенном параметре выгрузки журналов регистрации на удаленный FTP сервер по мере накопления информации о трафике и о событиях (каждые 1000 записей) будет осуществляться выгрузка на указанный FTP сервер с указанными параметрами.

5.6. Выгрузка системных сообщений на SYSLOG сервер

В ССПТ-2 имеется возможность отправки системных сообщений кроме локального журнала регистрации системных сообщений еще и на удаленный SYSLOG сервер. Данные сообщения будут отправляться на удаленный сервер в режиме реального времени по мере возникновения событий.

Для настройки приема системных сообщений на SYSLOG сервере (в случае, если используется Unix-подобная операционная система и syslog-демон из стандартной поставки) необходимо:

1. Добавить в файл конфигурации syslog-демона (по умолчанию /etc/syslog.conf) строки вида:

+
!fnp
***.* <имя_файла_регистрации>**

2. Получив права суперпользователя, перезагрузить syslog-демон, разрешив обработку syslog-сообщений, поступивших через сетевой интерфейс и указав

IP-адрес управляющего интерфейса ССПТ-2 в качестве разрешенного адреса, например, командой вида:

root# /usr/sbin/syslogd -n -a <IP_адрес_управляющего_интерфейса_ССПТ-2>/32

После этого системные сообщения, формируемые ССПТ-2, будут регистрироваться на SYSLOG сервере в указанном файле регистрации.

При использовании интерфейса командной строки для настройки выгрузки системных сообщений на удаленный SYSLOG сервер необходимо настроить IP-адрес SYSLOG сервера. Данный параметр настраивается командой **log export syslog server**, указав в качестве аргументов IP-адрес SYSLOG сервера:

fnpsh> log export syslog server 195.208.113.149
FNPSH-I-30B0-Адрес SYSLOG сервера изменен
fnpsh>

При использовании интерфейса командной строки для включения выгрузки системных сообщений на SYSLOG сервер необходимо воспользоваться командой **log export syslog enable**:

fnpsh> log export syslog enable
FNPSH-I-30AF-Выгрузка системных сообщений на SYSLOG сервер включена
fnpsh>
fnpsh> log show
Регистрация пакетов: включено
Регистрация ошибочных пакетов в сессиях: отключено
Регистрация ошибочных пакетов в NAT: отключено
Регистрация синхронизации по NTP: включено
Выгрузка журналов регистрации по FTP: включено
FTP-сервер: 195.208.113.148
Путь на FTP-сервере: /incoming/
Имя пользователя на FTP-сервере: sspt_log
Выгрузка системных сообщений по SYSLOG: включено
SYSLOG-сервер: 195.208.113.149
fnpsh>

6. АДМИНИСТРИРОВАНИЕ ССПТ-2 – ОСНОВНЫЕ РЕЖИМЫ

6.1. Режимы фильтрации

Фильтрация пакетов ССПТ-2 может производиться в трёх основных режимах:

1) в режиме пакетной фильтрации;

2) в режиме управления сессиями;

3) в режиме трансляции сетевых адресов.

В любом из этих режимов может быть включена дополнительная функция зеркалирования трафика. Диаграмма переходов между режимами фильтрации ССПТ-2 с соответствующими командами представлена на рисунке 6.1.

Диаграмма переходов между режимами фильтрации ССПТ-2

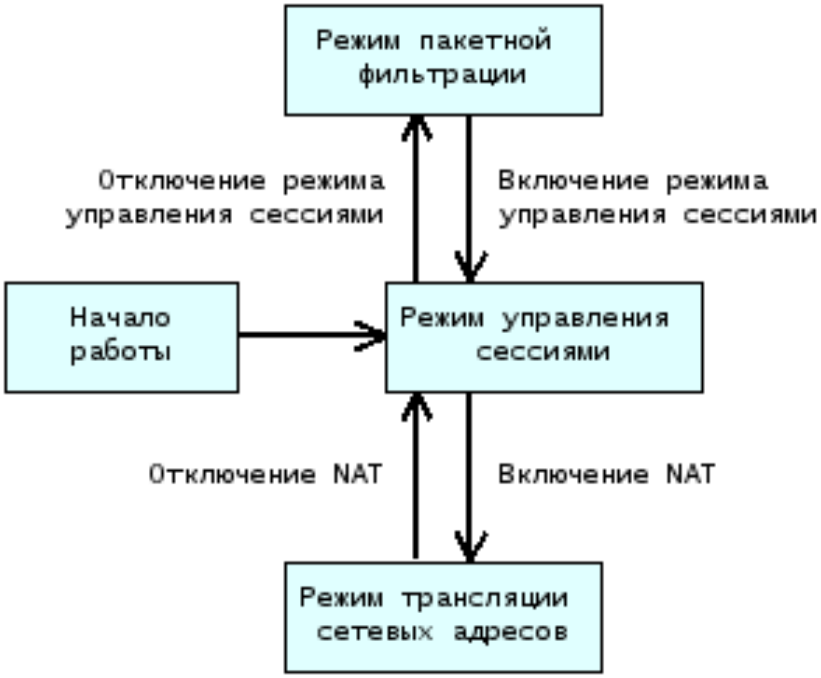

Рисунок 6.1

6.1.1. Режим пакетной фильтрации

В режиме пакетной фильтрации ССПТ-2 обрабатывает независимо каждый пакет на канальном, сетевом, и транспортном уровнях. При использовании интерфейса командной строки для включения режима пакетной фильтрации в конфигурации по умолчанию необходимо отключить режим управления сессиями:

fnpsh> session disable
Отключить управление сессиями? (Y/N) [N]: y
FNPSH-I-303C-Режим управления сессиями отключен
fnpsh>

В режиме пакетной фильтрации (рисунок 6.2) каждый пакет проверяется на соответствие правилам фильтрации, определенным в таблицах правил, в следующем порядке:

1) После получения пакета на один из фильтрующих интерфейсов ССПТ-2 производится идентификация пакета (рис.6.2, блок 1), в ходе которой определяется:

- тип принятого Ethernet-кадра;
- наличие и тип инкапсулированного протокола сетевого уровня;
- наличие и номер виртуальной локальной сети (ВЛВС), к которой принадлежит данный кадр;
- наличие и тип протокола транспортного уровня;

2) Производится обработка пакета в таблице MAC-правил (рис.6.2, блок 2), в ходе которой анализируются следующие параметры пакета:

- тип Ethernet-кадра;
- MAC-адреса отправителя и получателя;
- инкапсулированный протокол. Принимаются во внимание следующие поля заголовков: тип протокола в кадре Ethernet II; поле SSAP в кадре IEEE 802.3-LLC; поля OUI (код организации) и тип протокола в кадре IEEE 802.3-SNAP;
- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице MAC-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит

дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы (действие pass), – пакет передается на указанные в правиле выходные интерфейсы;

- в случае, если предписана дальнейшая обработка пакета (действие accept), – пакет передается на следующие уровни обработки в соответствии с типом инкапсулированного протокола: ARP пакет – в таблицу ARP-правил, IP пакет – в таблицы IP-правил, IPX пакет – в таблицы IPX-правил. Пакет, не содержащий протоколов ARP, IP или IPX, передается на указанные в MAC-правиле выходные интерфейсы без дальнейшей обработки;

3) В случае, если принятый пакет содержит протокол ARP, производится обработка пакета в таблице ARP-правил (рис.6.2, блок 3), в ходе которой анализируются следующие параметры пакета:

- MAC-адреса отправителя и получателя заголовка ARP;

- IP-адреса отправителя и получателя заголовка ARP;

- тип запроса;

- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице ARP-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы или дальнейшая обработка пакета (действия pass или accept)– пакет передается на указанные в правиле выходные интерфейсы;

Процедура обработки пакетов в режиме пакетной фильтрации

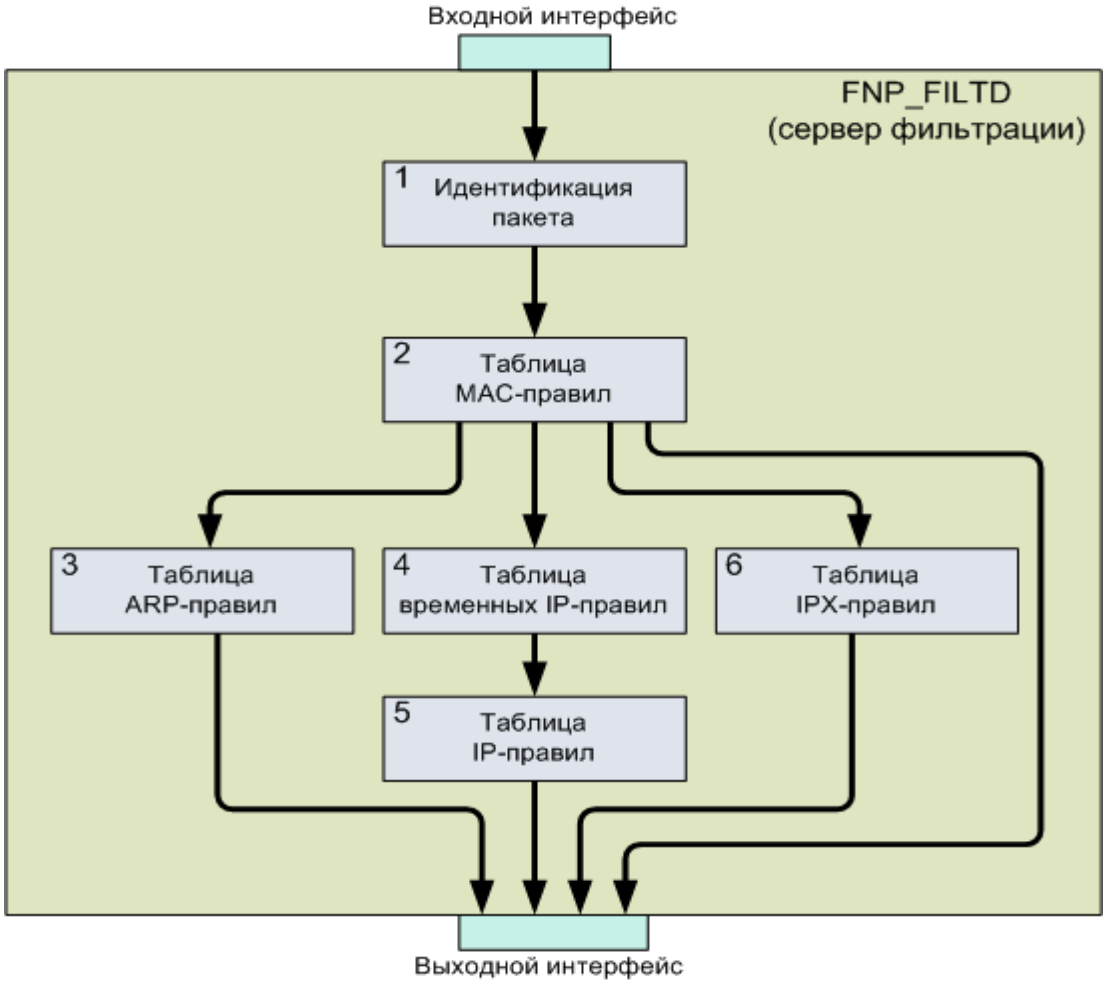

Рисунок 6.2

4) В случае, если принятый пакет содержит протокол IP, производится обработка пакета в таблице временных IP-правил (рис.6.2, блок 4), в ходе которой анализируются следующие параметры пакета:

- протокол транспортного уровня;
- IP-адреса отправителя и получателя;
- порты отправителя и получателя.

Если в результате обработки в таблице временных IP-правил выявляется правило, соответствующее данному пакету, этот пакет не передается ни на один из фильтрующих интерфейсов, и на этом обработка данного пакета заканчивается.

Таблица временных IP-правил может не содержать правил фильтрации. В этом случае пакет передается на обработку в таблицу IP-правил;

5) В ходе обработки пакета в таблице IP-правил (рис.6.2, блок 5) анализируются следующие параметры пакета:

- протокол транспортного уровня;
- IP-адреса отправителя и получателя;
- поле флагов заголовка IP пакета;
- поле типа сервиса заголовка IP пакета;
- поле времени жизни (TTL) заголовка IP пакета;
- длина IP пакета;
- TCP/UDP порты отправителя и получателя (при их наличии);
- тип и код ICMP-сообщения (при их наличии)
- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице IP-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;
- в случае, если предписана передача пакета на выходные интерфейсы или дальнейшая обработка пакета (действия pass или accept) – пакет передается на указанные в правиле выходные интерфейсы;

6) В случае, если принятый пакет содержит протокол IPX, производится обработка пакета в таблице IPX-правил (рис.6.2, блок 6), в ходе которой анализируются следующие параметры пакета:

- адреса сетей и хостов отправителя и получателя;
- тип пакета;
- сокеты отправителя и получателя;
- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице IPX-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы или дальнейшая обработка пакета (действия pass или accept)– пакет передается на указанные в правиле выходные интерфейсы.

В режиме пакетной фильтрации пакеты, обработанные сервером фильтрации, передаются на выходные интерфейсы без изменений.

6.1.2. Режим управления сессиями

Режим управления сессиями ССПТ-2 предназначен для дополнительной проверки пакетов на соответствие текущему состоянию сессии, к которой принадлежит данный пакет. Под сессией в дальнейшем понимается:

- для протокола TCP – виртуальное TCP-соединение;

- для протокола UDP – двусторонний обмен пакетами между клиентом и сервером;

- для протокола ICMP – обмен ICMP- сообщениями «Эхо-запрос» и «Эхо-ответ».

Для пакетов других протоколов управление сессиями не поддерживается. Такие пакеты передаются на выходные интерфейсы без создания сессии.

Использование режима управления сессиями дает следующие преимущества:

1) контроль хода виртуального TCP-соединения: каждый пакет проверяется на соответствие контексту данной сессии. При этом контролируются:

- флаги заголовка TCP: для различных состояний виртуального TCP-соединения определен свой возможный набор флагов;

- номера последовательностей и подтверждений заголовка TCP: для каждого пакета проверяется номер последовательности – он должен лежать в так называемом «окне приемника» TCP;

- неизменность параметров TCP-сессии (IP-адреса и номера портов);

2) контроль хода обмена пакетами по протоколу UDP: каждый пакет прове-

ряется на соответствие контексту данной сессии. При этом контролируется неизменность параметров UDP-сессии (IP-адреса и номеров портов);

3) контроль хода обмена ICMP-сообщениями «Эхо-запрос» и «Эхо-ответ»:: каждый пакет проверяется на соответствие контексту данной сессии. При этом контролируется неизменность параметров ICMP-сессии (IP-адреса, типы сообщений и идентификаторы запросов ICMP);

4) контроль данных прикладных протоколов;

5) возможность использования режима трансляции адресов:

6) блокировка атак, связанных с некорректной установкой флагов и номеров последовательностей протокола TCP;

7) автоматическое открытие клиентских портов, необходимых для текущей сессии;

8) создание одного правила для одного потока данных.

Режим управления сессиями по умолчанию включен в начальной конфигурации. При использовании интерфейса командной строки для того, чтобы включить режим управления сессиями, находясь в режиме пакетной фильтрации, необходимо использовать команду **session enable**:

```
fnpsh> session enable
FNPSH-I-303B-Режим управления сессиями включен
fnpsh>
```

Для того, чтобы просмотреть настройки режима управления сессиями, необходимо воспользоваться командой **session show**:

```
fnpsh> ses show
Управление сессиями:                          включено
Регистрация отброшенных пакетов:              отключено
Использование прикладных правил:              включено
Создание сессий для IP-правил по умолчанию:   включено
Использование данных канального уровня:       включено
Глубокий контроль TCP:                        включено
Размер таблицы сессий:                        8192
Тайм-ауты неактивности сессий (сек):
   Состояние TCP SYN:                         5 (по умолчанию)
   Состояние TCP ESTABLISED:                  86400 (по умолчанию)
```

Состояние TCP FIN: 600 (по умолчанию)
Состояние UDP SYN: 5 (по умолчанию)
Состояние TCP ESTABLISHED: 10 (по умолчанию)
Состояние ICMP SYN: 5 (по умолчанию)
Состояние ICMP ESTABLISHED: 20 (по умолчанию)
Обнаружение flood-атак: отключено
Генерация сообщения alarm: отключено
Пороговое значение для TCP (пакеты/сек): 800 (по умолчанию)
Пороговое значение для UDP (пакеты/сек): 1000 (по умолчанию)
Пороговое значение для ICMP (пакеты/сек): 100 (по умолчанию)
Время жизни временного IP правила (сек): 180 (по умолчанию)
Параметр регистрации временного IP-правила: отключено
Комментарий для временного IP правила: "Заблокированная flood атака"
fnpsh>

Сессии создаются на основе IP-правил в том случае, если это предписано соответствующей установкой правила. Каждое регулярное IP-правило имеет параметр session, в соответствии с которым создается или не создается сессия для пакетов, обработанных данным правилом. Параметр session IP-правила имеет следующие допустимые значения:

- **yes** или **ses**: сессии создаются по данному IP-правилу;

- **no** или **noses**: сессии не создаются по данному IP-правилу;

- **default** или **defses**: создание сессии по данному IP-правилу определяется глобальным параметром создания сессий по умолчанию для IP-правил.

Если пакет обработан глобальным IP-правилом, то необходимость создания сессии в этом случае определяется глобальным параметром создания сессии по умолчанию. При использовании интерфейса командной строки чтобы изменить глобальный параметр создания сессий по умолчанию, необходимо воспользоваться командой **session ip**:

fnpsh> session ip disable
Отключить создание сессий по умолчанию для IP-правил? (Y/N) [N]: y
FNPSH-I-3042-Сессии не будут создаваться по умолчанию для IP правил
fnpsh>
fnpsh>session ip enable
FNPSH-I-3041-Сессии будут создаваться по умолчанию для IP правил

fnpsh>

В начальной конфигурации сессии по умолчанию создаются для всех IP-правил.

В режиме управления сессиями пакеты проверяется на соответствие контексту сессии, к которой они принадлежат. В случае, если пакет не удовлетворяет контексту сессии, этот пакет удаляется (не передается ни на один выходной интерфейс). При этом возможна регистрация таких пакетов. При использовании интерфейса командной строки регистрация пакетов, отброшенных механизмом управления сессиями, включается командой **sssion log enable**:

fnpsh> session log enable
FNPSH-I-303D-Регистрация IP пакетов, отброшенных механизмом управления сессиямм, включена
fnpsh>

Для того, чтобы отключить регистрацию пакетов, отброшенных механизмом управления сессиями, необходимо воспользоваться командой sssion log disable:

fnpsh> session log disable
FNPSH-I-303E-Регистрация IP пакетов, отброшенных механизмом управления сессиямм, отключена
fnpsh>

В режиме управления сессиями пакеты должны быть отнесены к одной из существующих сессий. Такая принадлежность устанавливается на основании совпадения следующих параметров пакета и сессий:

- протокол транспортного уровня;
- ip-адреса отправителя и получателя;
- MAC-адреса отправителя и получателя;
- номер VLAN (при его наличии). VLAN, соответствующий потоку от клиента к серверу и VLAN, соответствующий потоку от сервера к клиенту, могут быть различны.
- номера портов отправителя и получателя (для протоколов TCP и UDP);
- идентификатор эхо-запроса для (протокола ICMP, утилита ping).

Данная проверка имеет следующие особенности:

- в режиме трансляции сетевых адресов не проверяется совпадение MAC-адресов;

- проверка MAC-адресов и номера VLAN может быть отключена командой **session mac disable** и включена командой **session mac enable.**

fnpsh> session mac disable
Отключить использование данных канального уровня? (Y/N) [N]: Y
FNPSH-I-304E-Использование данных канального уровня отключено
fnpsh>

fnpsh> session mac enable
FNPSH-I-304D-Использование данных канального уровня включено
fnpsh>

6.1.2.1 Обработка пакетов

В режиме управления сессиями пакеты проверяются (рис. 6.3) как на соответствие правилам фильтрации, определенным в таблицах правил, так и на соответствие контексту сессии, который хранится в таблице сессий, в следующем порядке (отличия от режима пакетного фильтра можно увидеть после обработки в таблице временных IP-правил):

1) После получения пакета на один из фильтрующих интерфейсов ССПТ-2 производится идентификация пакета (рис. 6.3, блок 1), в ходе которой определяется:

- тип принятого Ethernet-кадра;

- наличие и тип инкапсулированного протокола сетевого уровня;

- наличие и номер виртуальной локальной сети (ВЛВС), к которой принадлежит данный кадр;

- наличие и тип протокола транспортного уровня;

2) производится обработка пакета в таблице MAC-правил (рис. 6.3, блок 2), в ходе которой анализируются следующие параметры пакета:

- тип Ethernet-кадра;

- MAC-адреса отправителя и получателя;

- инкапсулированный протокол. Принимаются во внимание следующие поля заголовков: тип протокола в кадре Ethernet II; поле SSAP в кадре IEEE 802.3-LLC; поля OUI (код организации) и тип протокола в кадре IEEE 802.3-SNAP;

- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице MAC-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы (действие pass), – пакет передается на указанные в правиле выходные интерфейсы;

- в случае, если предписана дальнейшая обработка пакета (действие accept), – пакет передается на следующие уровни обработки в соответствии с типом инкапсулированного протокола: ARP пакет – в таблицу ARP-правил, IP пакет – в таблицы IP-правил, IPX пакет – в таблицы IPX-правил. Пакет, не содержащий протоколов ARP, IP или IPX, передается на указанные в MAC-правиле выходные интерфейсы;

3) В случае, если принятый пакет содержит протокол ARP, производится обработка пакета в таблице ARP-правил (рис. 6.3, блок 3), в ходе которой анализируются следующие параметры пакета:

- MAC-адреса отправителя и получателя заголовка ARP;

- IP-адреса отправителя и получателя заголовка ARP;

- тип запроса;

- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице ARP-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы или дальнейшая обработка пакета (действия pass или accept)– пакет передается на указанные в правиле выходные интерфейсы;

4) В случае, если принятый пакет содержит протокол IP, производится обработка пакета в таблице временных IP-правил (рис. 6.3, блок 4), в ходе которой анализируются следующие параметры пакета:

- протокол транспортного уровня;
- IP-адреса отправителя и получателя;
- порты отправителя и получателя.

Если в результате обработки в таблице временных IP-правил выявляется правило, соответствующее данному пакету, этот пакет не передается ни на один из фильтрующих интерфейсов, и на этом обработка данного пакета заканчивается.

Таблица временных IP-правил может не содержать правил фильтрации. В этом случае пакет передается на обработку механизму управления сессиями.

5) Механизм управления сессиями (рис. 6.3, блок 5) определяет, имеется ли в таблице сессия, соответствующая принятому пакету. Если такой сессии нет (данный пакет является первым пакетом в новом соединении), пакет отправляется на обработку в таблицу IP-правил. Если в таблице сессий имеется сессия, соответствующая принятому пакету, пакет отправляется на обработку в таблицу сессий.

Принадлежность пакета к той или иной сессии определяется:

- протоколом транспортного уровня;
- IP-адресами отправителя и получателя;
- портами отправителя и получателя (для протоколов TCP и UDP);
- идентификатором «Эхо-запроса» и «Эхо-ответа» (для протокола ICMP).

6) В ходе обработки пакета в таблице IP-правил (рис. 6.3, блок 6) анализируются следующие параметры пакета:

- протокол транспортного уровня;
- IP-адреса отправителя и получателя;
- поле флагов заголовка IP пакета;

- поле типа сервиса заголовка IP пакета;
- поле времени жизни (TTL) заголовка IP пакета;
- длину IP пакета;
- TCP/UDP порты отправителя и получателя (при их наличии);
- тип и код ICMP-сообщения (при их наличии);
- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице IP-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;
- в случае, если предписана передача пакета на выходные интерфейсы (действие pass) – пакет передаются на указанные в правиле выходные интерфейсы;
- в случае, если предписана дальнейшая обработка пакета (действие accept) – пакет или передается на обработку в таблицу прикладных правил (в случае, если включена фильтрация на прикладном уровне и в IP-правиле указан набор прикладных правил, по которым должна произойти дальнейшая обработка) или передается на указанные в правиле выходные интерфейсы.

В соответствии с параметром «Создание сессий» примененного IP-правила или глобальным параметром «Создание сессии по умолчанию» по данному пакету создается сессия (если соответствующие параметры это предписывают) в таблице сессий.

Процедура обработки пакетов в режиме управления сессиями

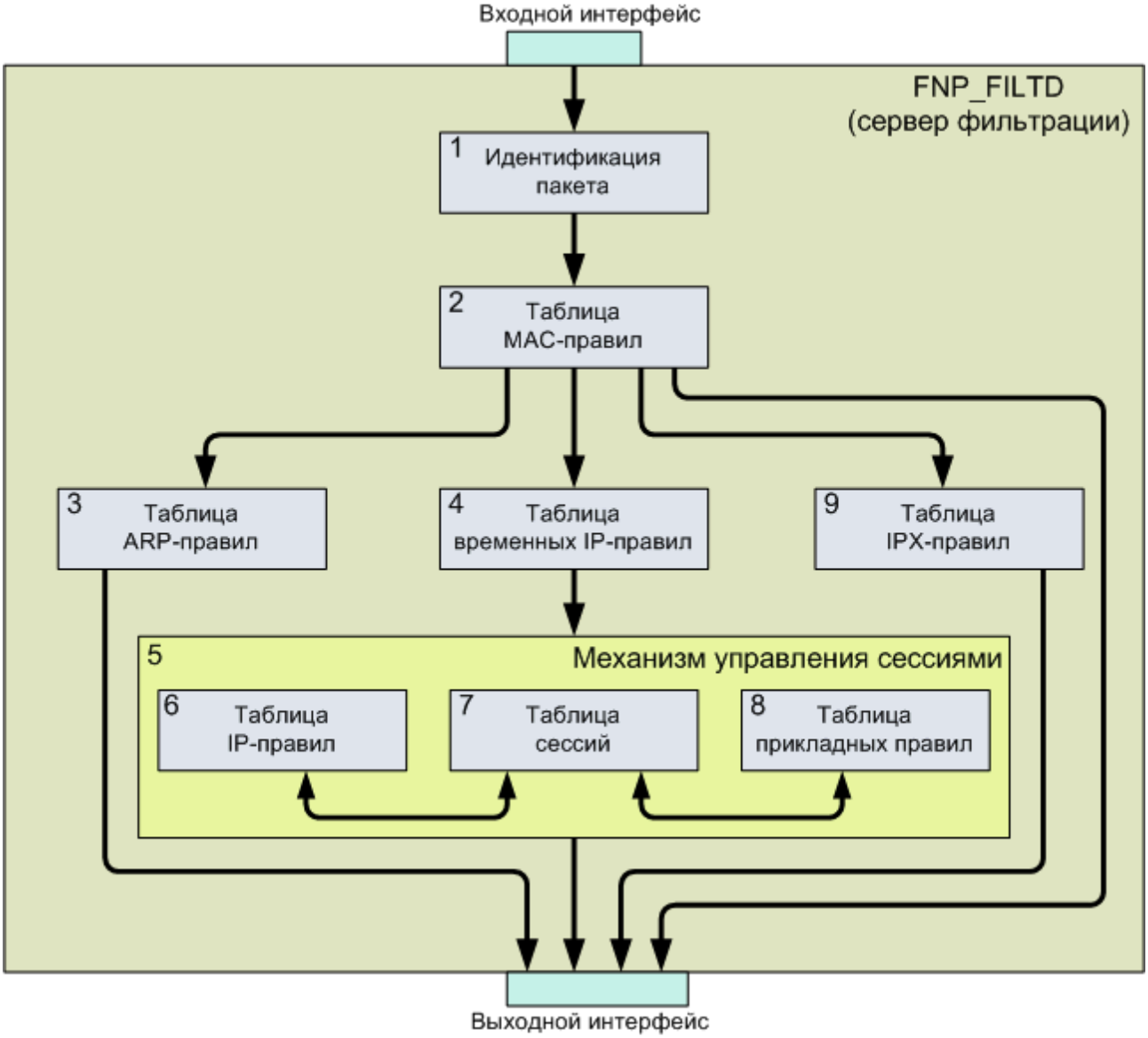

Рисунок 6.3

7) В ходе обработки пакета в таблице сессий (рис. 6.3, блок 7) анализируются на соответствие контексту сессии следующие параметры пакета:

- для протокола TCP – порты отправителя и получателя, флаги заголовка TCP, номера последовательностей и подтверждений, размер окна;

- для протокола UDP – порты отправителя и получателя;

- для протокола ICMP – идентификатор «Эхо-запроса» и «Эхо-ответа».

В случае, если хотя бы один параметр пакета не соответствует контексту сессии – данный пакет удаляется с диагностикой, указывающей на причину удаления.

В случае, если все параметры пакета соответствуют контексту сессии, данный пакет:

- отправляется на обработку в таблицу прикладных правил в случае, если включен параметр «Использование прикладных правил» и в IP-правиле, по которому создана сессия, определен набор прикладных правил для дальнейшей обработки;

- отправляется на выходные интерфейсы, если отключен параметр «Использование прикладных правил» или в IP-правиле, по которому создана сессия, не определен набор прикладных правил.

8) В ходе обработки в таблице прикладных правил (рис. 6.3, блок 8) к пакету последовательно применяются прикладные правила, перечисленные в IP-правиле, по которому создана сессия. В случае, если обнаруживается прикладное правило, применимое к данному пакету (т.е. все параметры прикладного правила соответствуют принятому пакету), выполняется действие, указанное в прикладном правиле. Для прикладных правил определены следующие действия:

- **accept** или **pass** – передача пакета на выходные интерфейсы;

- **drop** – удаление пакета и сессии, по которой обрабатывался пакет.

9) В случае, если принятый пакет содержит протокол IPX (рис. 6.3, блок 9), производится обработка пакета в таблице IPX-правил, в ходе которой анализируются следующие параметры пакета:

- адреса сетей и хостов отправителя и получателя;

- тип пакета;

- сокеты отправителя и получателя;

- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице IPX-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы или дальнейшая обработка пакета (действия pass или accept)– пакет передается на указанные в правиле выходные интерфейсы.

В режиме управления сессиями пакеты, обработанные сервером фильтрации, передаются на выходные интерфейсы без изменений.

6.1.2.2 Таблица сессий

Информация о текущих сессиях хранится в специальной структуре данных - **таблице сессий**. Оптимальный размер таблицы сессий определяется экспериментальным путем в зависимости от количества одновременно работающих сессий через данное устройство. Для нормальной работы достаточно таблицы, размер которой в два раза превосходит максимальное количество одновременно работающих сессий. В случае, если все записи таблицы будут заняты, запросы на добавление новых сессий в таблицу будут отвергаться путем удаления пакета с соответствующей диагностикой («Таблица сессий переполнена»). Минимальный размер таблицы сессий – 1024 записи, максимальный размер таблицы сессий – 65535 записей, размер таблицы сессий по умолчанию – 8192 записи. При использовании интерфейса командной строки чтобы изменить размер таблицы сессий, необходимо воспользоваться командой **session table size**:

fnpsh> session table size 16000
FNPSH-I-3049-Размер таблицы сессий изменен
fnpsh>

В таблице сессий хранится следующая информация для каждой текущей сессии:

- номер или индекс сессии;
- номер IP правила, в соответствии с которым была создана сессия;
- идентификатор ВЛВС (если таковой имеется или «-1», если нет);
- MAC-адреса отправителя и получателя;
- IP-адреса отправителя и получателя;
- входной и выходной интерфейсы;

- протоколы транспортного и прикладного уровней;

- номера портов отправителя и получателя для транспортного протокола (если таковые имеются);

- текущее состояние сессии;

- начальные номера последовательностей, текущие номера последовательностей и подтверждений, окна приемника и параметр масштабирования окна клиента и сервера для протокола TCP (если таковые имеются);

- идентификатор ICMP эхо-запроса и эхо-ответа (если таковые имеются);

- время начала сессии и время последней активности сессии;

- допустимый тайм-аут неактивности для сессии;

- количество пакетов и байт, переданных от клиента к серверу и обратно;

- параметры идентификации flood-атаки: время последней проверки и счетчик интенсивности пакетов в сессии;

- номера родительской или дочерней сессии (если таковые имеются);

- номер сработавшего прикладного правила (если таковой имеется);

- номер подставного порта или идентификатора ICMP эхо-запроса при работе в режиме трансляции сетевых адресов.

Работа таблицы сессий полностью автоматизирована и в общем случае не требует вмешательства администратора. Для того, чтобы посмотреть содержимое таблицы сессий, необходимо воспользоваться командой **session table show**. Результат выполнения данной команды представлен на рисунке 6.4.

Вывод команды session table show

Таблица сессий

Номер	IP-N	Тайм-аут	VLAN	Клиент	Сервер	Протоколы	Состояние	Пакеты
4	0	5	-1	0:195.208.113.155:520	1:195.208.113.159:520	udp/efs	SYN	1-0
27	10	86400	-1	1:195.208.113.119:60748	0:194.67.45.129:80	tcp/http	FINFINACK	5-4
48	10	4	-1	1:195.208.113.119:50177	0:80.68.240.131:80	tcp/unknown	SYN	1-0
137	10	86399	-1	1:195.208.113.119:60747	0:81.19.66.19:80	tcp/http	ESTABLISH	3-2
154	10	9	-1	1:195.208.113.119:55376	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
183	10	86399	-1	1:195.208.113.119:51531	0:82.204.218.9:80	tcp/http	ESTABLISH	4-2
184	10	86400	-1	1:195.208.113.119:52395	0:82.204.218.12:80	tcp/http	ESTABLISH	64-72
191	10	9	-1	1:195.208.113.119:64952	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
283	10	3	-1	1:195.208.113.119:60749	0:194.67.45.129:80	tcp/http	TIMEWAIT	5-5
385	10	86399	-1	1:195.208.113.119:61368	0:81.19.80.25:80	tcp/http	ESTABLISH	4-3
387	10	9	-1	1:195.208.113.119:49537	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
419	10	9	-1	1:195.208.113.119:57617	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
692	10	9	-1	1:195.208.113.119:63178	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
699	10	10	-1	1:195.208.113.119:63826	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
750	10	3	-1	1:195.208.113.119:64350	0:194.67.45.98:80	tcp/http	TIMEWAIT	5-5
934	10	9	-1	1:195.208.113.119:58619	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
940	10	9	-1	1:195.208.113.119:61147	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
1158	10	9	-1	1:195.208.113.119:50396	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
1198	10	9	-1	1:195.208.113.119:60460	0:194.85.4.53:53	udp/domain	ESTABLISH	1-1
1237	10	3	-1	1:195.208.113.119:49232	0:194.67.45.98:80	tcp/http	TIMEWAIT	5-5
1332	10	4	-1	1:195.208.113.119:49228	0:80.68.240.131:80	tcp/unknown	SYN	1-0

123456789 Выбрано/всего сессий: 33/33 Текущая/всего страниц: 1/2

N - отправка 0, F10 - выход

Рисунок 6.4

Вывод команды session table show имеет полноэкранный интерфейс и в реальном масштабе времени (обновление экрана каждые 5 секунд) выводит текущее содержимое основных полей таблицы сессий.

Администратор имеет возможность прервать текущую сессию, воспользовавшись, при использовании интерфейса командной строки, командой session table delete:

fnpsh> ses tab del 2537
Удалить сессию 2537? (Y/N) [N]: y
FNPSH-I-304B-Сессия удалена
fnpsh>

После удаления сессии из таблицы все пакеты, принадлежащие данной сессии и продолжающие поступать на фильтрующие интерфейсы ССПТ-2, будут удаляться (если по этим пакетам не может быть организована новая сессия). Новая сессия добавляется в таблицу (если это предписано IP-правилом, по которому обработан пакет, или глобальным параметром создания сессий по IP-правилам) при

получении пакета, удовлетворяющего следующим условиям:

- для протокола TCP – должен быть установлен флаг SYN и сброшены флаги ACK,FIN,RST,PUSH,URG ;

- для протокола UDP – без условий;

- для протокола ICMP – сообщение должно представлять собой ICMP «Эхо-запрос».

Также администратор может полностью очистить таблицу сессий командой session table clear:

fnpsh>session table clear
Очистить таблицу сессий? (Y/N) [N]: y
FNPSH-I-304A-Таблица сессий очищена
fnpsh>

Команда **session table clear** может использоваться с опцией **nolog**. В этом случае очистка таблицы сессий произойдет значительно быстрее, но сессии не будут зарегистрированы в журнале регистрации трафика.

fnpsh>session table clear nolog
Очистить таблицу сессий без регистрации? (Y/N) [N]: y
FNPSH-I-304A-Таблица сессий очищена без регистрации
fnpsh>

По мере получения пакетов каждая сессия проходит последовательно несколько стадий (состояний), различных для разных типов протоколов. Набор состояний, их описание и возможные переходы между ними для разных типов протоколов показаны в таблицах 6.1, 6.2, 6.3. В графе «Состояние» каждой из таблиц в скобках указаны наименование состояний, как они выглядят в выводе команды **session table show**.

Автоматическое удаление информации о сессии из таблицы может произойти в двух случаях:

1) соединение закрылось участниками в явном виде путем обмена соответствующими пакетами (характерно для протокола TCP);

2) сработал тайм-аут неактивности для сессии (характерно для протоколов UDP и ICMP). Это означает, что в течение определенного времени не прошло ни одного пакета, соответствующего данной сессии.

Периодически, каждые 10 секунд, таблица сессий проверяется на наличие неактивных сессий. Если во время этой проверки будут найдены неактивные сессии, они будут удалены с диагностикой «Завершение по тайм-ауту».

Численное значение тайм-аутов неактивности различно для разных протоколов и состояний. При использовании интерфейса командной строки для изменения тайм-аута неактивности по умолчанию служит команда **session timeout**. Аргументами этой команды являются имя протокола, фаза соединения, для которого необходимо поменять тайм-аут, и новое значение тайм-аута в секундах.

Например, команда смены тайм-аута неактивности для фазы ESTABLISHED протокола UDP выглядит следующим образом:

fnpsh> session timeout udp established <тайм_аут>
FNPSH-I-3044-Тайм-аут неактивности UDP сессии изменен
fnpsh>

Для протокола TCP определены 3 фазы соединения:

1) **syn** (синхронизация): соответствует состояниям SYN_RECEIVED и SYNACK_RECEIVED, определенным для TCP-сессии;

2) **established** (соединение установлено): соответствует состоянию ESTABLISHED, определенному для TCP-сессии;

3) **fin** (соединение закрывается): соответствует состояниям FIN1_RECEIVED, FIN2_RECEIVED, FIN1ACK1_RECEIVED, FIN2ACK1_RECEIVED определенным для TCP-сессии.

Тайм-аут неактивности для UDP сессий может быть установлен в пределах от 1 до 2147483647 секунд включительно.

Таблица 6.1 - Состояния TCP-сессии

Состояние	Тайм-аут по умолчанию (с)	Описание	Возможные переходы и их условия
SYN_RECEIVED (SYN)	5	Виртуальное TCP-соединение устанавливается - получен SYN-пакет от клиента	В состояние SYNACK_RECEIVED – при получении ответного SYN-пакета от сервера. В состояние CLOSED – при получении RST-пакета от сервера. В состояние CLOSED – после истечения тайм-аута неактивности.
SYNACK_RECEIVED (SYNACK)		Виртуальное TCP-соединение устанавливается - получен ответный SYN-пакет от сервера	В состояние ESTABLISHED – при получении ответного ACK-пакета от клиента, подтверждающего установление виртуального соединения. В состояние CLOSED – при получении RST-пакета от клиента. В состояние CLOSED – после истечения тайм-аута неактивности.
ESTABLISHED (ESTABLISH)	Глубокий анализ TCP включен – 3600 Глубокий анализ TCP выключен – 60	Виртуальное TCP-соединение установлено. В этом состоянии происходит передача данных прикладного уровня между клиентом и сервером	В состояние ESTABLISHED – при получении ACK-пакета от клиента или сервера. В состояние FIN1_RECEIVED при получении FIN-пакета от одного из участников соединения. В состояние RESET – при получении RST-пакета от одного из участников соединения. В состояние CLOSED – после истечения тайм-аута неактивности.

Продолжение таблицы 6.1

Состояние	Тайм-аут по умолчанию(с)	Описание	Возможные переходы и их условия
FIN1_RECEIVED (FIN)	Глубокий анализ TCP включен – 180 Глубокий анализ TCP выключен – таймаут отсутствует	Один из участников соединения прекратил передачу данных – от него получен FIN-пакет.	В состояние FIN1ACK1_RECEIVED – при получении ACK-пакета, подтверждающего присланный ранее FIN-пакет. В состояние FIN2_RECEIVED при получении FIN-пакета от другого участника соединения.
FIN1_RECEIVED (FIN) (продолжение)	Глубокий анализ TCP включен – 180 Глубокий анализ TCP выключен – таймаут отсутствует	Один из участников соединения прекратил передачу данных – от него получен FIN-пакет.	В состояние FIN2ACK1_RECEIVED – при получении FIN-пакета, являющегося одновременно ACK-пакетом, подтверждающим присланный ранее FIN-пакет. В состояние RESET – при получении RST-пакета от одного из участников соединения. В состояние CLOSED – после истечения тайм-аута неактивности.
FIN2_RECEIVED (FINFIN)	Глубокий анализ TCP включен – 180 Глубокий анализ TCP выключен – таймаут отсутствует	Оба участника соединения прекратили передачу данных - получены FIN-пакеты от обоих участников соединения, но ни один из них еще не подтвержден	В состояние FIN2ACK1_RECEIVED – при получении ACK-пакета, подтверждающего присланный ранее FIN-пакет. В состояние RESET – при получении RST-пакета от одного из участников соединения. В состояние CLOSED – после истечения тайм-аута неактивности.

Продолжение таблицы 6.1

Состояние	Тайм-аут по умолчанию(с)	Описание	Возможные переходы и их условия
FIN1ACK1_RECEIVED (FINACK)	Глубокий анализ TCP включен – 180 Глубокий анализ TCP выключен – таймаут отсутствует	Один из участников соединения прекратил передачу данных и второй участник подтвердил это – от него получен ACK-пакет.	В состояние FIN2ACK1_RECEIVED – при получении FIN-пакета от другого участника соединения. В состояние RESET – при получении RST-пакета от одного из участников соединения. В состояние CLOSED – после истечения тайм-аута неактивности.
FIN2ACK1_RECEIVED (FINFINACK)	Глубокий анализ TCP включен – 180 Глубокий анализ TCP выключен – таймаут отсутствует	Оба участника соединения прекратили передачу данных (получено по одному FIN пакету с каждой стороны) и один из участников подтвердил прекращение передачи	В состояние TIMEWAIT при получении ACK-пакета, подтверждающего закрытие соединения со второй стороны. В состояние RESET при получении RST-пакета от одного из участников соединения. В состояние CLOSED после истечения тайм-аута неактивности.
TIME_WAIT (TIMEWAIT)	3	Оба участника соединения прекратили передачу данных и подтвердили это. Ожидание запоздавших пакетов	В состояние CLOSED после истечения тайм-аута сессии.
RESET (RESET)	2	Один из участников соединения сбросил закрыл сессию путем отправки RST-пакета. Ожидание серии RST-пакетов (характерно для некоторых приложений)	В состояние CLOSED после истечения тайм-аута сессии.

Продолжение таблицы 6.1

Состояние	Тайм-аут по умолчанию(с)	Описание	Возможные переходы и их условия
CLOSED		Сессия закрыта	В состояние SYN_RECEIVED при получении SYN-пакета, открывающего новую сессию.

Для протоколов UDP и ICMP определены 2 фазы соединения:

1) **syn** (синхронизация): соответствует состояниям SYN_RECEIVED, определенному для UDP-и ICMP-сессий;

2) **established** (соединение установлено): соответствует состоянию ESTABLISHED, определенному для UDP-и ICMP-сессий.

Данные значения тайм-аутов являются значениями по умолчанию и используются в следующих случаях:

1) сессия создана по глобальному IP-правилу;

2) сессия создана по регулярному IP-правилу, параметр «тайм-аут сессии» которого предписывает использовать значения по умолчанию.

Механизм поиска неактивных сессий может быть отключен для отдельных сессий путем задания значения тайм-аута неактивности, равного нулю.

Таблица 6.2 - Состояния UDP-сессии

Состояние	Тайм-аут по умолчанию(с)	Описание	Возможные переходы и их условия
SYN_RECEIVED (SYN)	5	UDP-сессия устанавливается - получен пакет от клиента	В состояние SYN_RECEIVED при получении очередного пакета от клиента. В состояние ESTABLISHED при получении ответа от сервера.
ESTABLISHED (ESTABLISH)	10	UDP-сессия установлена - получен пакет от сервера	В состояние CLOSED после истечения тайм-аута неактивности.

Таблица 6.3 - Состояния ICMP-сессии

Состояние	Тайм-аут по умолчанию(с)	Описание	Возможные переходы и их условия
SYN_RECEIVED (SYN)	5	ICMP-сессия устанавливается - получен ICMP «Эхо-запрос» от клиента	В состояние SYN_RECEIVED при получении очередного «Эхо-запроса» от клиента. В состояние ESTABLISHED при получении ICMP «Эхо-ответа» от сервера.
ESTABLISHED (ESTABLISH)	20	ICMP-сессия установлена - получен ICMP «Эхо-ответ» от сервера.	В состояние CLOSED – после истечения тайм-аута неактивности.

В этом случае сессия не будет проверяться на неактивность и будет удалена из таблицы сессий только в случае явного закрытия соединения или по команде администратора. Например, чтобы, при использовании интерфейса командной строки, отключить проверку на неактивность всех TCP-сессий в состоянии ESTABLISHED, необходимо использовать следующую команду:

fnpsh> ses timeout tcp estab 0
Отключить проверку тайм-аута для TCP? (Y/N) [N]: y
FNPSH-I-3043-Таймаут неактивности TCP сессии изменен
fnpsh>

Тайм-аут неактивности для TCP сессий может быть установлен:

- для состояний SYN и FIN – в пределах от 1 до 2147483647 секунд включительно;

- для состояния ESTABLISHED – в пределах от 0 (тайм-аут неактивности отсутствует) до 2147483647 секунд включительно.

Внимание!!! Отключение механизма поиска неактивных сессий может привести к заполнению таблицы сессий и неработоспособности ССПТ-2. Данная опция рекомендуется к использованию только для TCP-сессий и только в случае осознанной необходимости.

6.1.2.3 Механизм обнаружения flood-атак

ССПТ-2 имеет встроенный механизм блокировки атак типа flood или «затоп-

ление» (например, SYN-flood или ICMP-flood). Данный вид атак связан с направлением потока пакетов высокой интенсивности на атакуемый хост, вследствие чего последний не имеет возможности нормально продолжать свое функционирование. ССПТ-2 способен обнаруживать и предотвращать такие атаки следующим образом:

1) постоянно контролируются значения интенсивности создания сессий (количество созданных сессий в секунду) и интенсивности пакетов в сессии (количество пакетов в секунду для каждой сессии);

2) в случае, если значение интенсивности создания сессий превысит некоторое пороговое значение, различное для различных протоколов, срабатывает механизм блокировки: в таблице сессий производится поиск IP-адресов, больше других участвующих в создании сессий, после чего в таблицу временных IP-правил добавляется правило, блокирующее доступ с/на эти адреса. Данная проверка осуществляется для протоколов TCP, UDP и ICMP;

3) в случае, если значение интенсивности пакетов в сессии превысит некоторое пороговое значение, различное для различных протоколов, срабатывает механизм блокировки: в таблицу временных IP-правил добавляется правило, блокирующее доступ с/на эти адреса. Данная проверка осуществляется для протоколов UDP и ICMP.

В настройках по умолчанию механизм блокировки flood-атак отключен. При использовании интерфейса командной строки для включения механизма блокировки flood-атак необходимо использовать команду **session flood enable** (режим управления сессиями должен быть включен):

fnpsh> session flood enable
FNPSH-I-30A3-Обнаружение flood-атак включено
fnpsh>

При использовании интерфейса командной строки для изменения пороговых значений интенсивности применяется команда **session flood threshold**, аргументами которой служат имя протокола и новое пороговое значение. Например, чтобы

установить пороговое значение в 2000 пакетов/секунду для протокола TCP, необходимо использовать следующую команду:

fnpsh> session flood threshold tcp 2000
FNPSH-I-30A5-Пороговое значение изменено
fnpsh>

При срабатывании механизма блокировки flood-атак в журнал регистрации событий заносится соответствующее предупреждение. Кроме этого для оперативного отображения возникшей ситуации имеется возможность регистрации предупреждения об атаке в системном журнале. При использовании интерфейса командной строки чтобы включить эту опцию, необходимо использовать команду **session flood alarm enable**:

fnpsh> session flood alarm enable
FNPSH-I-30A1-Сигнализация обнаружения flood-атак включена
fnpsh>

С помощью группы команд **session flood rule** имеется возможность устанавливать параметры временного IP-правила, которое создается для блокировки flood-атаки:

1) команда **session flood rule lifetime** задает время жизни временного IP-правила;

2) команда **session flood rule log** определяет параметр регистрации временного IP-правила (т.е. будут ли регистрироваться пакеты, подпадающие под данное временное IP-правило);

3) команда **session flood rule comments** задает комментарий для временного IP-правила.

6.1.2.4 Фильтрация на прикладном уровне

В ССПТ-2 определена функция фильтрации на прикладном уровне. Прикладные правила фильтрации содержатся в таблице прикладных правил (или AP-правил, от словосочетания Application Protocol). Таблица AP-правил по умолчанию пуста, глобального правила в таблице AP-правил нет. В настройках по умолчанию фильтрация на прикладном уровне отключена. Для того, чтобы воспользоваться

функцией фильтрации на прикладном уровне, необходимо:

1) включить параметр «Использование прикладных правил», при использовании интерфейса командной строки с помощью команды **session ap enable** (режим управления сессиями должен быть включен):

fnpsh> session ap enable
FNPSH-I-303F-Использование AP правил включено
fnpsh>

2) добавить прикладные правила в таблицу AP-правил;

3) для IP-правил определить перечень прикладных правил (параметр «Прикладные правила»), которые будут просматриваться при обработке пакета по соответствующим сессиям.

Обработка пакета механизмом управления сессиями в этом случае будет выглядеть следующим образом:

1) если пакет соответствует контексту сессии, проверяется, определен ли список прикладныех правил для IP-правила, по которому создана сессия;

2) если список прикладных правил определен, то пакет последовательно передается на обработку этим прикладным правилам до первого полного совпадения всех параметров. Если такое совпадение произошло, к пакету применяется данное AP-правило. Если для данного пакета совпадения не произошло, пакет передается на выходные интерфейсы;

3) если список прикладных правил не определен, то пакет передается на выходные интерфейсы.

Любой прикладной протокол может быть отфильтрован по следующим параметрам:

1) имя или номер прикладного протокола (в соответствии с RFC 1700). Для прикладных протоколов HTTP, SMTP, FTP, TELNET идентификация прикладного протокола происходит независимо от известного порта сервиса;

2) произвольная ASCII-строка длиной до 250 символов;

3) произвольные двоичные данные длиной до 16 байт по указанному смеще-

нию относительно начала прикладных данных или без указания смещения (в этом случае поиск происходит по всем прикладным данным пакета).

Кроме этого для некоторых прикладных протоколов определены дополнительные параметры, по которым возможна фильтрация:

1) для протокола HTTP:

- имя или фрагмент имени хоста (web-ресурса), к которому происходит обращение;

- метод HTTP-запроса;

- имя или фрагмент имени файла, запрашиваемого у HTTP-сервера.

2) для протокола FTP:

- имя (login) и пароль, предъявляемые пользователем при доступе на FTP-сервер;

- имя или фрагмент имени файла, запрашиваемого у FTP-сервера.

- команда протокола FTP;

3) для протокола SMTP:

- e-mail адреса или фрагменты адресов отправителя и получателя;

4) для протоколов распределенных СУБД:

- SQL-запросы или фрагменты запросов.

Внимание!!! В силу особенностей работы прикладных протоколов имеются ограничения на построение политики безопасности для протоколов SMTP и FTP. Для указанных протоколов невозможно построение политики типа «все, что не разрешено – запрещено».

6.1.3. Режим трансляции сетевых адресов

В режиме трансляции сетевых адресов (режим NAT – Network Address Translation) происходит подмена адресов и портов внутренней сети с целью

1) сокрытия структуры внутренней сети путем ограничения доступа из внешней сети – во внутреннюю сеть пропускаются только пакеты, принадлежащие к сессиям, уже находящимся в таблице сессий. Если для пакета из внешней сети не

находится сессии в таблице сессий (пакет – инициатор соединения), такой пакет удаляется (за исключением режима Переадресации);

2) экономии пространства IP-адресов – внутренняя сеть в данной реализации использует один внешний IP-адрес для обращения к ресурсам внешней сети.

В отличие от других режимов фильтрации в данном режиме фильтрующие интерфейсы отличаются по своему назначению:

1) интерфейс 0 (имя по умолчанию – eth0): внешний. К данному интерфейсу подключается внешняя сеть;

2) интерфейс 1 (имя по умолчанию – eth1): внутренний. К данному интерфейсу подключается внутренняя (защищаемая) сеть;

3) остальные интерфейсы (при их наличии): демилитаризованная зона (DMZ). К данному интерфейсу возможно подключение хостов, доступ к которым необходимо обеспечить как из внешней, так и из внутренней сети.

ССПТ-2 обеспечивает трансляцию адресов (передачу из внутренней сети во внешнюю и обратно) для следующих протоколов:

- TCP;
- UDP;
- ICMP-сообщения типа «Эхо-запрос» и «Эхо-ответ» .

Пакеты остальных протоколов не передаются из внутренней сети во внешнюю сеть и демилитаризованную зону и обратно.

Для перехода в режим трансляции сетевых адресов необходимо настроить следующие параметры ССПТ-2:

1) IP-адрес и маску подсети внутреннего интерфейса. Данный IP-адрес будет выступать в качестве шлюза по умолчанию для хостов внутренней сети. При использовании интерфейса командной строки для установки IP-адреса и маски внутреннего интерфейса необходимо воспользоваться командой **nat private ip**, например:

fnpsh> nat private ip 192.168.10.254/255.255.255.0
FNPSH-I-306E-IP адрес внутреннего интерфейса NAT изменен
fnpsh>

Данной командой для внутреннего интерфейса был установлен IP-адрес 192.168.10.254 и маска 255.255.255.0. Данный IP-адрес является виртуальным адресом, т.е. адресом, функционирующим только на уровне сервера фильтрации (FNP_FILTD). Это означает, что на фильтрующем интерфейсе eth1, который в режиме трансляции сетевых адресов является внутренним интерфейсом, по-прежнему не поднимается стек TCP/IP, т.е. устройство продолжает функционировать в невидимом режиме. Для использования во внутренней сети рекомендуется использовать специально выделенные для таких целей блоки частных IP-адресов для автономного использования:

- 10.0.0.0 – 10.255.255.255;
- 172.16.0.0 – 172.31.255.255;
- 192.168.0.0 – 192.168.255.255.

2) IP-адрес и маску подсети внешнего интерфейса. Данный IP-адрес будет использоваться в качестве адреса источника пакетов, передаваемых во внешнюю сеть. При использовании интерфейса командной строки для установки IP-адреса и маски внешнего интерфейса необходимо воспользоваться командой **nat public ip**, например:

fnpsh> nat public ip 195.208.10.1/255.255.255.224
FNPSH-I-306B-IP адрес внешнего интерфейса NAT изменен
fnpsh>

Данной командой для внешнего интерфейса был установлен IP-адрес 195.208.10.1 и маска 255.255.255.224. Данный IP-адрес является виртуальным адресом, т.е. адресом, функционирующим только на уровне сервера фильтрации (FNP_FILTD). Это означает, что на фильтрующем интерфейсе eth0, который в режиме трансляции сетевых адресов является внешним интерфейсом, по-прежнему не поднимается стек TCP/IP, т.е. устройство продолжает функционировать в невидимом режиме.

3) IP-адрес шлюза по умолчанию для внешнего интерфейса. Хост с данным IP-адресом будет использоваться в качестве шлюза по умолчанию для пакетов, от-

правляемых во внешнюю сеть. При использовании интерфейса командной строки для установки IP-адреса шлюза по умолчанию необходимо воспользоваться командой **nat public gateway**, например:

fnpsh> nat public gateway 195.208.10.30
FNPSH-I-306D-Адрес шлюза внешнего интерфейса NAT изменен
fnpsh>

Данной командой для внешнего интерфейса был установлен IP-адрес 195.208.10.30. Адрес шлюза по умолчанию должен находиться в одной IP-подсети с IP-адресом внешнего интерфейса.

4) MAC-адрес шлюза по умолчанию, который будет использоваться для формирования пакетов во внешнюю сеть через шлюз по умолчанию. В режиме трансляции сетевых адресов поддерживается статическая ARP-таблица, содержащая соответствия между IP-адресами и MAC-адресами внутренней и внешней локальной сети, а также демилитаризованной зоны. При использовании интерфейса командной строки для установки MAC-адреса шлюза по умолчанию необходимо добавить новую запись в ARP-таблицу с помощью команды **nat arp add**, указав фильтрующий интерфейс, через который доступен данный хост, его IP-адрес и MAC-адрес:

fnpsh> nat arp add eth0 195.208.10.30 c0:de:12:34:cc:ef
FNPSH-I-3074-Новая запись добавлена в ARP таблицу
fnpsh>

Внимание!!! Для корректной работы МЭ ССПТ-2 в локальных сетях не допускается установка на его сетевые интерфейсы в режиме NAT групповых MAC-адресов (групповой MAC-адрес это адрес, в котором первый бит старшего байта равен «единице» (1)).

После установки данных параметров на ССПТ-2 может быть включен режим трансляции адресов, для этого необходимо воспользоваться командой **nat enable** (при этом уже должен быть включен режим управления сессиями):

fnpsh> nat enable
FNPSH-I-3068-NAT включен
fnpsh>

Кроме приведенных выше обязательных параметров, которые должны быть

установлены при включении режима трансляции сетевых адресов, имеются дополнительные параметры настройки:

1) Возможны ситуации, когда пакеты удаляются в процессе трансляции адресов из-за невозможности передачи данного пакета на указанные выходные интерфейсы в данном режиме работы ССПТ-2 (например, ARP-пакеты не передаются из внутренней сети во внешнюю сеть и демилитаризованную зону). При использовании интерфейса командной строки для того, чтобы зарегистрировать такие пакеты в журнале регистрации пакетов, предусмотрена команда **nat log enable**:

fnpsh> nat log enable
FNPSH-I-3070-Регистрация пакетов, удаленных NAT, включена
fnpsh>

2) Для трансляции номера порта пакета, передаваемого из внутренней сети во внешнюю сеть или демилитаризованную зону, по умолчанию используется диапазон портов 45000-60000. При использовании интерфейса командной строки для изменения данного диапазона предусмотрена команда **nat port**:

fnpsh> nat port 30000-40000
Изменить диапазон портов NAT? (Y/N) [N]: y
FNPSH-I-306A-Диапазон портов NAT изменен. Необходимо перезапустить пакетный фильтр
fnpsh>

Допустимые значения для задания диапазона портов: 30000-65535.

3) Для работы в режиме трансляции сетевых адресов необходимо, чтобы ССПТ-2 отвечал на ARP-запросы к IP-адресам своих внутреннего и внешнего интерфейсов. По умолчанию в качестве MAC-адреса внешнего интерфейса используется значение 02:01:01:01:01:01, в качестве MAC-адреса внутреннего интерфейса используется значение 02:01:01:01:01:02. При этом данные значения используются только сервером фильтрации FNP_FILTD для обеспечения заданного режима работы, т.е. не устанавливаются в качестве MAC-адресов фильтрующих интерфейсов eth0 и eth1. При использовании интерфейса командной строки для изменения MAC-адреса внешнего интерфейса предназначена команда **nat public mac**:

fnpsh> nat public mac 03:12:01:02:02:02
FNPSH-I-3072-MAC адрес внешнего интерфейса NAT изменен
fnpsh>

При использовании интерфейса командной строки для изменения MAC-адреса внутреннего интерфейса предназначена команда **nat private mac**:

fnpsh> nat private mac 03:12:01:03:03:03
FNPSH-I-3072-MAC адрес внутреннего интерфейса NAT изменен
fnpsh>

Во избежание временной потери связности данные команды рекомендуется выполнять при отключенном режиме трансляции сетевых адресов.

При использовании интерфейса командной строки для просмотра параметров настройки режима трансляции сетевых адресов предназначена команда **nat show**:

fnpsh> nat show
Трансляция сетевых адресов (NAT): включено
Регистрация отброшенных пакетов: включено
Аутентификация пользователей: отключено
Тайм-аут неактивности пользователей(сек): 600
Диапазон портов: 30000-40000
Внешний интерфейс: eth0
  MAC-адрес: 02:01:01:01:01:01
  IP-адрес: 195.208.10.1
  Маска подсети: 255.255.255.224
  IP-адрес шлюза по умолчанию: 195.208.10.30
  Переадресация: отключено
Внутренний интерфейс: eth1
  MAC-адрес: 02:01:01:01:01:02
  IP-адрес: 192.168.10.254
  Маска подсети: 255.255.255.0
Интерфейсы DMZ: eth2
  Переадресация: отключено
fnpsh>

Пример подключения сегментов сети к ССПТ-2 в режиме трансляции сетевых адресов с приведенными выше основными параметрами представлен на рисунке 6.5.

На рисунке 6.5 к интерфейсу eth1 ССПТ-2 подключена внутренняя сеть с ад-

ресами 192.168.10.1 – 192.168.10.253. Адрес 192.168.10.254 используется хостами во внутренней сети в качестве шлюза по умолчанию. К интерфейсам eth2 и eth3 подключается демилитаризованная зона, в которой могут использоваться адреса 195.208.10.2 – 195.208.10.29 и шлюз по умолчанию 195.208.10.30. К интерфейсу eth0 подключается внешний шлюз по умолчанию 195.208.10.30. Трансляция сетевых адресов в этом случае будет проходить следующим образом (рисунок 6.6).

Предположим, что хост из внутренней сети с IP-адресом 192.168.10.13 и MAC-адресом 01:18:C0:D5:FE:19 отправляет запрос к HTTP серверу с IP-адресом 200.13.18.3, находящемуся во внешней сети. В этом случае на интерфейс eth1 ССПТ-2 поступит пакет со следующими параметрами:

1) MAC-адрес источника: 01:18:C0:D5:FE:19;

2) MAC-адрес приемника: 02:01:01:01:01:02 (MAC-адрес по умолчанию внутреннего интерфейса ССПТ-2);

3) IP-адрес источника: 192.168.10.13;

4) IP-адрес приемника: 200.13.18.3;

5) TCP-порт источника: 1026;

6) TCP-порт приемника: 80 (обращение к HTTP-серверу).

После обработки (трансляции сетевых адресов) через интерфейс eth0 ССПТ-2 в адрес внешнего шлюза по умолчанию будет отправлен пакет со следующими параметрами:

1) MAC-адрес источника: 02:01:01:01:01:01 (MAC-адрес по умолчанию внешнего интерфейса ССПТ-2);

2) MAC-адрес приемника: c0:de:12:34:cc:ef (MAC-адрес внешнего шлюза по умолчанию, который был установлен ранее при настройке параметров режима трансляции сетевых адресов);

3) IP-адрес источника: 195.208.10.1 (IP-адрес внешнего интерфейса ССПТ-2);

4) IP-адрес приемника: 200.13.18.3 (IP-адрес HTTP-сервера, остается без изменения);

Подключение ССПТ-2 в режиме трансляции сетевых адресов

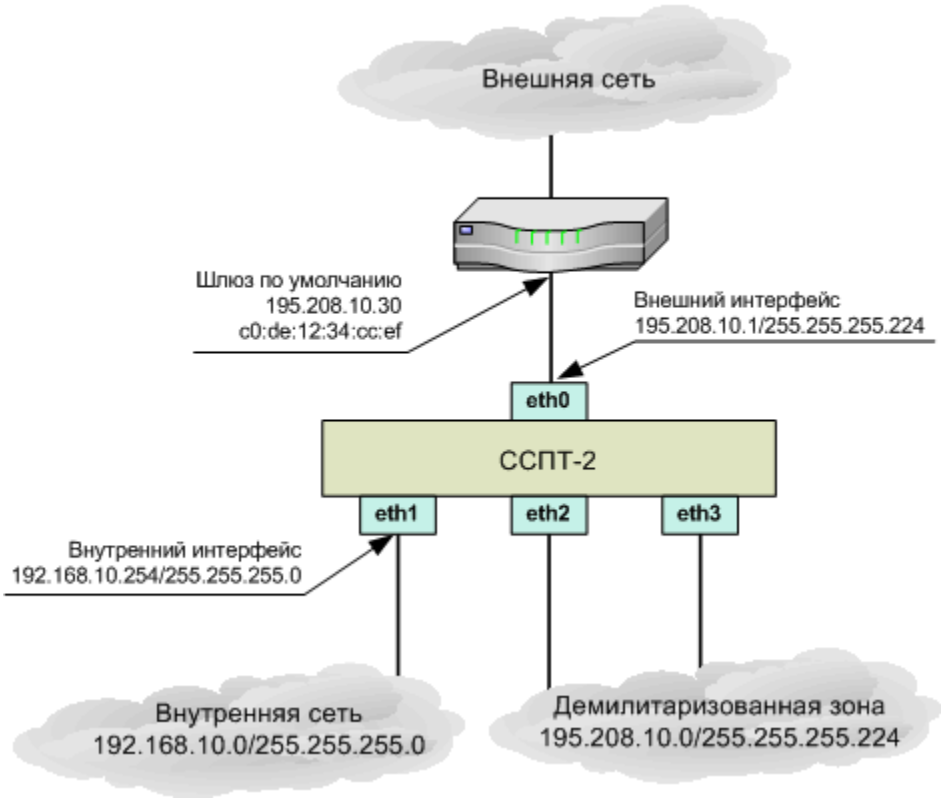

Рисунок 6.5

5) TCP-порт источника: 45000 (значение из диапазона портов, используемых для трансляции);

6) TCP-порт приемника: 80 (порт HTTP-сервера, остается без изменения).

Ответный пакет от HTTP-сервера, который поступит на интерфейс eth0 ССПТ-2, будет содержать следующие параметры:

1) MAC-адрес источника: c0:de:12:34:cc:ef (MAC-адрес внешнего шлюза по умолчанию);

2) MAC-адрес приемника: 02:01:01:01:01:01 (MAC-адрес по умолчанию внешнего интерфейса ССПТ-2);

3) IP-адрес источника: 200.13.18.3 (IP-адрес адрес HTTP-сервера);

4) IP-адрес приемника: 195.208.10.1 (IP-адрес внешнего интерфейса ССПТ-2);

5) TCP-порт источника: 80 (порт HTTP-сервера);

6) TCP-порт приемника: 45000 (значение порта, используемое в данной сессии).

Трансляция адресов при обмене пакетами с хостом из внешней сети

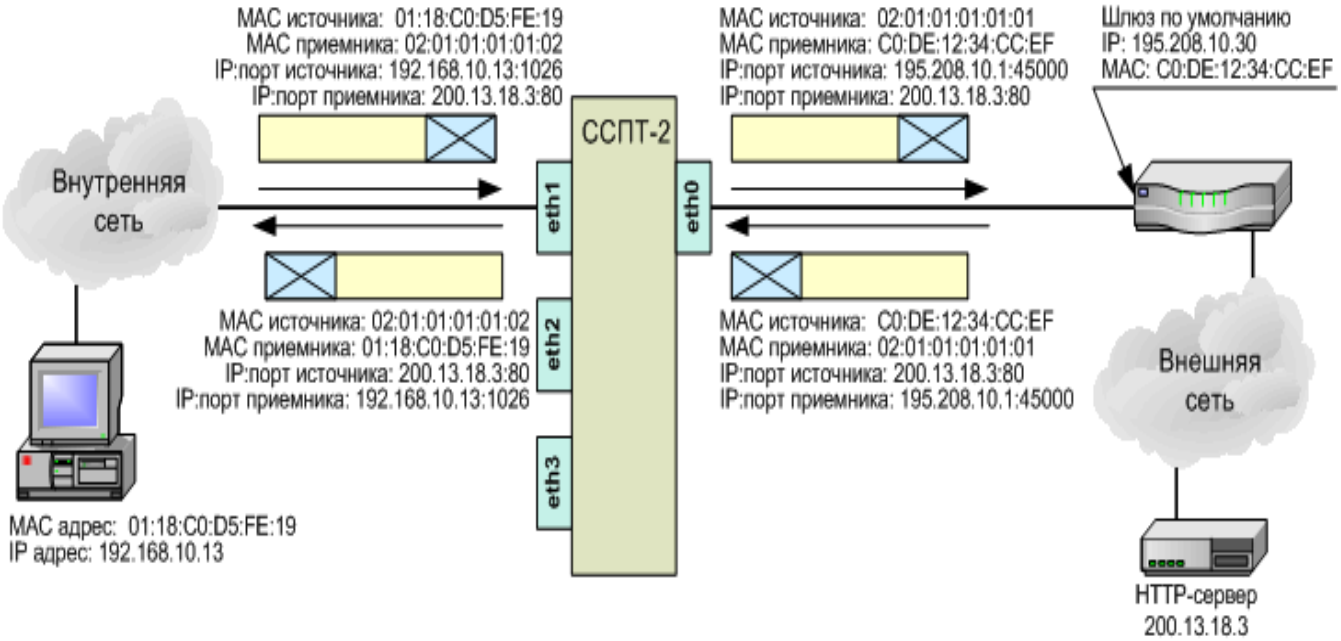

Рисунок 6.6

После обратной трансляции адресов через интерфейс eth1 во внутреннюю сеть будет отправлен пакет со следующими параметрами:

1) MAC-адрес источника: 02:01:01:01:01:02 (MAC-адрес по умолчанию внутреннего интерфейса ССПТ-2);

2) MAC-адрес приемника: 01:18:C0:D5:FE:19 (MAC-адрес хоста из внутренней сети, отправившего запрос на HTTP-сервер);

3) IP-адрес источника: 200.13.18.3 (IP-адрес адрес HTTP-сервера, остается без изменений);

4) IP-адрес приемника: 192.168.10.13 (IP-адрес хоста из внутренней сети, отправившего запрос на HTTP-сервер);

5) TCP-порт источника: 80 (ответ от HTTP-сервера);

6) TCP-порт приемника: 1026 (порт, с которого был отправлен запрос).

6.1.3.1. Процедура обработки пакетов

В режиме трансляции сетевых адресов пакеты при передаче из внутренней во внешнюю сеть и демилитаризованную зону (и обратно) помимо проверки механизмом управления сессиями подвергаются подмене MAC-адресов источника и приемника, IP-адресов источника и приемника, а также портов источника и приемника для протоколов TCP и UDP либо идентификатора последовательности для протокола ICMP. Процедура обработки пакета в этом случае выглядит следующим образом (рис.6.7):

1) После получения пакета на один из фильтрующих интерфейсов ССПТ-2 производится идентификация пакета (рис.6.7, блок 1), в ходе которой определяется:

- тип принятого Ethernet-кадра;

- наличие и тип инкапсулированного протокола сетевого уровня;

- наличие и номер виртуальной локальной сети (ВЛВС), к которой принадлежит данный кадр;

- наличие и тип протокола транспортного уровня;

2) Производится обработка пакета в Таблице MAC-правил (рис.6.7, блок 2), в ходе которой анализируются следующие параметры пакета:

- тип Ethernet-кадра;

- MAC-адреса отправителя и получателя;

- инкапсулированный протокол. Принимаются во внимание следующие поля заголовков: тип протокола в кадре Ethernet II; поле SSAP в кадре IEEE 802.3-LLC; поля OUI (код организации) и тип протокола в кадре IEEE 802.3-SNAP;

- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице MAC-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы (дей-

ствие pass), – пакет передается в блок 14 с целью проверки выходных интерфейсов и, по результатам проверки в блоке 14, на выходные интерфейсы;

- в случае, если предписана дальнейшая обработка пакета (действие accept), – пакет передается на следующие уровни обработки в соответствии с типом инкапсулированного протокола: ARP пакет – в таблицу ARP-правил, IP пакет – в таблицы IP-правил, IPX пакет – в таблицы IPX-правил. Пакет, не содержащий протоколов ARP, IP или IPX, передается в блок 14 с целью проверки выходных интерфейсов и, по результатам проверки в блоке 14, на выходные интерфейсы;

3) В случае, если принятый пакет содержит протокол ARP, производится обработка пакета в Таблице ARP-правил (рис. 6.7, блок 3), в ходе которой анализируются следующие параметры пакета:

- MAC-адреса отправителя и получателя заголовка ARP;
- IP-адреса отправителя и получателя заголовка ARP;
- тип запроса;
- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице ARP-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы или дальнейшая обработка пакета (действия pass или accept) – пакет передается в один из блоков:

- 4 (в случае, если ARP-пакет поступил на внутренний интерфейс);

- 5 (в случае, если ARP-пакет поступил на внешний интерфейс) для дальнейшей обработки;

4) ARP-пакеты из внутренней сети обрабатываются (рис. 6.7, блок 4) следующим образом:

- если это ARP-запрос к IP-адресу внутреннего интерфейса, генерируется

ARP-ответ от имени IP-адреса внутреннего интерфейса с указанием MAC-адреса внутреннего интерфейса (значение по умолчанию – 02:01:01:01:01:02) и отсылается во внутреннюю сеть;

- во всех остальных случаях ARP-пакет удаляется (не передается ни на один фильтрующий интерфейс);

Внимание!!! ARP-пакеты из внутренней сети не передаются во внешнюю сеть и демилитаризованную зону;

5) ARP-пакеты из внешней сети и из демилитаризованной зоны обрабатываются (рис. 6.7, блок 5) следующим образом:

- если это ARP-запрос к IP-адресу внешнего интерфейса, генерируется ARP-ответ от имени IP-адреса внешнего интерфейса с указанием MAC-адреса внешнего интерфейса (значение по умолчанию – 02:01:01:01:01:01) и отсылается на тот интерфейс, с которого был принят ARP-запрос;

- во всех остальных случаях ARP-пакет передается на указанные выходные интерфейсы за исключением внутреннего интерфейса (через блок 14, исключающий внутренний интерфейс из списка выходных).

Внимание!!! ARP-пакеты из внешней сети и демилитаризованной зоны не передаются во внутреннюю сеть.

6) В случае, если принятый пакет содержит протокол IP, производится обработка пакета в таблице временных IP-правил (рис. 6.7, блок 6), в ходе которой анализируются следующие параметры пакета:

- протокол транспортного уровня;

- IP-адреса отправителя и получателя;

- порты отправителя и получателя.

Если в результате обработки в таблице временных IP-правил выявляется правило, соответствующее данному пакету, этот пакет не передается ни на один из фильтрующих интерфейсов, и на этом обработка данного пакета заканчивается.

7) Механизм управления сессиями (рис.6.7, блок 7) выполняет следующие действия:

а) Выявление пакетов, запрещенных к передаче из внутренней во внешнюю сеть и демилитаризованную зону. К таким пакетам относятся следующие пакеты, принятые на внутренний интерфейс:

- IP-пакеты с адресом источника, не принадлежащим внутренней IP-сети;

- IP-пакеты с адресом приемника, принадлежащим внутренней IP-сети;

- IP-пакеты с адресом приемника, равным IP-адресу внутреннего или внешнего интерфейса ССПТ-2;

- IP-пакеты, не содержащие один из протоколов: TCP, UDP или ICMP «Эхо-запрос»;

- Фрагментированные IP-пакеты.

Пакеты, удовлетворяющие одному из приведенных выше условий, удаляются (не передаются ни на один фильтрующий интерфейс);

Таблица временных IP-правил может не содержать правил фильтрации. В этом случае пакет сразу передается на обработку Механизму управления сессиями

б) Выявление пакетов, предназначенных для передачи во внутреннюю сеть для последующего Преобразования к виду внутренней сети. К таким пакетам относятся следующие пакеты, принятые на внешний интерфейс или интерфейсы демилитаризованной зоны:

- IP-пакеты с адресом приемника, равным IP-адресу внешнего интерфейса ССПТ-2 и принадлежащие ранее открытой сессии;

- IP-пакеты с адресом приемника, равным IP-адресу внешнего интерфейса ССПТ-2 и удовлетворяющие одной из записи в таблице переадресации (п. 6.1.3.3) в том случае, если переадресация с интерфейса, на который был получен данный пакет, разрешена;

Пакеты, удовлетворяющие приведенным выше условиям, передаются на обработку в блок Преобразования пакетов к виду внутренней сети. Пакеты, принятые на внешнем интерфейсе или на интерфейсах демилитаризованной зоны и не удовлетворяющие данным условиям, удаляются (не передаются ни на один фильтрующий интерфейс). После обработки в блоке Преобразования пакетов к виду внут-

ренней сети пакеты продолжают обрабатываться механизмом управления сессиями с этой точки;

Процедура обработки пакетов в режиме трансляции сетевых адресов

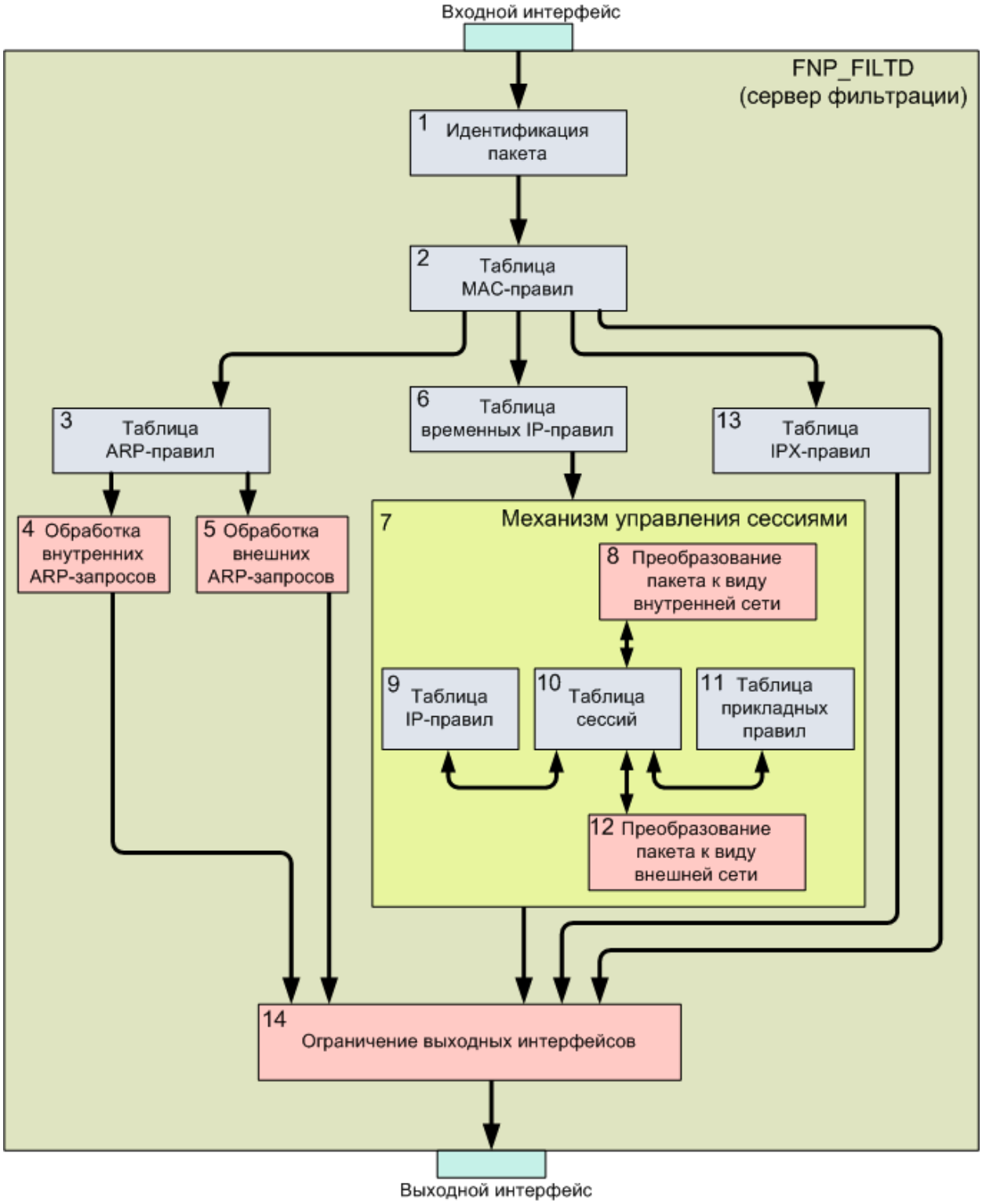

Рисунок 6.7

в) Определение наличия в таблице сессий сессии, соответствующей принятому пакету. Если такой сессии нет (данный пакет является первым пакетом в новом соединении), пакет отправляется на обработку в Таблицу IP-правил. Если в таблице сессий имеется сессия, соответствующая принятому пакету, пакет отправляется на обработку в Таблицу сессий.

Принадлежность пакета к той или иной сессии определяется:

- протоколом транспортного уровня;

- IP-адресами отправителя и получателя;

- портами отправителя и получателя (для протоколов TCP и UDP);

- идентификатором «Эхо-запроса» и «Эхо-ответа» (для протокола ICMP);

г) Выявление пакетов, предназначенных для передачи во внешнюю сеть или демилитаризованную зону, для последующего Преобразования к виду внешней сети. К таким пакетам относятся пакеты, принадлежащие установленной ранее сессии.

Пакеты, удовлетворяющие приведенному выше условию, передаются на обработку в блок Преобразования пакетов к виду внешней сети. Пакеты, не удовлетворяющие приведенному условию на данном этапе обработки, удаляются (не передаются ни на один фильтрующий интерфейс). После обработки в блоке Преобразования пакетов к виду внешней сети пакеты передаются в блок Ограничения выходных интерфейсов для последующей передачи на выходные интерфейсы;

8) В ходе обработки пакета в блоке Преобразования пакетов (рис.6.7, блок 8) к виду внутренней сети пакеты преобразуются к виду внутренней сети следующим образом:

- если пакет принадлежит открытой ранее сессии, информация о внутреннем хосте (его MAC-адрес, IP-адрес и номер порта для TCP и UDP либо идентификатор последовательности для ICMP) извлекается из информации о данной сессии, хранящейся в таблице сессий;

- если пакет соответствует одному из правил Переадресации, информация о IP-адресе и TCP-порте внутреннего хоста извлекается из соответствующего прави-

ла переадресации, информация о MAC-адресе внутреннего хоста извлекается из ARP-таблицы ССПТ-2.

Используя полученную информацию, производится подмена следующих параметров пакета:

- MAC-адрес источника подменяется на MAC-адрес внутреннего интерфейса ССПТ-2;

- MAC-адрес приемника подменяется на полученный MAC-адрес внутреннего хоста;

- IP-адрес приемника подменяется на полученный IP-адрес внутреннего хоста;

- порт приемника (для TCP или UDP) подменяется на полученный номер порта внутреннего хоста;

- идентификатор последовательности (для ICMP) подменяется на полученный идентификатор последовательности внутреннего хоста.

-После данной процедуры пересчитываются контрольные суммы заголовков IP, TCP, UDP или ICMP в зависимости от протокола.

9) В ходе обработки пакета в Таблице IP-правил (рис.6.7, блок 9) анализируются следующие параметры пакета:

- протокол транспортного уровня;

- IP-адреса отправителя и получателя;

- поле флагов заголовка IP пакета;

- поле типа сервиса заголовка IP пакета;

- поле времени жизни (TTL) заголовка IP пакета;

- длину IP пакета;

- TCP/UDP порты отправителя и получателя (при их наличии);

- тип и код ICMP-сообщения (при их наличии)

- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице IP-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит

дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы (действие pass) – устанавливаются выходные интерфейсы и пакет возвращается Механизму управления сессиями для последующей обработки;

- в случае, если предписана дальнейшая обработка пакета (действие accept) – пакет или передается на обработку в Таблицу прикладных правил (в случае, если включена фильтрация на прикладном уровне и в IP-правиле указан набор прикладных правил, по которым должна произойти дальнейшая обработка) или устанавливаются выходные интерфейсы и пакет возвращается Механизму управления сессиями для последующей обработки.

В соответствии с параметром «Создание сессий» примененного IP-правила или глобальным параметром «Создание сессии по умолчанию» по данному пакету создается сессия (если соответствующие параметры это предписывают) в таблице сессий.

Внимание!!! Сессии должны обязательно создаваться для передачи пакетов из внутренней во внешнюю сеть и демилитаризованную зону и обратно;

10) В ходе обработки пакета в Таблице сессий (рис.6.7, блок 10) анализируются на соответствие контексту сессии следующие параметры пакета:

- для протокола TCP – порты отправителя и получателя, флаги заголовка TCP, номера последовательностей и подтверждений, размер окна;

- для протокола UDP – порты отправителя и получателя;

- для протокола ICMP – идентификатор «Эхо-запроса» и «Эхо-ответа».

В случае, если хотя бы один параметр пакета не соответствует контексту сессии – данный пакет удаляется с диагностикой, указывающей на причину удаления. В случае, если все параметры пакета соответствуют контексту сессии, данный пакет:

- отправляется на обработку в Таблицу прикладных правил в случае, если

включен параметр «Использование прикладных правил» и в IP-правиле, по которому создана сессия, определен набор прикладных правил для дальнейшей обработки;

- устанавливаются выходные интерфейсы и пакет возвращается Механизму управления сессиями для последующей обработки, если отключен параметр «Использование прикладных правил» или в IP-правиле, по которому создана сессия, не определен набор прикладных правил.

11) В ходе обработки в Таблице прикладных правил (рис.6.7, блок 11) к пакету последовательно применяются прикладные правила, перечисленные в IP-правиле, по которому создана сессия. В случае, если обнаруживается прикладное правило, применимое к данному пакету (т.е. все параметры прикладного правила соответствуют принятому пакету), выполняется действие, указанное в прикладном правиле. Для прикладных правил определены следующие действия:

- **accept** или **pass** – устанавливаются выходные интерфейсы и пакет возвращается Механизму управления сессиями для последующей обработки;

- **drop** – удаление пакета и сессии, по которой обрабатывался пакет;

12) В ходе обработки пакета в блоке Преобразования пакетов к виду внешней сети (рис.6.7, блок 12) пакеты преобразуются к виду внешней сети следующим образом:

- из ARP-таблицы извлекается необходимый MAC-адрес приемника, соответствующий IP-адресу приемника;

- если пакет является первым пакетом в сессии (инициирующий пакет), для данной сессии выделяется значение подставного порта (для TCP и UDP) или идентификатора последовательности (для ICMP «Эхо-запроса»);

- если пакет не является первым пакетом в сессии, информация о значении подставного порта (для TCP и UDP) или идентификатора последовательности (для ICMP) извлекается из информации о сессии в таблице сессий.

Используя полученную информацию, производится подмена следующих параметров пакета:

- MAC-адрес источника подменяется на MAC-адрес внешнего интерфейса ССПТ-2;

- MAC-адрес приемника подменяется на полученный MAC-адрес;

- IP-адрес источника подменяется на IP-адрес внешнего интерфейса;

- порт источника (для TCP или UDP) подменяется на полученное значение подставного порта;

- идентификатор последовательности (для ICMP) подменяется на полученное значение подставного идентификатора последовательности.

После данной процедуры пересчитываются контрольные суммы заголовков IP, TCP, UDP или ICMP в зависимости от протокола.

13) В случае, если принятый пакет содержит протокол IPX, производится обработка пакета в Таблице IPX-правил (рис.6.7, блок 13), в ходе которой анализируются следующие параметры пакета:

- адреса сетей и хостов отправителя и получателя;

- тип пакета;

- сокеты отправителя и получателя;

- номер ВЛВС, к которой принадлежит данный кадр.

В результате обработки в таблице IPX-правил выявляется правило, соответствующее данному пакету. В соответствии с действием этого правила происходит дальнейшая обработка пакета:

- в случае, если предписано удаление пакета (действие drop), - пакет не передается ни на один из фильтрующих интерфейсов;

- в случае, если предписана передача пакета на выходные интерфейсы или дальнейшая обработка пакета (действия pass или accept) – пакет передается в блок Ограничения выходных интерфейсов.

14) Блок Ограничения выходных интерфейсов необходим для того, чтобы:

- ограничить выходные интерфейсы пакетов с транслированными адресами только интерфейсом, через который доступен адресат данного пакета;

- не допустить передачу во внутреннюю сеть пакетов, не прошедших транс-

ляцию адресов.

6.1.3.2. Статическая ARP-таблица

Для того, чтобы обеспечить обмен пакетами между внутренней сетью и хостами в демилитаризованной зоне или хостами, расположенными до шлюза по умолчанию с адресами из IP-подсети внешнего интерфейса, необходимо прописать соответствие между IP-адресами и MAC-адресами данных хостов. Для хранения этих записей предназначена статическая ARP-таблица ССПТ-2.

Внимание!!! Статическая ARP-таблица не может содержать несколько записей с одинаковыми IP-адресами.

Работа со статической ARP-таблицей осуществляется с помощью группы команд **nat arp**. Например (рисунок 6.8), если необходимо обеспечить взаимодействие хостов внутренней сети с SMTP-сервером, подключенным к интерфейсу Eth3 демилитаризованной зоны и с WEB-сервером, доступным через внешний интерфейс eth0 и расположенным до шлюза по умолчанию, то при использовании интерфейса командной строки необходимо использовать команду **nat arp add**:

```
fnpsh> nat arp add eth3 195.208.10.11 00:c0:ab:cf:6d:12
FNPSH-I-3074-Новая запись добавлена в ARP таблицу
fnpsh> nat arp add eth0 195.208.10.20 00:c0:ab:e7:18:dc
FNPSH-I-3074-Новая запись добавлена в ARP таблицу
fnpsh>
```

При использовании интерфейса командной строки для просмотра содержимого статической ARP-таблицы используется команда **nat arp show**:

```
fnpsh> nat arp show viewer=no
Интерфейс      IP-адрес       MAC-адрес
eth0           195.208.10.30  c0:de:12:34:cc:ef
eth2           195.208.10.11  00:c0:ab:cf:6d:12
eth0           195.208.10.20  00:c0:ab:e7:18:dc
fnpsh>
```

При использовании интерфейса командной строки для удаления записи из статической ARP-таблицы используется команда **nat arp delete**. Удалить запись из

ARP-таблицы можно по следующим параметрам:

- по IP-адресу: удалится запись, содержащая указанный IP-адрес;

- по MAC-адресу: удалятся записи, содержащие указанный MAC-адрес;

- по имени интерфейса: удалятся записи, содержащие указанное имя интерфейса.

Например, чтобы удалить запись, позволяющую обращаться из внутренней сети к WEB-серверу 195.208.10.20, можно использовать следующую команду:

fnpsh> nat arp delete 195.208.10.20
Удалить запись <eth0 195.208.10.20 00:c0:ab:e7:18:dc>? (Y/N) [N]: y
FNPSH-I-3075-Запись удалена из ARP таблицы
fnpsh>

6.1.3.3 Переадресация пакетов на внутренний интерфейс

Для получения доступа из внешней сети или демилитаризованной зоны к хостам внутренней сети предусмотрена функция переадресации. Данная функция удобна в случае необходимости обеспечения доступа к внутренним серверам из внешней сети через двухпортовый ССПТ-2, а также в других случаях при необходимости обеспечения доступа к внутренним хостам. Функцией переадресации поддерживаются протоколы TCP и UDP. Для организации доступа к внутреннему хосту необходимо проделать следующие шаги:

1) разрешить переадресацию. Для разрешения переадресации с внешнего интерфейса используется команда nat redirect public enable. Для разрешения переадресации с интерфейсов демилитаризованной зоны используется команда nat redirect dmz enable;

2) добавить необходимое правило в таблицу переадресации. Данное правило содержит тип используемого транспортного протокола (TCP или UDP), номер внешнего TCP/UDP-порта, на который приходит запрос, IP-адрес и TCP/UDP-порт во внутренней сети, куда необходимо переадресовать данный запрос. Для добавления правила в таблицу переадресации служит команда nat redirect add.

Внимание !!! Номер внешнего TCP/UDP-порта должен находиться в диапазоне от 0 до 65535.

3) в статическую ARP-таблицу добавить запись, указав соответствие между IP-адресом хоста во внутренней сети, на который будут переадресовываться пакеты из внешней сети, и его MAC-адресом.

Например, необходимо обеспечить доступ из внешней сети по протоколу SSH на хост во внутренней сети с IP-адресом 192.168.10.13 (рисунок 6.8).

При использовании интерфейса командной строки для этого необходимо проделать следующие действия:

1) разрешить переадресацию из внешней сети:

fnpsh> nat redirect public enable
FNPSH-I-307C-Переадресация с внешнего интерфейса включена
fnpsh>

2) добавить необходимое правило в таблицу переадресации, указав через пробел тип транспортного протокола (в данном случае TCP), номер внешнего TCP-порта, IP-адрес и TCP-порт во внутренней сети:

fnpsh> nat redirect add tcp 22 192.168.10.13 22
FNPSH-I-3077-Новая запись добавлена в таблицу переадресации
fnpsh>

3) добавить запись в статическую ARP-таблицу:

fnpsh> nat arp add eth1 192.168.10.13 01:18:c0:d5:fe:19
FNPSH-I-3074-Новая запись добавлена в ARP таблицу
fnpsh>

После проделанных действий возможно получение доступа из внешней сети к SSH-серверу хоста во внутренней сети с IP-адресом 192.168.10.13. Для этого необходимо с помощью SSH-клиента с компьютера во внешней сети обратиться на 22 порт внешнего интерфейса ССПТ-2, например, следующим образом:

/home/abc> ssh 195.208.10.1
Password:*******
192.168.10.13>

6.1.3.4 Аутентификация сетевых пользователей

ССПТ-2 поддерживает функцию аутентификации сетевых пользователей, работающих во внутренней, внешней сети или демилитаризованной зоне, для ограничения доступа к сетевым ресурсам пользователей, не прошедших процедуру аутентификации. Данная функция поддерживается только в режиме трансляции сетевых адресов. Для обеспечения устойчивости идентификации и аутентификации сетевых пользователей к пассивному и/или активному прослушиванию сети обмен информацией между пользователями ЛВС и ССПТ-2 защищается «Программной библиотекой защиты конфиденциальной информации «АГАВА-С» версии 5.1».

Пример подключения ССПТ-2 в режиме трансляции сетевых адресов

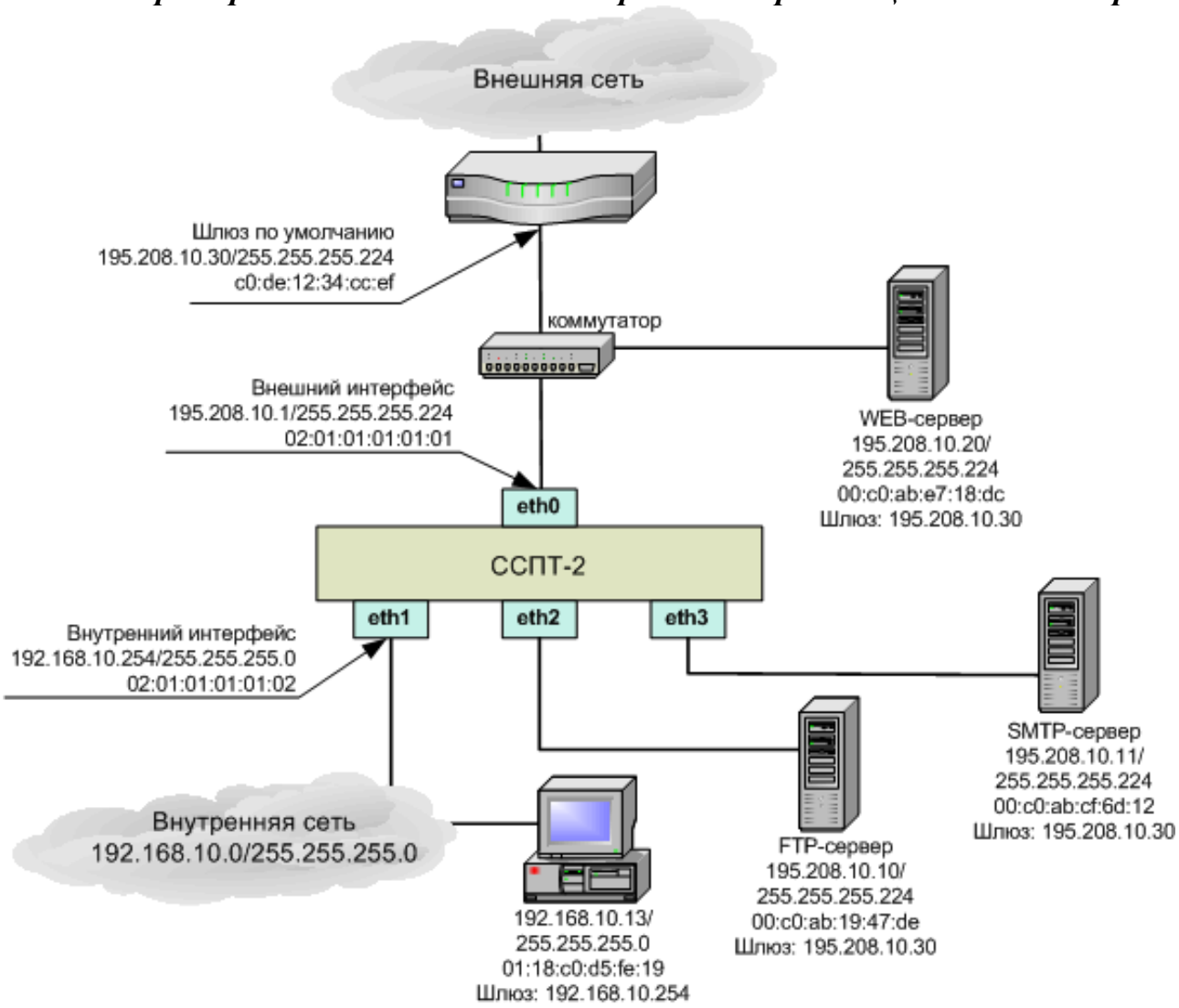

Рисунок 6.8

Для использования функции аутентификации сетевых пользователей

необходимо (на примере одного пользователя):

1) Включить функцию аутентификации сетевых пользователей с помощью команды nat authentication enable:

   fnpsh> nat authentication enable
   FNPSH-I-1217-Включение аутентификации пользователей
   fnpsh>

2) добавить пользователя в базу данных сетевых пользователей с помощью команды nat user add (возможно указание привязки нового пользователя к IP-адресу, MAC-адресу и/или фильтрующему интерфейсу):

   fnpsh> nat user add andrey 10.0.0.150
   Новый пароль:
   Новый пароль повторно:
   FNPSH-I-301D-Новый сетевой пользователь добавлен (andrey)
   fnpsh>

3) Сформировать открытый и закрытый ключи шифрования с приязкой к IP-адресу персонального компьютера, с которого будет осуществляться доступ через ССПТ-2, с помощью команды nat key add:

   fnpsh> nat key add 10.0.0.150
   FNPSH-I-30C4-Новая запись добавлена в файл ключей аутентификации (10.0.0.150)
   fnpsh>

4) С помощью утилиты fnpld выгрузить с ССПТ-2 файлы сертификата шифрования ССПТ-2, а также закрытого и открытого ключа шифрования для заданного IP-адреса (см. п. 3).
5) Установить файлы сертификата шифрования ССПТ-2, закрытого и открытого ключей шифрования на персональный компьютер, с которого будет осуществляться доступ через ССПТ-2. Данный персональный компьютер должен иметь тот IP-адрес, для которого вырабатывались ключи шифрования в п.3.
6) Перед началом работы с сетевыми ресурсами, расположенными за ССПТ-2, пройти процедуру аутентификации путем запуска на персональном компьютере

утилиты аутентификации fnpnl с указанием идентификатора пользователя и пароля. Эти данные будут переданы на ССПТ-2 для проведения процедуры аутентификации.

7) В случае, если аутентификация прошла успешно, данные пользователя (идентификатор, IP-адрес, MAC-адрес и фильтрующий интерфейс) запоминаются в таблице активных сетевых пользователей.

При включенной функции аутентификации сетевых пользователей каждый сетевой пакет, полученный на одном из фильтрующих интерфейсов, проверяется на принадлежность одному из активных пользователей. Если такое соответствие установлено, пакет обрабатывается в соответствии с режимом фильтрации, если соответствия не установлено, пакет отбрасывается с соответствующей диагностикой.

Каждой записи в таблице активных пользователей соответствует таймер неактивности, который обнуляется каждый раз, когда приходит пакет от данного пользователя. В случае отсутствия пакетов от пользователя за время, равное тайм-ауту неактивности (по умолчанию 600 секунд), запись о данном пользователе удаляется из таблицы активных пользователей. Чтобы такому пользователю в дальнейшем получить доступ к сетевым ресурсам через ССПТ-2, ему необходимо вновь пройти процедуру аутентификации. Для изменения значения тайм-аута неактивности сетевых пользователей необходимо воспользоваться командой nat authentication timeout, указав тайм-аут в секундах:

fnpsh> nat authentication timeout 43200

FNPSH-I-30C2-Тайм-аут неактивности сетевых пользователей изменен

fnpsh>

6.1.4. Управление процессом фильтрации

В рамках управления процессом фильтрации администратор может выполнить следующие действия:

- остановить процесс фильтрации;
- запустить процесс фильтрации;
- перезапустить процесс фильтрации;
- получить информацию о состоянии процесса фильтрации.

При использовании интерфейса командной строки для остановки процесса фильтрации (пакетного фильтра) предназначена команда **filter stop**:

fnpsh> filter stop
Остановить пакетный фильтр? (Y/N) [N]: y
FNPSH-I-303A-Пакетный фильтр остановлен
fnpsh>

При остановленном пакетном фильтре ССПТ-2 не передает пакеты через свои фильтрующие интерфейсы. При использовании интерфейса командной строки для запуска процесса фильтрации (пакетного фильтра) предназначена команда **filter start**:

fnpsh> filter start
FNPSH-I-3048-Пакетный фильтр запущен
fnpsh>

В момент запуска пакетный фильтр получает конфигурацию и правила фильтрации из соответствующих файлов и начинает работать в соответствии с ними. При использовании интерфейса командной строки для перезапуска процесса фильтрации (пакетного фильтра) предназначена команда **filter restart**:

fnpsh> filter restart
Перезапустить пакетный фильтр? (Y/N) [N]: y
FNPSH-I-3062-Пакетный фильтр перезапущен
fnpsh>

При использовании интерфейса командной строки для просмотра информации о текущем состоянии процесса фильтрации предназначена команда **filter**

status, которая отображает информацию о времени работы фильтра с момента последнего старта и статистику обработанных пакетов по интерфейсам во внутреннем просмотрщике командного интерфейса администратора ССПТ-2 (см. рисунок 6.9)

Состояние процесса фильтрации

```
Фильтр В РАБОТЕ 7 минут 40 секунд, с 23.11.2006 11:47:31 (MSK)
                    Статистика трафика: Весь трафик

Пакеты              eth0            eth1            eth2
  Получено           925               0               0
 Отправлено            0              53              53
   Удалено           872               0               0
 Повреждено            0               0               0

Байты               eth0            eth1            eth2
  Получено         80244               0               0
 Отправлено            0            3264            3264
   Удалено         76980               0               0
 Повреждено            0               0               0

                IPX <-- Весь трафик --> Ethernet II
H - справка     Q, F10 - выход
```

Рисунок 6.9

6.2. Трансляция (зеркалирование) трафика

В ССПТ-2 предусмотрена функция зеркалирования трафика, позволяющая перенаправлять копии пакетов на заданный интерфейс независимо от действия фильтрующего правила, которым обработан пакет. Данная функция может быть полезна при необходимости отслеживания всего трафика, проходящего через какой-либо фильтрующий интерфейс дополнительным средствами анализа, например системой обнаружения вторжений или системой регистрации пакетов.

Внимание!!! Не допускается перенаправлять зеркалируемый трафик на используемый фильтрующий интерфейс.

Интерфейс, на который производится зеркалирование (далее - зеркалирующий), перестает работать в режиме фильтрации, т.е. все пакеты, пришедшие на этот интерфейс из подключенного к нему сетевого сегмента, удаляются без обработки.

Если в правилах фильтрации зеркалирующий интерфейс указывается в качестве выходного, то, в соответствии с таким правилом, на этот интерфейс будут передаваться пакеты, что при определенных условиях может привести к возникновению дублирующих пакетов на зеркалирующем интерфейсе.

Функция зеркалирования работает во всех режимах фильтрации ССПТ-2. При этом, в режиме трансляции сетевых адресов внешний (Eth0) и внутренний (Eth1) интерфейсы не могут выступать в роли слушающего интерфейса, т.е. интерфейса, на который отправляются копии пакетов.

При использовании интерфейса командной строки для включения функции зеркалирования предназначена командой **interface filter <зеркалируемый_интерфейс> mirror <слушающий_интерфейс> <направление>**. Например, чтобы перенаправлять на интерфейс Eth2 копии всех пакетов, прошедших (полученных и отправленных) через интерфейс Eth0 (рисунок 6.10), необходимо воспользоваться командой:

fnpsh> interface filter eth0 mirror eth2 all
FNPSH-I-3035-Зеркалирование интерфейсов включено
fnpsh>

Опция <направление> в команде включения зеркалирования указывает на то, копии каких пакетов в зависимости от направления передачи через зеркалируемый интерфейс будут переданы на слушающий интерфейс. Для данной опции определены следующие возможные значения:

1) in: на слушающий интерфейс будут переданы копии только входящих пакетов;

2) out: на слушающий интерфейс будут переданы копии только исходящих пакетов;

3) all: на слушающий интерфейс будут переданы копии и входящих, и исходящих пакетов, т.е. весть трафик, проходящий через данный фильтрующий интерфейс.

При использовании интерфейса командной строки для отключения функции

зеркалирования необходимо воспользоваться командой interface filter <зеркалируемый_интерфейс> mirror disable:

fnpsh> interface filter eth0 mirror disable
Выключить зеркалирование интерфейсов? (Y/N) [N]: y
FNPSH-I-3034-Зеркалирование интерфейсов отключено
fnpsh>

Пример использования функции зеркалирования трафика

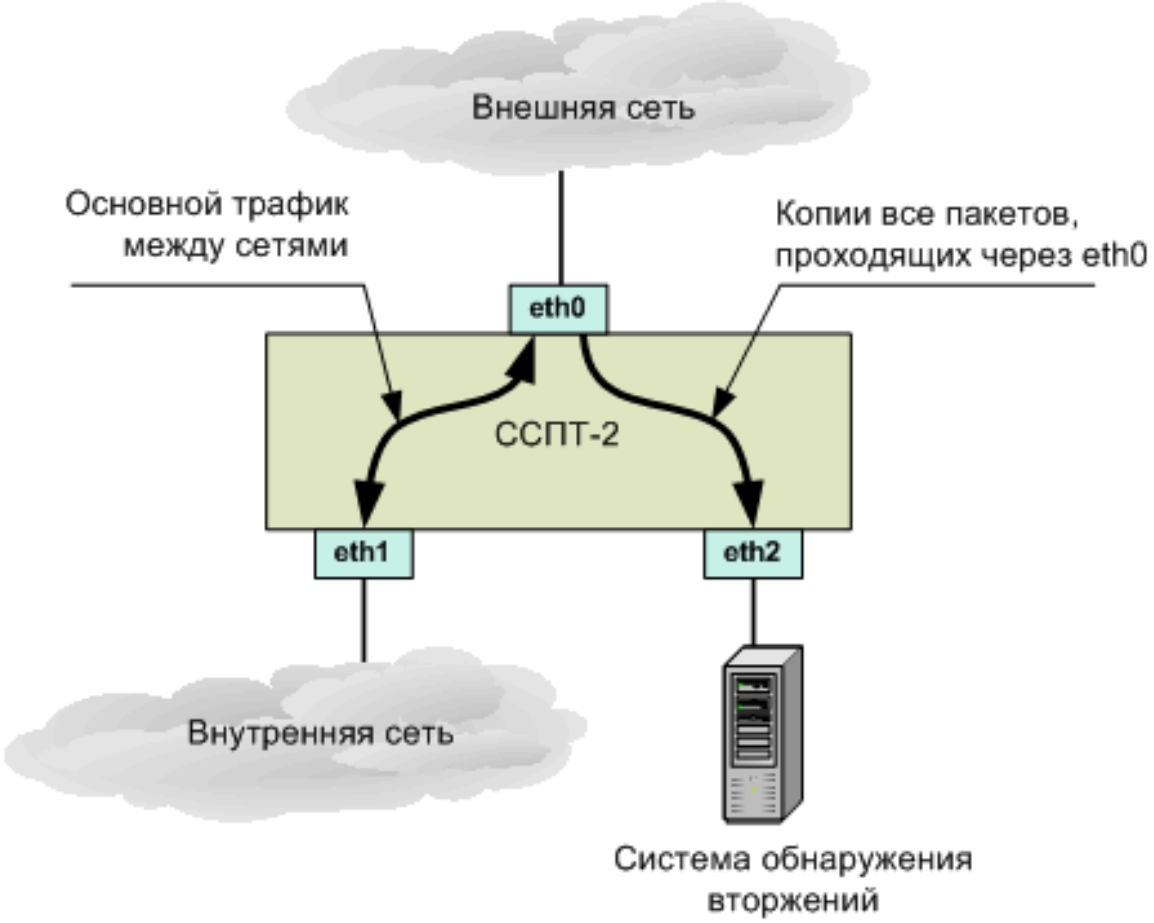

Рисунок 6.10

6.3. Система фильтрации высокой готовности на основе ССПТ-2

На основе межсетевых экранов ССПТ-2 может быть создана система фильтрации высокой готовности для обеспечения отказоустойчивости процесса фильтрации. Система высокой готовности может работать в трех режимах:

1) Режим «активный/резервный»;

2) Режим балансировки;

3) Режим Spanning Tree.

Логическая система фильтрации, построенная на ССПТ-2, обеспечивает восстановление процесса фильтрации, прерванного по причине аппаратного или программного сбоя, в прежнем объеме за время не более 10 секунд. Для обеспечения режима высокой готовности конфигурация обоих изделий должна быть одинакова, за исключением настроек модуля резервирования и адресов управляющего интерфейса.

Управление и настройка параметров ССПТ-2, используемых как единая система фильтрации, осуществляется из командного интерфейса администратора. Порядок настройки системы фильтрации (параметров ССПТ-2), ее запуска и останова, а также описание используемых при этом команд, представлены ниже.

6.3.1. Организация системы фильтрации высокой готовности в режиме «активный/резервный»

6.3.1.1. Описание

Система фильтрации высокой готовности в режиме «активный/резервный» строится на основе принципа «горячего» резервирования. В этой системе два ССПТ-2 подключаются к сегментам локальной сети параллельно (с использованием сетевых коммутирующих устройств) и работают как единая логическая система фильтрации (рис.6.11). При этом один ССПТ-2 является активным (master) и производит фильтрацию трафика, а второй - резервным (slave) и работает в режиме «горячего» резервирования, не пропуская при этом все принимаемые на свои фильтрующие интерфейсы пакеты. Синхронизация и обмен сообщениями между ССПТ-2 master и ССПТ-2 slave с целью выявления отказов и переключения режимов работы происходит через управляющие Ethernet-интерфейсы (EthC) устройств.

Логическая система фильтрации, построенная на ССПТ-2, обеспечивает бесперебойное функционирование системы фильтрации при любом отказе аппаратных или программных компонентов ССПТ-2 master, если он приводит к прекращению работы пакетного фильтра ССПТ-2 master.

Доступность ССПТ-2 для передачи трафика в режимах **Master** и **Slave** обеспечивается специальным режимом работы фильтрующих интерфейсов. В режиме **Master** фильтрующие интерфейсы ССПТ-2 активны, т.е. несущая между интерфейсами ССПТ-2 и портами коммутатора поднята. В режиме **Slave**, а также в случае штатного или аварийного останова сервера фильтрации фильтрующие интерфейсы ССПТ-2 заблокированы, т.е. несущая между интерфейсами ССПТ-2 и портами коммутатора отсутствует. Такой характер работы обеспечивается соответствующими настройками портов коммутаторов и фильтрующих интерфейсов ССПТ-2. В приведенном ниже примере показан порядок настройки системы фильтрации высокой готовности в режиме «активный/резервный». Предполагается, что используются ССПТ-2 и коммутаторы, поддерживающие скорости 10/100/1000 Мбит/с.

6.3.1.2. Необходимое оборудование и материалы

Для организации системы фильтрации высокой готовности в режиме «активный/резервный» (рис.6.11) необходимо:

- два межсетевых экрана ССПТ-2;
- два управляемых коммутатора 2-го уровня;
- четыре прямых кабеля типа «витая пара» (категории 5) для соединения ССПТ-2 с коммутаторами;
- один перекрестный (cross-over) кабель типа «витая пара» (категории 5) для соединения управляющих Ethernet-интерфейсов ССПТ-2 или три прямых кабеля типа «витая пара» (категории 5) и один концентратор/коммутатор для соединения управляющих Ethernet-интерфейсов ССПТ-2 и управляющего компьютера.

6.3.1.3. Настройка ССПТ-2 и дополнительного оборудования

Для настройки схемы высокой готовности, представленной на рисунке 6.11 необходимо проделать следующие шаги:

1) Настройка коммутаторов. На управляемых коммутаторах 3 и 4 для портов 1 и 2 отключить свойство **autonegotiation** и установить максимальную скорость, поддерживаемую и портами коммутатора, и фильтрующими интерфейсами ССПТ-

2 (в нашем случае - 1000BaseTX/full-duplex). Отключить протокол Spanning Tree на портах 1 и 2 коммутаторов 3 и 4. Порядок настройки коммутаторов описан в соответствующих руководствах.

2) Подключение ССПТ-2. Соединить управляющие Ethernet-интерфейсы устройств ССПТ-2 напрямую с помощью cross-over кабеля “витая пара” либо через концентратор/коммутатор с помощью двух прямых кабелей “витая пара”.

3) Настройка по интерфейсу командной строки ССПТ-2 (№1) в режиме Master:

- настроить управляющий Ethernet-интерфейс:

fnpsh> interface control address 192.168.2.1/255.255.255.0
FNPSH-I-3024-IP адрес управляющего интерфейса изменен
fnpsh>

- установить IP-адрес смежного устройства:

fnpsh> reserv neighbour 192.168.2.2
FNPSH-I-3081-IP-адрес смежного устройство изменен
fnpsh>

- настроить активный режим работы для данного устройства в системе фильтрации высокой готовности:

fnpsh> reserv mode master
FNPSH-I-307E-Режим резервирования изменен
fnpsh>

Установить параметры фильтрующих интерфейсов для активного и заблокированного состояния. При этом необходимо руководствоваться следующими правилами: для активного состояния интерфейсов устанавливаются параметры **media** и **duplex,** соответствующие максимальной скорости, поддерживаемой ССПТ-2 и коммутаторами; для заблокированного состояния устанавливаются параметры **media** и **duplex,** соответствующие минимальной скорости, поддерживаемой ССПТ-2. В нашем случае необходимо сделать следующие настройки:

fnpsh> reserv interface active media 1000
FNPSH-I-30AC-Скорость фильтрующих интерфейсов при резервировании изменена

fnpsh> reserv interface active duplex full

FNPSH-I-30AD-Режим передачи фильтрующих интерфейсов при резервировании изменен

fnpsh> reserv interface blocked media 10

FNPSH-I-30AC-Скорость фильтрующих интерфейсов при резервировании изменена

fnpsh> reserv interface blocked duplex half

FNPSH-I-30AD-Режим передачи фильтрующих интерфейсов при резервировании изменен

fnpsh>

Последние две команды необязательны, они соответствуют настройкам по умолчанию для данных параметров.

3) Настройка по интерфейсу командной строки ССПТ-2 (№2) в режиме Slave:

- настроить управляющий Ethernet-интерфейс:

fnpsh> interface control address 192.168.2.2/255.255.255.0
FNPSH-I-3024-IP адрес управляющего интерфейса изменен
fnpsh>

- установить IP-адрес смежного устройства:

fnpsh> reserv neighbour 192.168.2.1
FNPSH-I-3081-IP-адрес смежного устройство изменен
fnpsh>

- настроить резервный режим работы устройства в системе фильтрации высокой готовности:

fnpsh> reserv mode slave
FNPSH-I-307E-Режим резервирования изменен
fnpsh>

Пример организации системы фильтрации высокой готовности в режиме «активный/резервный»

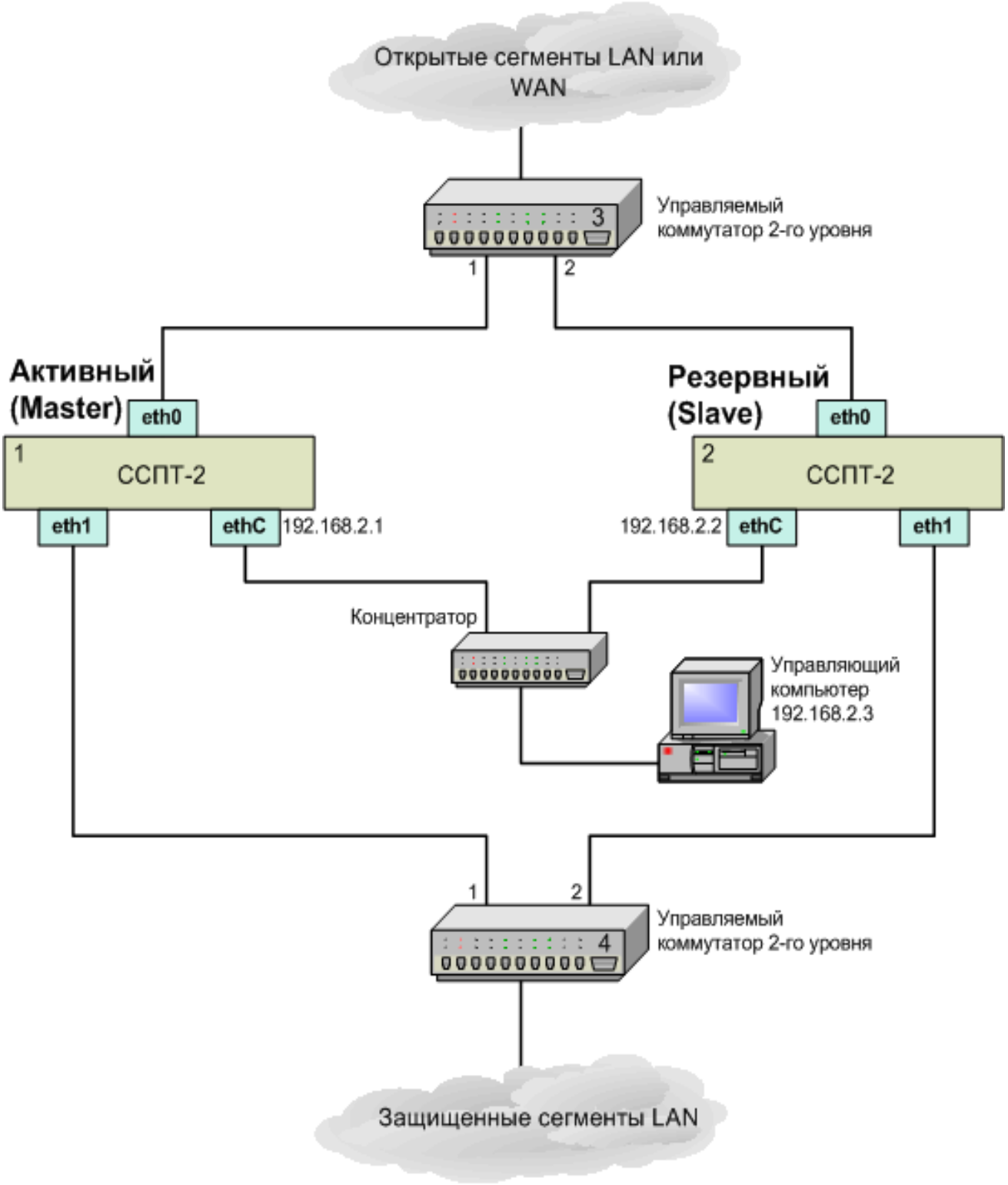

Рисунок 6.11

Установить параметры фильтрующих интерфейсов для активного и заблокированного состояния. При этом необходимо руководствоваться следующими правилами: для активного состояния интерфейсов устанавливаются параметры **media** и **duplex,** соответствующие максимальной скорости, поддерживаемой ССПТ-2 и коммутаторами; для заблокированного состояния устанавливаются параметры **media** и **duplex,** соответствующие минимальной скорости, поддерживаемой ССПТ-2. В нашем случае необходимо сделать следующие настройки:

fnpsh> reserv interface active media 1000
FNPSH-I-30AC-Скорость фильтрующих интерфейсов при резервировании изменена
fnpsh> reserv interface active duplex full
FNPSH-I-30AD-Режим передачи фильтрующих интерфейсов при резервировании изменен
fnpsh> reserv interface blocked media 10
FNPSH-I-30AC-Скорость фильтрующих интерфейсов при резервировании изменена
fnpsh> reserv interface blocked duplex half
FNPSH-I-30AD-Режим передачи фильтрующих интерфейсов при резервировании изменен
fnpsh>

Последние две команды необязательны, они соответствуют настройкам по умолчанию для данных параметров. Параметры media и duplex для активного и заблокированного состояний интерфейсов должны быть идентичны на обоих ССПТ-2.

После выполнения указанных настроек система фильтрации высокой готовности в режиме «активный/резервный» готова к включению.

6.3.1.4. Включение и останов системы фильтрации высокой готовности в режиме «активный/резервный»

Включение системы фильтрации высокой готовности в режиме «активный/резервный» осуществляется следующим образом.

Включить резервирование на ССПТ-2 №1:

fnpsh> reserv enable
FNPSH-I-307F-Резервирование включено
fnpsh>

Проконтролировать включение режима резервирования на ССПТ-2 №1:

fnpsh> reserv show
Резервирование: включено
Режим: MASTER (активный)
Смежное устройство:
IP-адрес: 192.168.2.2
Режим: не определено
Интерфейсы в активном состоянии: 1000baseTX / full-duplex
Интерфейсы в заблокированном состоянии: 10baseT/UTP / half-duplex
fnpsh>

После включения режима резервирования на ССПТ-2 №1 фильтрующие интерфейсы автоматически переводятся в состояние, заданное параметром «Интерфейсы в активном состоянии» (команда «reserv interface active»).

Включить резервирование на ССПТ-2 №2:

fnpsh> reserv enable

FNPSH-I-307F-Резервирование включено

fnpsh>

Проконтролировать включение режима резервирования на ССПТ-2 №2:

fnpsh> reserv show
Резервирование: включено
Режим: SLAVE (резервный)
Смежное устройство:
IP-адрес: 192.168.2.1
Режим: master (активный)
Интерфейсы в активном состоянии: 1000baseTX / full-duplex
Интерфейсы в заблокированном состоянии: 10baseT/UTP / half-duplex
fnpsh>

После включения режима резервирования на ССПТ-2 №2 фильтрующие интерфейсы автоматически переводятся в состояние, заданное параметром «Интерфейсы в заблокированном состоянии» (команда «reserv interface blocked»).

Подключить ССПТ-2 №1 и ССПТ-2 №2 к коммутаторам 3 и 4 как показано на рисунке 6.11:

- интерфейс **eth0** ССПТ-2 №1 к порту 1 коммутатора 3;
- интерфейс **eth1** ССПТ-2 №1 к порту 1 коммутатора 4;

- интерфейс **eth0** ССПТ-2 №2 к порту 2 коммутатора 3;

- интерфейс **eth1** ССПТ-2 №2 к порту 2 коммутатора 4.

Проконтролировать наличие несущей по светодиодам «Link» на интерфейсах **eth0** и **eth1** устройства ССПТ-2 №1, работающего в режиме **Master**, и отсутствие несущей по светодиодам «Link» на интерфейсах **eth0** и **eth1** устройства ССПТ-2 №2, работающего в режиме **Slave**.

После проделанных шагов система фильтрации высокой готовности в режиме «активный/резервный» приступает к работе.

Для корректного останова системы фильтрации высокой готовности в режиме «активный/резервный» необходимо проделать следующие шаги:

Отключить ССПТ-2 №2 (Slave) следующим образом:

- отсоединить интерфейсы **eth0** и **eth1** устройства ССПТ-2 №2 (**Slave**) от портов коммутатора 3 и 4:

- отключить резервирование на ССПТ-2 №2 (**Slave**):

fnpsh> reserv disable
Отключить резервирование? (Y/N) [N]: y
FNPSH-I-3080-Резервирование отключено
fnpsh>

После отключения режима резервирования на ССПТ-2 №2 фильтрующие интерфейсы автоматически переводятся в состояние, в котором они находились до включения резервирования.

Отключить ССПТ-2 №1 (Master) следующим образом:

- отключить резервирование на ССПТ-1 №2 (**Master**):

fnpsh> reserv disable
Отключить резервирование? (Y/N) [N]: y
FNPSH-I-3080-Резервирование отключено

После отключения режима резервирования на ССПТ-2 №1 фильтрующие интерфейсы автоматически переводятся в состояние, в котором они находились до включения резервирования.

После проделанных шагов ССПТ-2 №1 останется в схеме и продолжит работу, как межсетевой экран без резервирования.

6.3.2. Организация системы фильтрации высокой готовности в режиме балансировки

6.3.2.1. Описание

Система высокой готовности в режиме балансировки нагрузки основана на схеме объединения двух физических каналов между коммутаторами в один логический канал, называемый транком (стандарт IEEE 802.3ad, Link Aggregation). В такой системе два ССПТ-2 подключаются в разрыв физических каналов между коммутаторами и работают как одна логическая система фильтрации (рисунок 6.12). При этом оба устройства ССПТ-2 является активными и производят фильтрацию трафика. Распределение нагрузки на физические каналы осуществляют коммутаторы, настроенные соответствующим образом. Синхронизация и обмен сообщениями между ССПТ-2 с целью выявления аппаратных и программных отказов и переключения режимов работы, происходит через управляющие Ethernet-интерфейсы (ethC). В случае, если в такой схеме откажет (по причине программного или аппаратного сбоя) одно из устройств ССПТ-2, коммутаторы перераспределят трафик на доступные физические каналы и, таким образом, система фильтрации останется работоспособной.

Доступность ССПТ-2 для передачи трафика в режим**е балансировки** обеспечивается специальным режимом работы фильтрующих интерфейсов. При штатном функционировании в режиме балансировки фильтрующие интерфейсы обоих ССПТ-2 активны, т.е. несущая между интерфейсами ССПТ-2 и портами коммутаторов поднята. В случае штатного или аварийного останова сервера фильтрации (программного компонента ССПТ-2, отвечающего за передачу пакетов между интерфейсам) фильтрующие интерфейсы ССПТ-2, на котором это произошло, блокируются, т.е. несущая между интерфейсами данного ССПТ-2 и портами коммутатора отсутствует. Такой характер работы обеспечивается соответствующими настройками портов коммутаторов и фильтрующих интерфейсов ССПТ-2. В приведенном ниже примере показан порядок настройки системы фильтрации высокой готовности в режиме балансировки. Предполагается, что используются ССПТ-2 и

коммутаторы, поддерживающие скорости 10/100/1000 Мбит/с.

6.3.2.2. Необходимое оборудование и материалы

Для организации системы фильтрации высокой готовности в режиме балансировки (рис.6.12) необходимо:

- два межсетевых экрана ССПТ-2;

- два управляемых коммутатора 2-го уровня, поддерживающих стандарт IEEE 802.3ad;

- четыре прямых кабеля типа «витая пара» (категории 5) для соединения ССПТ-2 с коммутаторами;

- один перекрестный (cross-over) кабель типа «витая пара» (категории 5) для соединения управляющих Ethernet-интерфейсов ССПТ-2 или три прямых кабеля типа «витая пара» (категории 5) и один концентратор/коммутатор для соединения управляющих Ethernet-интерфейсов ССПТ-2 и управляющего компьютера.

6.3.2.3. Настройка ССПТ-2 и дополнительного оборудования

Для настройки по интерфейсу командной строки схемы высокой готовности, представленной на рисунке 6.12 необходимо проделать следующие шаги:

1) Настройка коммутаторов. На управляемых коммутаторах 3 и 4 для портов 1 и 2 отключить свойство **autonegotiation** и установить скорости, соответствующие максимальным скоростям фильтрующих интерфейсов ССПТ-2 **eth0** и **eth1** (в нашем случае - 1000BaseTX/full-duplex). Настроить агрегирование каналов (транк) для портов 1 и 2 коммутаторов 3 и 4. Порядок настройки коммутаторов описан в соответствующих руководствах.

2) Соединить управляющие Ethernet-интерфейсы устройств ССПТ-2 напрямую с помощью cross-over кабеля “витая пара” либо через концентратор/коммутатор с помощью двух прямых кабелей “витая пара”.

3) Настройка ССПТ-2 №1 в режиме балансировки:

- настроить управляющий Ethernet-интерфейс:

fnpsh> interface control address 192.168.2.1/255.255.255.0
FNPSH-I-3024-IP адрес управляющего интерфейса изменен
fnpsh>

- установить IP-адрес смежного устройства:

fnpsh> reserv neighbour 192.168.2.2
FNPSH-I-3081-IP-адрес смежного устройство изменен
fnpsh>

- настроить режим балансировки системы фильтрации высокой готовности:

fnpsh> reserv mode balance
FNPSH-I-307E-Режим резервирования изменен
fnpsh>

Установить параметры фильтрующих интерфейсов для активного и заблокированного состояния. При этом необходимо руководствоваться следующими правилами: для активного состояния интерфейсов устанавливаются параметры **media** и **duplex,** соответствующие максимальной скорости, поддерживаемой ССПТ-2 и коммутаторами; для заблокированного состояния устанавливаются параметры **media** и **duplex,** соответствующие минимальной скорости, поддерживаемой ССПТ-2. Настройки для активного состояния интерфейсов будут использоваться при штатном функционировании системы резервирования в режиме балансировки. Настройки для заблокированного состояния интерфейсов будут использоваться в случае штатного (по команде администратора) или аварийного останова сервера фильтрации (программного компонента ССПТ-2, отвечающего за передачу пакетов между интерфейсам). В нашем случае необходимо сделать следующие настройки:

fnpsh> reserv interface active media 1000
FNPSH-I-30AC-Скорость фильтрующих интерфейсов при резервировании изменена
fnpsh> reserv interface active duplex full
FNPSH-I-30AD-Режим передачи фильтрующих интерфейсов при резервировании изменен
fnpsh> reserv interface blocked media 10
FNPSH-I-30AC-Скорость фильтрующих интерфейсов при резервировании изменена
fnpsh> reserv interface blocked duplex half
FNPSH-I-30AD-Режим передачи фильтрующих интерфейсов при резервировании изменен
fnpsh>

Последние две команды необязательны, они соответствуют настройкам по умолчанию для данных параметров.

4) Настройка ССПТ-2 №2 в режиме балансировки:

- настроить управляющий Ethernet-интерфейс:

fnpsh> interface control address 192.168.2.2/255.255.255.0
FNPSH-I-3024-IP адрес управляющего интерфейса изменен
fnpsh>

- установить IP-адрес смежного устройства:

fnpsh> reserv neighbour 192.168.2.1
FNPSH-I-3081-IP-адрес смежного устройство изменен
fnpsh>

- настроить режим балансировки системы фильтрации высокой готовности:

fnpsh> reserv mode balance
FNPSH-I-307E-Режим резервирования изменен
fnpsh>

Установить параметры фильтрующих интерфейсов для активного и заблокированного состояния. При этом необходимо руководствоваться следующими правилами: для активного состояния интерфейсов устанавливаются параметры **media** и **duplex,** соответствующие максимальной скорости, поддерживаемой ССПТ-2 и коммутаторами; для заблокированного состояния устанавливаются параметры **media** и **duplex,** соответствующие минимальной скорости, поддерживаемой ССПТ-2. Настройки для активного состояния интерфейсов будут использоваться при штатном функционировании системы резервирования в режиме балансировки. Настройки для заблокированного состояния интерфейсов будут использоваться в случае штатного (по команде администратора) или аварийного останова сервера фильтрации (программного компонента ССПТ-2, отвечающего за передачу пакетов между интерфейсам). В нашем случае необходимо сделать следующие настройки:

fnpsh> reserv interface active media 1000
FNPSH-I-30AC-Скорость фильтрующих интерфейсов при резервировании изменена
fnpsh> reserv interface active duplex full

FNPSH-I-30AD-Режим передачи фильтрующих интерфейсов при резервировании изменен

fnpsh> reserv interface blocked media 10

FNPSH-I-30AC-Скорость фильтрующих интерфейсов при резервировании изменена

fnpsh> reserv interface blocked duplex half

FNPSH-I-30AD-Режим передачи фильтрующих интерфейсов при резервировании изменен

fnpsh>

Последние две команды необязательны, они соответствуют настройкам по умолчанию для данных параметров.

После выполнения указанных настроек система фильтрации высокой готовности в режиме балансировки готова к включению.

6.3.2.4. Включение и останов системы фильтрации высокой готовности в режиме балансировки

Включение системы фильтрации высокой готовности в режиме балансировки по интерфейсу командной строки осуществляется следующим образом:

1) Включить резервирование на ССПТ-2 №1:

fnpsh> reserv enable
FNPSH-I-307F-Резервирование включено
fnpsh>

Проконтролировать включение режима резервирования на ССПТ-2 №1:

fnpsh> reserv show
Резервирование: включено
Режим: BALANCE (балансировка)
Смежное устройство:
IP-адрес: 192.168.2.2
Режим: не определено
Интерфейсы в активном состоянии: 1000baseTX / full-duplex
Интерфейсы в заблокированном состоянии: 10baseT/UTP / half-duplex
fnpsh>

После включения режима резервирования на ССПТ-2 №1 фильтрующие интерфейсы автоматически переводятся в состояние, заданное параметром «Интерфейсы в активном состоянии» (команда «reserv interface active»).

Пример организации системы фильтрации высокой готовности в режиме балансировки

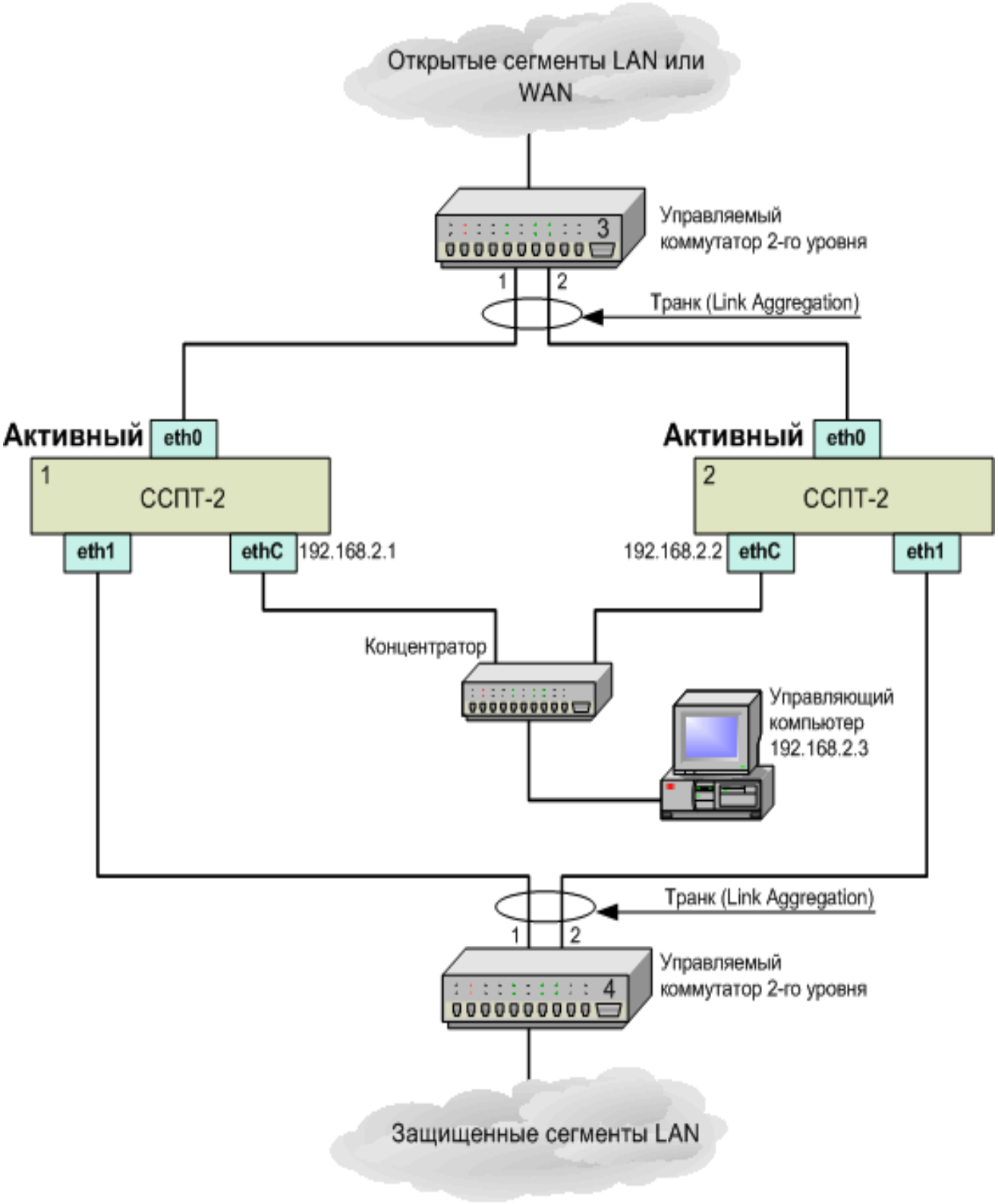

Рисунок 6.12

2) Включить резервирование на ССПТ-2 №2:

fnpsh> reserv enable
FNPSH-I-307F-Резервирование включено
fnpsh>

Проконтролировать включение режима резервирования на ССПТ-2 №2:

fnpsh> reserv show
Резервирование: включено
Режим: BALANCE (балансировка)
Смежное устройство:
IP-адрес: 192.168.2.1
Режим: balance (балансировка)
Интерфейсы в активном состоянии: 1000baseTX / full-duplex
Интерфейсы в заблокированном состоянии: 10baseT/UTP / half-duplex
fnpsh>

После включения режима резервирования на ССПТ-2 №2 фильтрующие интерфейсы автоматически переводятся в состояние, заданное параметром «Интерфейсы в активном состоянии» (команда «reserv interface active»).

3) Подключить ССПТ-2 №1 и ССПТ-2 №2 к коммутаторам 3 и 4 как показано на рисунке 6.12:

- интерфейс eth0 ССПТ-2 №1 к порту 1 коммутатора 3;
- интерфейс eth1 ССПТ-2 №1 к порту 1 коммутатора 4;
- интерфейс eth0 ССПТ-2 №2 к порту 2 коммутатора 3;
- интерфейс eth1 ССПТ-2 №2 к порту 2 коммутатора 4;

4) Проконтролировать наличие несущей по светодиодам «Link» на интерфейсах eth0 и eth1 устройства ССПТ-2 №1 и на интерфейсах eth0 и eth1 устройства ССПТ-2 №2.

После проделанных шагов система фильтрации высокой готовности в режиме балансировки приступает к работе.

Для корректного останова по интерфейсу командной строки системы фильтрации высокой готовности в режиме балансировки необходимо проделать следующие шаги:

1) Отключить ССПТ-2 №2 следующим образом:

- отсоединить интерфейсы eth0 и eth1 устройства ССПТ-2 №2 от портов коммутатора 3 и 4.

- отключить резервирование на ССПТ-2 №2:

fnpsh> reserv disable
Отключить резервирование? (Y/N) [N]: y
FNPSH-I-3080-Резервирование отключено
fnpsh>

После отключения режима резервирования на ССПТ-2 №2 фильтрующие интерфейсы автоматически переводятся в состояние, в котором они находились до включения резервирования.

2) Отключить резервирование ССПТ-2 №1 следующим образом:

fnpsh> reserv disable
Отключить резервирование? (Y/N) [N]: y
FNPSH-I-3080-Резервирование отключено

После отключения режима резервирования на ССПТ-2 №1 фильтрующие интерфейсы автоматически переводятся в состояние, в котором они находились до включения резервирования.

После проделанных шагов ССПТ-2 №1 останется в схеме и продолжит работу, как межсетевой экран без резервирования.

6.3.3. Организация системы фильтрации высокой готовности в режиме Spanning Tree

6.3.3.1. Описание

Протокол Spanning Tree (STP) предназначен для выявления и устранения петель в физической структуре коммутируемой сети. Коммутаторы, поддерживающие протокол Spanning Tree, обмениваясь служебными сообщениями, блокируют избыточные связи в топологии сети, тем самым, гарантируя наличие единственного пути из одной точки сети в другую.

Система высокой готовности в режиме Spanning Tree основана на схеме соединения двух коммутаторов двумя физическими каналами. При этом коммутато-

ры обнаруживают наличие резервной связи и блокируют соответствующие порты. В этой системе два ССПТ-2 подключаются в разрыв физических каналов между коммутаторами и работают как одна логическая система фильтрации (рисунок 3.12). При этом оба устройства ССПТ-2 является активными, но фильтрацию трафика производит только одно устройство, так как одновременно задействован только один физический канал. Переключение каналов осуществляется коммутаторами. Синхронизация и обмен сообщениями между ССПТ-2 с целью выявления программных отказов и переключения режимов работы, происходит через управляющие Ethernet-интерфейсы (**ethC**). В случае, если в такой схеме откажет (по причине программного или аппаратного сбоя) одно из устройств ССПТ-2, коммутаторы обнаружат отказ по отсутствию служебных сообщений Spanning Tree и включат в работу резервную связь. Таким образом, система фильтрации остается работоспособной.

6.3.3.2. Необходимое оборудование и материалы

Для организации системы фильтрации высокой готовности в режиме Spanning Tree (рисунок 6.13) необходимо:

- два межсетевых экрана ССПТ-2;

- два управляемых коммутатора 2-го уровня, поддерживающих стандарт IEEE 802.1d (Spanning Tree) или IEEE 802.1w (Rapid Spanning Tree);

- четыре прямых кабеля типа «витая пара» (категории 5) для соединения ССПТ-2 с коммутаторами;

- один перекрестный (cross-over) кабель типа «витая пара» (категории 5) для соединения управляющих Ethernet-интерфейсов ССПТ-2 или три прямых кабеля типа «витая пара» (категории 5) и один концентратор/коммутатор для соединения управляющих Ethernet-интерфейсов ССПТ-2 и управляющего компьютера.

6.3.3.3. Настройка ССПТ-2 и дополнительного оборудования

Для настройки схемы высокой готовности, представленной на рисунке 6.13 необходимо проделать следующие шаги:

1) Настройка коммутаторов. На управляемых коммутаторах 3 и 4 для портов

1 и 2 включить использование протокола Spanning Tree или Rapid Spanning Tree. Порядок настройки коммутаторов описан в соответствующих руководствах.

2) Подключение ССПТ-2. Подключить управляющие Ethernet-интерфейсы устройств ССПТ-2 напрямую с помощью cross-over кабеля “витая пара” либо через концентратор/коммутатор с помощью двух прямых кабелей “витая пара”.

3) Настройка ССПТ-2 №1 в режиме Spanning Tree (по интерфейсу командной строки):

- настроить управляющий Ethernet-интерфейс:

fnpsh> interface control address 192.168.2.1/255.255.255.0
FNPSH-I-3024-IP адрес управляющего интерфейса изменен
fnpsh>

- установить IP-адрес смежного устройства:

fnpsh> reserv neighbour 192.168.2.2
FNPSH-I-3081-IP-адрес смежного устройство изменен
fnpsh>

- настроить режим Spanning Tree в схеме горячего резервирования:

fnpsh> reserv mode stp
FNPSH-I-307E-Режим резервирования изменен
fnpsh>

4) **Настройка ССПТ-2 №2 в режиме Spanning Tree** (по интерфейсу командной строки):

- настроить управляющий Ethernet-интерфейс:

fnpsh> interface control address 192.168.2.2/255.255.255.0
FNPSH-I-3024-IP адрес управляющего интерфейса изменен
fnpsh>

- установить IP-адрес смежного устройства:

fnpsh> reserv neighbour 192.168.2.1
FNPSH-I-3081-IP-адрес смежного устройство изменен
fnpsh>

- настроить режим Spanning Tree в схеме горячего резервирования:

fnpsh> reserv mode stp

FNPSH-I-307E-Режим резервирования изменен
fnpsh>

После выполнения указанных настроек система фильтрации высокой готовности в режиме Spanning Tree готова к включению.

6.3.3.4. Включение и останов системы фильтрации высокой готовности в режиме Spanning Tree

Включение системы фильтрации высокой готовности в режиме Spanning Tree по интерфейсу командной строки осуществляется следующим образом.

1) Включить резервирование на ССПТ-2 №1:

fnpsh> reserv enable
FNPSH-I-307F-Резервирование включено
fnpsh>

Проконтролировать включение режима резервирования на ССПТ-2 №1:

fnpsh> reserv show
Резервирование: включено
Режим: STP (Spanning Tree)
Смежное устройство:
IP-адрес: 192.168.2.2
Режим: не определено
Скорость/дуплекс режима MASTER: 1000baseTX / full-duplex
Скорость/дуплекс режима SLAVE: 10baseT/UTP / half-duplex
fnpsh>

2) Включить резервирование на ССПТ-2 №2:

fnpsh> reserv enable
FNPSH-I-307F-Резервирование включено
fnpsh>

Проконтролировать включение режима резервирования на ССПТ-2 №2:

fnpsh> reserv show
Резервирование: включено
Режим: STP (Spanning Tree)
Смежное устройство:
IP-адрес: 192.168.2.1
Режим: stp (Spanning Tree)
Скорость/дуплекс режима MASTER: 1000baseTX / full-duplex
Скорость/дуплекс режима SLAVE: 10baseT/UTP / half-duplex
fnpsh>

Пример организации системы фильтрации высокой готовности в режиме Spanning Tree

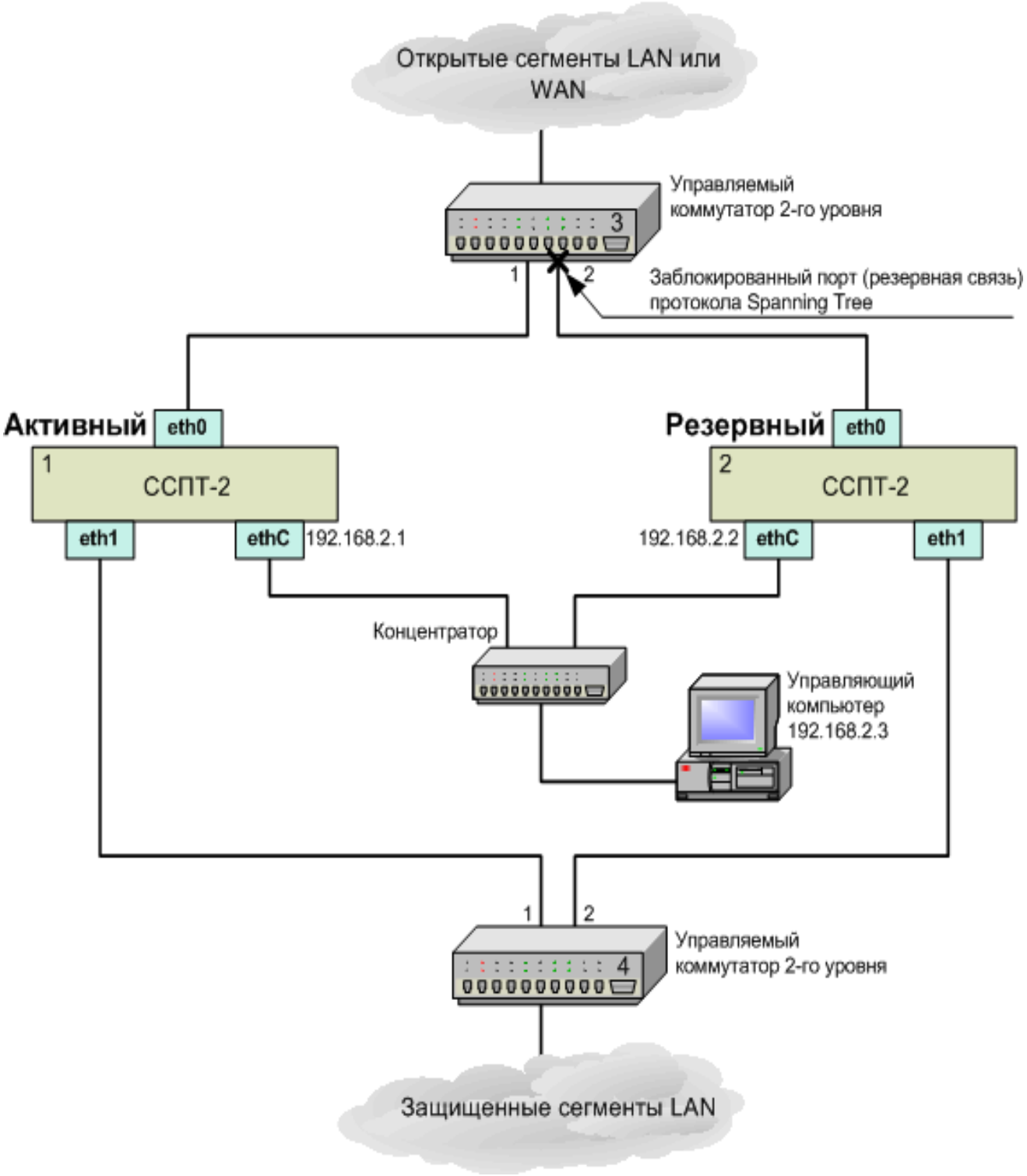

Рисунок 6.13

3) Подключить ССПТ-2 №1 и ССПТ-2 №2 к коммутаторам 3 и 4 как показано на рисунке 6.13:

- интерфейс eth0 ССПТ-2 №1 к порту 1 коммутатора 3;
- интерфейс eth1 ССПТ-2 №1 к порту 1 коммутатора 4;
- интерфейс eth0 ССПТ-2 №2 к порту 2 коммутатора 3;
- интерфейс eth1 ССПТ-2 №2 к порту 2 коммутатора 4.

4) Проконтролировать наличие несущей по светодиодам «Link» по крайней мере на интерфейсах eth0 и eth1 одного из устройств ССПТ-2.

После проделанных шагов система фильтрации высокой готовности в режиме Spanning Tree приступает к работе.

При использовании интерфейса командной строки для корректного останова системы фильтрации высокой готовности в режиме Spanning Tree необходимо проделать следующие шаги:

1) Отключить ССПТ-2 №2 следующим образом:

- отсоединить интерфейсы eth0 и eth1 устройства ССПТ-2 №2 от портов коммутатора 3 и 4;
- отключить резервирование на ССПТ-2 №2:

fnpsh> reserv disable
Отключить резервирование? (Y/N) [N]: y
FNPSH-I-3080-Резервирование отключено
fnpsh>

2) Отключить резервирование ССПТ-2 №1 следующим образом:

fnpsh> reserv disable
Отключить резервирование? (Y/N) [N]: y
FNPSH-I-3080-Резервирование отключено
fnpsh>

После проделанных шагов ССПТ-2 №1 останется в схеме и продолжит работу, как межсетевой экран без резервирования.

6.3.4. Синхронизация конфигурации и правил фильтрации

При работе в схеме высокой готовности предусмотрена синхронизация конфигурации и правил фильтрации между ССПТ-2, включенных в схему. Синхронизация происходит асинхронно по запросу администратора и только в случае наличия и доступности смежного ССПТ-2. При использовании интерфейса командной строки для выполнения синхронизации правил фильтрации необходимо, находясь в командном интерфейсе администратора одного из ССПТ-2, использовать команду:

fnpsh> reserv rule synchronize
Синхронизировать правила? (Y/N) [N]: y
FNPSH-I-3086-Синхронизация правил выполнена
fnpsh>

После выполнения данной команды на смежный ССПТ-2 будут переданы все правила фильтрации данного ССПТ-2.

При использовании интерфейса командной строки для выполнения синхронизации конфигурации необходимо, находясь в командном интерфейсе администратора одного из ССПТ-2, использовать команду:

fnpsh> reserv config synchronize
Синхронизировать конфигурацию? (Y/N) [N]: y
FNPSH-I-30b1-Синхронизация конфигурации выполнена
fnpsh>

После выполнения данной команды на смежный ССПТ-2 будет переданы параметры конфигурации данного ССПТ-2 за исключением настроек управляющего и фильтрующих интерфейсов и настроек резервирования.

7. АДМИНИСТРИРОВАНИЕ ССПТ-2 – WEB ИНТЕРФЕЙС

7.1. Общие положения

В качестве дополнительного средства удаленного администрирования в ССПТ-2 предусмотрена возможность использования **WEB - интерфейса** администратора. Удаленное управление по WEB – интерфейсу допускается только по выделенному каналу. Поэтому в конфигурации изделия по умолчанию управление по WEB - интерфейсу администратора не предусмотрено. WEB – интерфейс активируется только по каналу локального управления командой администратора, имеющего полные полномочия.

Для включения/отключения WEB – интерфейса используются следующие команды:

system web enable - включение WEB интерфейса, команда выполняется только при локальном администрировании (через системную консоль);

system web disable - отключение WEB интерфейса, команда выполняется только при локальном администрировании (через системную консоль).

WEB – интерфейс предоставляет возможность удаленного администрирования ССПТ-2 по выделенному каналу, используя стандартный WEB браузер, установленный на управляющем компьютере.

Для обеспечения устойчивости идентификации и аутентификации к активному воздействию на процесс управления со стороны канала связи и перехвату информации в канале управления, при удаленном управлении с использованием WEB-интерфейса должен использоваться выделенный канал управления, размещенный на охраняемой территории и контролируемый организационно-административными методами.

7.2. Вход в систему, главное окно

Для управления межсетевым экраном ССПТ-2 с помощью графического WEB-интерфейса администратора необходимо использовать графический WEB-браузер, установленный на управляющем компьютере (Рекомендуется использование Internet Explorer 6 или 7).

После запуска WEB-браузера на управляющем компьютере в адресной строке следует набрать команду:

https://<IP_адрес_управляющего_интерфейса>.

Параметр <IP_адрес_управляющего_интерфейса> может принимать следующие значения:

192.168.1.1 – для случая соединения с ССПТ-2 по последовательному порту RS-232;

IP-адрес управляющего Ethernet-интерфейса ССПТ-2 – для случая соединения с ССПТ-2 по сети Ethernet.

После того, как <IP_адрес> введён, необходимо выбрать Enter. На экране управляющего компьютера появится приглашение к входу в систему (рис.7.1).

Приглашение к входу в систему

Рисунок 7.1

Далее необходимо выбрать кнопку «Вход».

На экране управляющего компьютера появится окно для ввода имени и пароля пользователя (рис. 7.2).

Для авторизации необходимо ввести имя пользователя, соответствующий пароль и выбрать кнопку «Вход». На экране управляющего компьютера появится главное окно графического WEB-интерфейса ССПТ-2 (рис. 7.3)

Окно авторизации пользователя

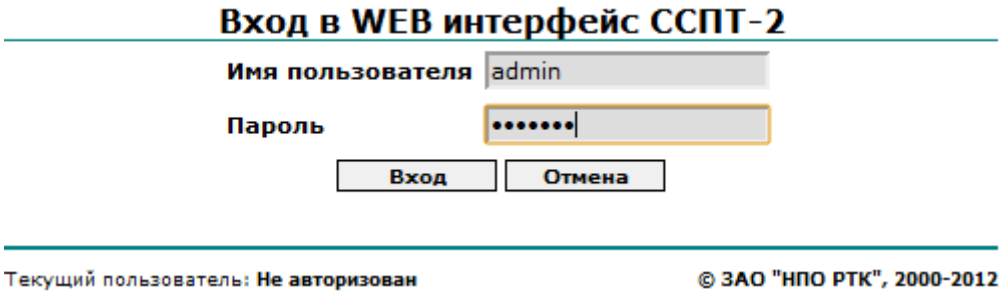

Рисунок 7.2

В первой строке окна расположены кнопки, которым соответствуют различные режимы настройки и управления ССПТ-2, а именно:

«Состояние» – общая системная информация и информация о состоянии фильтра. Это окно мы видим при входе на экран;

«Настройки» – системные настройки, настройки управления пользователями, настройки интерфейсов, установки NAT, настройки управления сетевыми пользователями, управление ключами аутентификации, настройки резервирования и авторизации через RADIUS- сервер;

«Правила» – добавление, удаление, редактирование правил фильтрации;

«Сессии» – управление сессиями и информация об установленных сессиях;

«Регистрация» – настройка подсистемы регистрации и просмотр зарегистрированной информации;

«Командная строка» – ввод команд интерфейса командной строки (рис.7.5).

Окно ввода команд интерфейса командной строки (рис.7.5) позволяет использовать все возможности интерфейса командной строки при управлении через WEB - интерфейс без переподключения к устройству.

Главное окно (Системная информация)

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка Выход

Система | Фильтрация

Состояние: Системная информация

Системная информация	
Центральный процессор	Pentium(R) Dual-Core CPU E5300 @ 2.60GHz
Ядер ЦПУ	2
Объем памяти	1063124992
Версия ПО ССПТ-2	FNP2_SNAPSHOT_1_3-p1.2 (Jul 3 2012)
Всего интерфейсов	3
Фильтрующие интерфейсы	2: eth0, eth1
Тайм-аут неактивности пользователя (сек)	600
Управляющий интерфейс	
IP-адрес	192.168.78.4
Маска сети	255.255.255.0
Несущая/Скорость	100baseTX/full-duplex
Состояние процессов	
Пакетная фильтрация	Выключить
Контроль целостности	
Авторизация	
Регистрация	
Резервирование	
Удаленное администрирование	
SNMP интерфейс	
Управление устройством	
	Останов/Перезагрузка

Справка

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.3

Главное окно (Фильтрация)

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка | Выход

Система | Фильтрация

Состояние: Фильтрация

Состояние фильтрации		
Фильтрация включена	07/04/12 12:04:46 (GMT)	
Фильтрация продолжается	7 дней 2 часа 9 минут 21 секунда	
Информация о трафике		
Фильтрующие интерфейсы	eth0	eth1
Несущая/Скорость	1000baseTX/full-duplex	1000baseTX/full-duplex
Кадров/байт получено	0/0	0/0
Включая		
Кадров/байт Ethernet II	0/0	0/0
Кадров/байт IEEE 802.3 LLC	0/0	0/0
Кадров/байт IEEE 802.3 RAW	0/0	0/0
Кадров/байт IEEE 802.3 SNAP	0/0	0/0
Пакетов/байт ARP	0/0	0/0
Пакетов/байт RARP	0/0	0/0
Дейтаграмм/байт IP	0/0	0/0
Сегментов/байт TCP	0/0	0/0
Дейтаграмм/байт UDP	0/0	0/0
Сообщений/байт ICMP	0/0	0/0
Дейтаграмм/байт IPX	0/0	0/0
Кадров/байт отправлено	0/0	0/0
Кадров/байт удалено	0/0	0/0
Поврежденных кадров/байт	0/0	0/0

Справка

Текущий пользователь: **admin** (admin)

© ЗАО "НПО РТК", 2000-2012

Рисунок 7.4

Окно ввода команд интерфейса командной строки

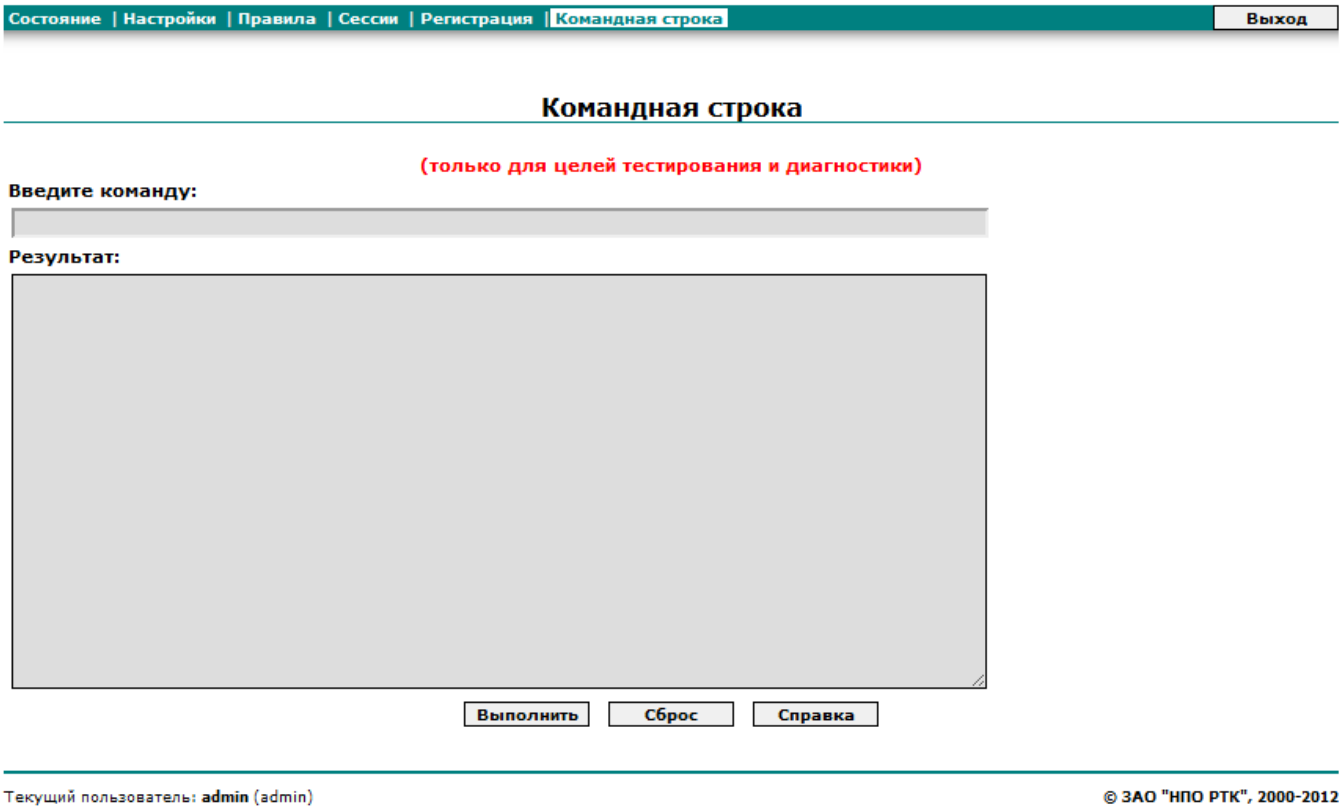

Рисунок 7.5

7.3. Настройки конфигурации и режимов

Для управления введения или изменения системных настроек необходимо в главном окне выбрать «Настройки» и в появившемся окне (рис.7.6) выбрать слово, соответствующее тем режимам или функциям, которые предполагается изменить («Система», «Пользователи», «Интерфейсы», «NAT», «Сетевые пользователи», «Ключи аутентификации», «Горячий резерв», «RADIUS»).

Все действия, которые необходимо выполнить для настроек режимов работы и параметров системы, определены в разделах 4, 6.

7.3.1. Системные настройки

Первоначально (или если выбрать «Система»), на экране управляющего компьютера появится окно настроек параметров системы (рис.7.6). В представленном окне возможно выполнение следующих действий:

- сохранение текущей конфигурации и ее выгрузки;
- применение, удаление или выгрузка любой из сохраненных конфигураций;
- изменение и обновление системного времени;
- отключение и перезагрузка устройства.

При выборе сохранения текущей конфигурации («Сохранить» в таблице «Текущая конфигурация») на экране управляющего компьютера появится окно (рис.7.7) для ввода имени, под которым конфигурация будет сохранена. После ввода имени конфигурации выбирается кнопка «Сохранить» и текущая конфигурация будет сохранена и обозначена в списке конфигураций установленным именем. При выборе показа текущей конфигурации на экране управляющего компьютера появится окно (рис.7.8) с текущей конфигурацией, которая может быть сохранена на управляющем компьютере.

Любая из дополнительных конфигураций может быть применена, показана на экране компьютера или удалена из списка дополнительных конфигураций (рис.7.9-7.11). Для этого необходимо выбрать соответствующую команду в строке соответствующей конфигурации таблицы «Дополнительные конфигурации».

Внимание!!! Дополнительную конфигурацию, в которой WEB-интерфейс или RADIUS требует смены состояния, возможно применить только пользователю **admin** и только при работе через **системную консоль**.

Окно настроек параметров системы

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка | Выход

Система | Пользователи | Интерфейсы | NAT | Сетевые пользователи | Ключи аутентификации | Горячий резерв | RADIUS

Настройки: Система

Текущая конфигурация

Сохранить | Показать

Дополнительные конфигурации

Имя конфигурации	Последнее обновление	Действия
Использовано: 0 Свободно: 16		

Системное время

Системная дата (дд.мм.гггг)	11.07.2012
Системное время (чч:мм:сс)	14:17:12
Часовой пояс	GMT+0000
NTP	отключено
IP-адрес NTP-сервера	не определено
Регистрация NTP	включено
Тайм-аут NTP (сек)	3600

Изменить | Обновить

Справка

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.6

Окно сохранения текущей конфигурации системы

Конфигурация: Сохранить

Имя конфигурации:	

Сохранить | Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.7

Выгрузка текущей конфигурации системы

```
interface control address 192.168.78.4/255.255.255.0
gateway set 192.168.78.254
interface control media auto
interface control acl clear
interface filter eth0 enable
interface filter eth0 media auto
interface filter eth1 enable
interface filter eth1 media auto
interface filter eth0 mirror disable
session enable
session ip enable
session ap disable
session log disable
session timeout tcp syn 5
session timeout tcp estab 86400
session timeout tcp fin 600
session timeout udp syn 5
session timeout udp estab 10
session timeout icmp syn 5
session timeout icmp estab 20
session table size 8192
session flood disable
session flood alarm disable
session flood threshold tcp 1000
session flood threshold udp 500
session flood threshold icmp 300
session flood rule lifetime 60
session flood rule log disable
session flood rule comments "Blocked flood attack"
system time ntp log enable
system time ntp timeout 3600
system time ntp delete
system fnpsh timeout 600
system snmp enable
system web enable
log packet enable
log export ftp clear
log export ftp disable
log export syslog disable
nat disable
nat log disable
nat authentication disable
nat authentication timeout 600
nat port 45000-60000
nat public mac 02:01:01:01:01:01
nat public delete
nat private mac 02:01:01:01:01:02
nat private delete
nat arp clear
nat redirect public disable
nat redirect clear
reserv disable
reserv interface active media 100
reserv interface active duplex full
reserv interface blocked media 10
reserv interface blocked duplex half
user radius timeout 5
user radius retry 3
user radius disable
```

Рисунок 7.8

Применение дополнительной конфигурации системы

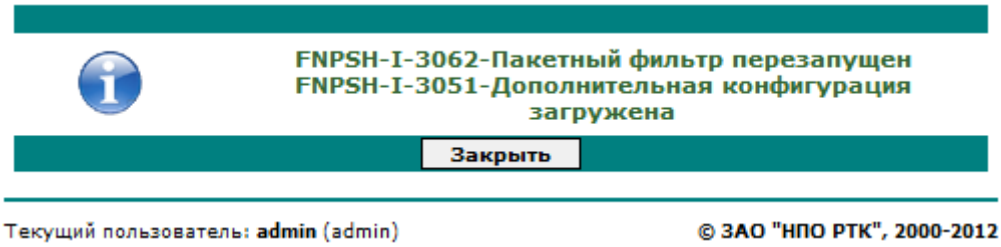

Рисунок 7.9

Выгрузка дополнительной конфигурации системы

```
interface control address 192.168.78.4/255.255.255.0
gateway set 192.168.78.254
interface control media auto
interface control acl clear
interface filter eth0 enable
interface filter eth0 media auto
interface filter eth1 enable
interface filter eth1 media auto
interface filter eth0 mirror disable
session enable
session ip enable
session ap disable
session log disable
session timeout tcp syn 5
session timeout tcp estab 86400
session timeout tcp fin 600
session timeout udp syn 5
session timeout udp estab 10
session timeout icmp syn 5
session timeout icmp estab 20
session table size 8192
session flood disable
session flood alarm disable
session flood threshold tcp 1000
session flood threshold udp 500
session flood threshold icmp 300
session flood rule lifetime 60
session flood rule log disable
session flood rule comments "Blocked flood attack"
system time ntp log enable
system time ntp timeout 3600
system time ntp delete
system fnpsh timeout 600
system snmp enable
system web enable
log packet enable
log export ftp clear
log export ftp disable
log export syslog disable
nat disable
nat log disable
nat authentication disable
nat authentication timeout 600
nat port 45000-60000
nat public mac 02:01:01:01:01:01
nat public delete
nat private mac 02:01:01:01:01:02
nat private delete
nat arp clear
nat redirect public disable
nat redirect clear
reserv disable
reserv interface active media 100
reserv interface active duplex full
reserv interface blocked media 10
reserv interface blocked duplex half
user radius timeout 5
user radius retry 3
user radius disable
```

Рисунок 7.10

Для обновления системного времени необходимо в таблице «Системное время» окна настроек параметров системы (рис.7.6) выбрать кнопку «Обновить». На экране управляющего компьютера появится окно обновления системного времени по данным сервера NTP (рис.7.13). При выборе «Обновить» появится сообщение о выполнении операции (рис.7.14).

Окно удаления дополнительной конфигурации системы

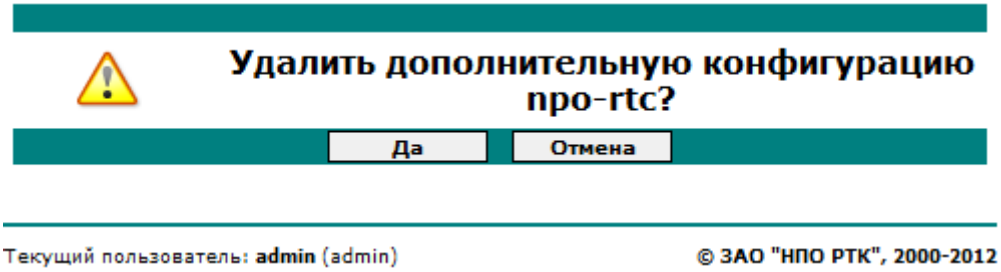

Рисунок 7.11

Подтверждение удаления дополнительной конфигурации системы

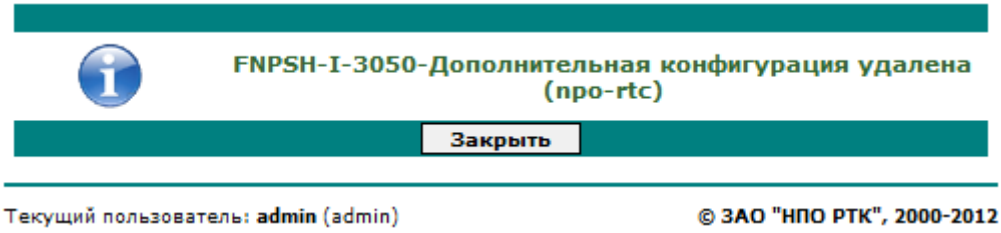

Рисунок 7.12

Окно обновления системного времени

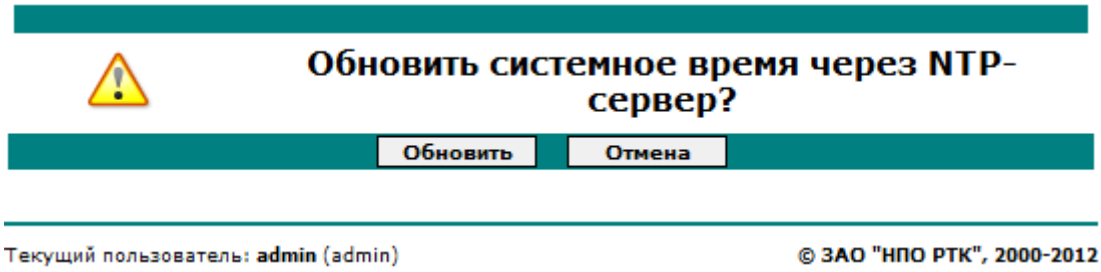

Рисунок 7.13

Подтверждение изменения системного времени

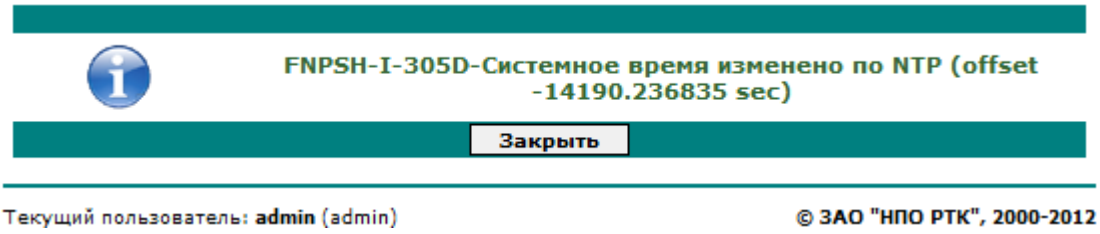

Рисунок 7.14

Для отключения или перезагрузки устройства необходимо в таблице «Системная информация» окна состояния системы (рис.7.3) выбрать кнопку «Останов/Перезагрузка». На экране управляющего компьютера появится окно отключения устройства (рис.7.15).

Окно отключения устройства

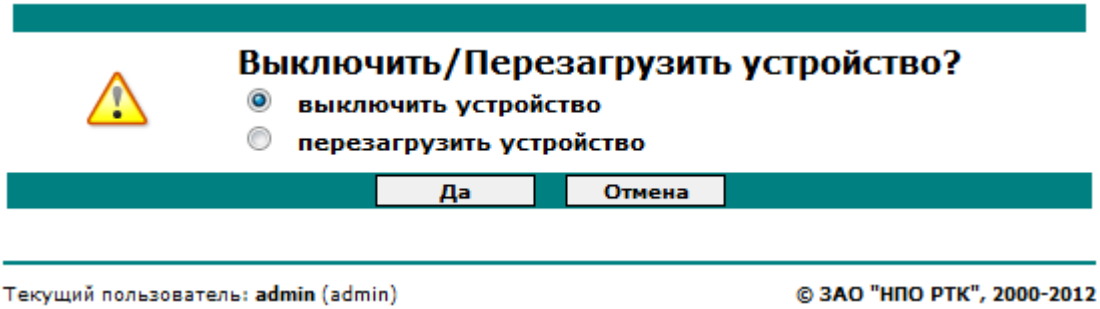

Рисунок 7.15

Для отключения или перезагрузки устройства необходимо выбрать соответствующую команду. Связь с устройством при этом прервется.

7.3.2. Управление пользователями

Для управления списком пользователей необходимо в главном окне (рис.7.3) выбрать «Настройки» и в появившемся окне (рис.7.6) выбрать слово «Пользователи». На экране управляющего компьютера появится окно просмотра и управления списком пользователей (рис. 7.16).

Для управления списком пользователей используются кнопки:

добавить;

изменить;

удалить.

При выборе кнопки «добавить» на экран выводится окно добавления пользователя (рис.7.17), в которое вводятся имя пользователя, его пароль (и пароль повторно) и полномочия (п.4.5 руководства). Для введения нового пользователя необходимо выбрать кнопку «сохранить».

Окно просмотра и настроек пользователей

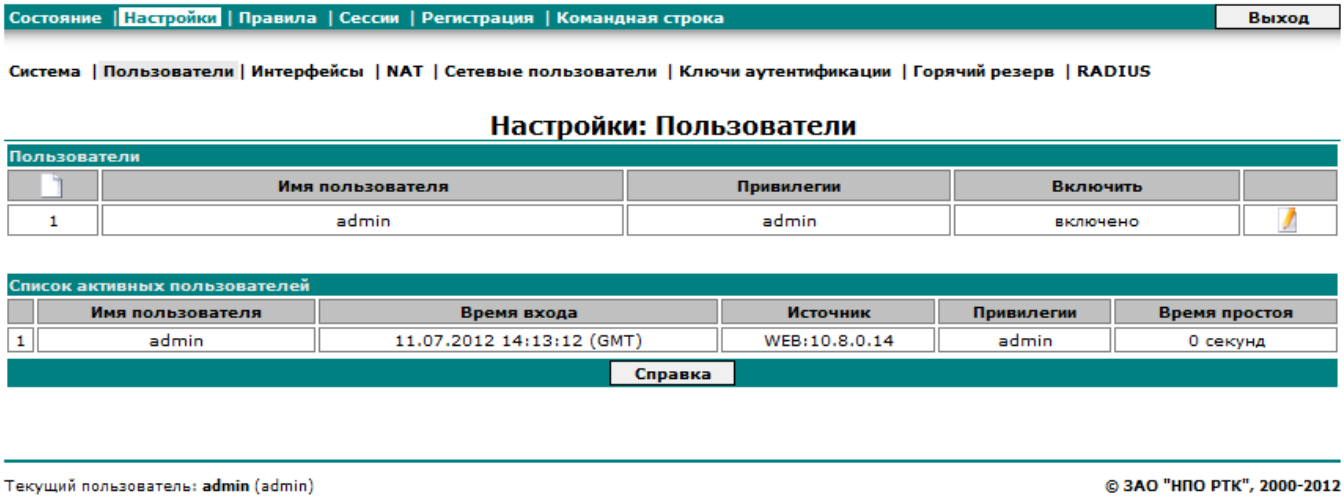

Рисунок 7.16

Для удаления пользователя необходимо выбрать кнопку «удалить». После подтверждения удаления администратором (рис.7.18) пользователь будет удален из списка пользователей.

Окно добавления пользователей

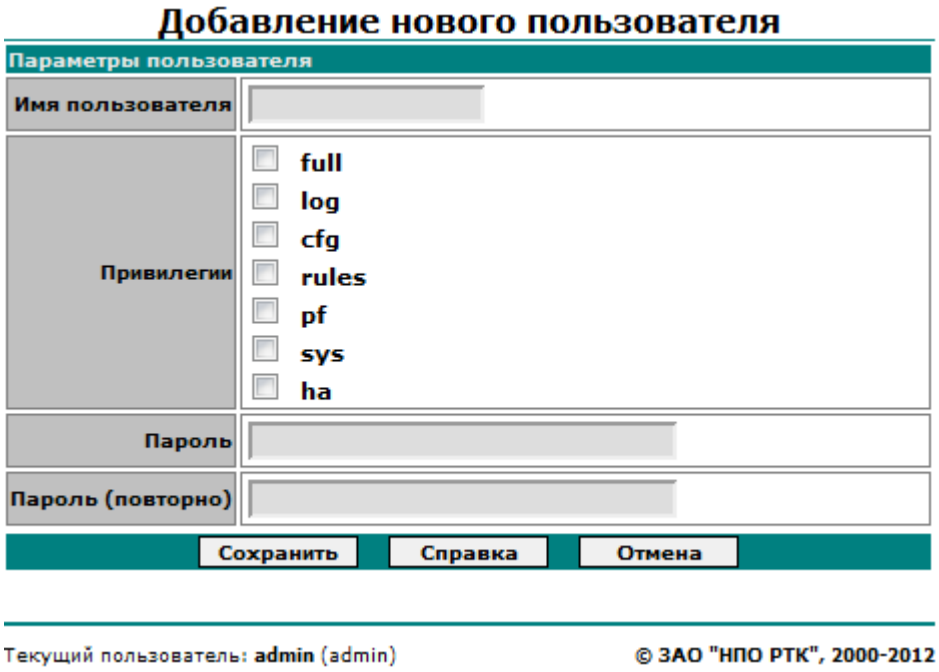

Рисунок 7.17

Окно удаления пользователя

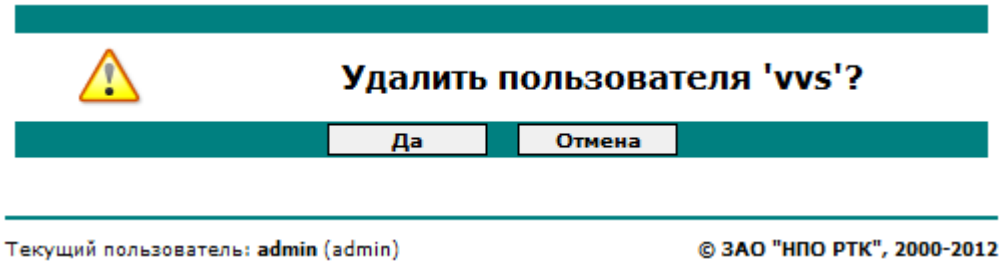

Рисунок 7.18

Для изменения параметров пользователя необходимо выбрать кнопку «изменить», и ввести новые данные в появившемся окне (рис.7.19).

Для подтверждения изменения параметров пользователя необходимо выбрать кнопку «сохранить».

После выполнения любой из указанных операций система сообщает о ее выполнении (рис.7.20).

Окно изменения данных пользователя

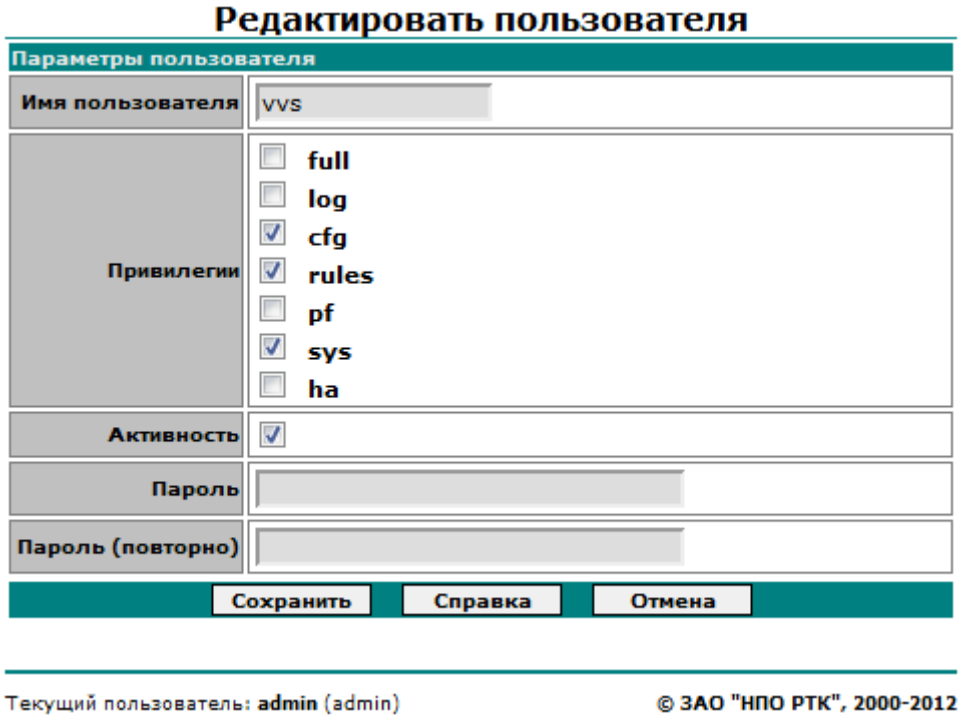

Рисунок 7.19

Подтверждение выполнения операции

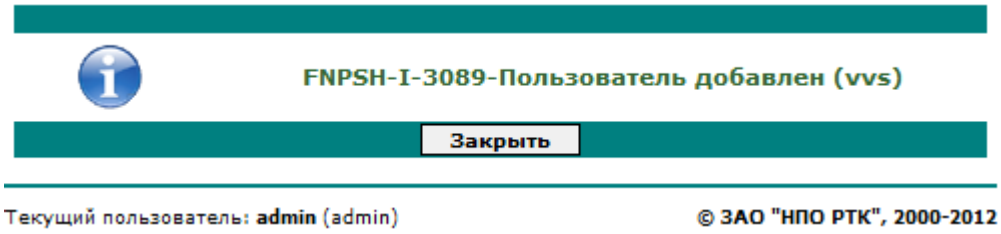

Рисунок 7.20

7.3.3. Настройки интерфейсов

Если в главном окне (рис.7.3) выбрать «Настройки», а в появившемся окне (рис. 7.6) выбрать «Интерфейсы», то на экране управляющего компьютера появится окно настроек интерфейсов устройства (рис.7.21). В представленном окне возможно выполнение следующих действий:

- редактирование настроек управляющего интерфейса и удаление маршрута по умолчанию;

- редактирование списка контроля доступа (IP-адресов управляющих компь-

ютеров);

- редактирование настроек фильтрующих интерфейсов.

Для редактирования настроек управляющего интерфейса необходимо в таблице «Управляющий интерфейс» выбрать кнопку «Изменить». На экране появится окно (рис.7.22) в котором можно произвести изменения перечисленных в нем настроек.

Если выбрать кнопку «Удалить», то на экране появится окно (рис.7.23) в котром можно произвести удаление маршрута по умолчанию.

Для редактирования списка контроля доступа (IP-адресов управляющих компьютеров) необходимо в таблице «Список Управления Доступом» выбрать кнопку добавить. На экране появится окно (рис.7.24) в котором можно ввести IP-адрес управляющего компьютера, с которого разрешен доступ к управляющему интерфейсу устройства.

Для удаления записи необходимо в соответствующей строке таблицы «Список Управления Доступом» выбрать кнопку удалить. Появится окно запроса на удаление записи (рис. 7.25). При выборе кнопки «Да» запись будет удалена.

Для очистки таблицы «Список Управления Доступом» необходимо выбрать кнопку «Очистить», и в появившемся окне (рис.7.26) выбрать «Да».

Для редактирования настроек фильтрующего интерфейса необходимо в таблице «Фильтрующие интерфейсы» выбрать кнопку изменить. На экране появится окно (рис.7.27) в котором можно изменить перечисленные параметры выбранного фильтрующего интерфейса устройства. Для применения настроек необходимо выбрать кнопку «Сохранить».

Окно настроек интерфейсов

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка — Выход

Система | Пользователи | Интерфейсы | NAT | Сетевые пользователи | Ключи аутентификации | Горячий резерв | RADIUS

Настройки: Интерфейсы

Управляющий интерфейс

	Установлено	Определено
Состояние	включено	включено
IP-адрес	192.168.78.4	192.168.78.4
Маска сети	255.255.255.0	255.255.255.0
Несущая/Скорость	autoselect	100baseTX/full-duplex

Шлюз по умолчанию

Состояние	включено	
IP-адрес	192.168.78.254	192.168.78.254

Удалить

Изменить

Список управления доступом

	IP-адрес	

Очистить

Фильтрующие интерфейсы

Интерфейс	Установлено			Определено		
	Состояние	Скорость	Зеркалирование	Состояние	Несущая/Скорость	
0:eth0	вкл	auto	отключено	вкл	1000baseTX/full-duplex	
1:eth1	вкл	auto	отключено	вкл	1000baseTX/full-duplex	

Справка

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.21

Изменение настроек управляющего интерфейса

Редактирование настроек управляющего интерфейса

Внимание! Связь может быть потеряна

Управляющий интерфейс

Состояние	☑ включено
IP-адрес	192.168.78.4
Маска сети	255.255.255.0
Несущая/Скорость	auto ☑ full-duplex

Шлюз по умолчанию

Состояние	☑ включено
IP-адрес	192.168.78.254

Сохранить | Справка | Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.22

Удаление маршрута по умолчанию

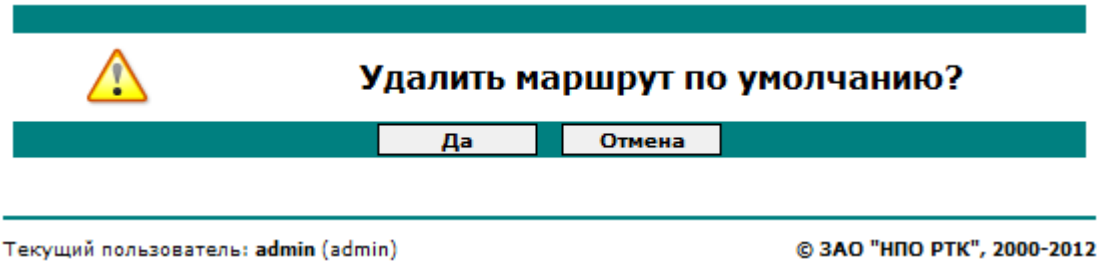

Рисунок 7.23

Окно добавления нового адреса

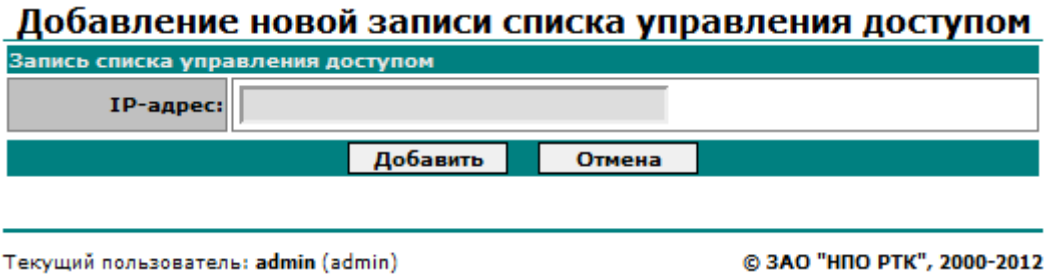

Рисунок 7.24

Удаление записи

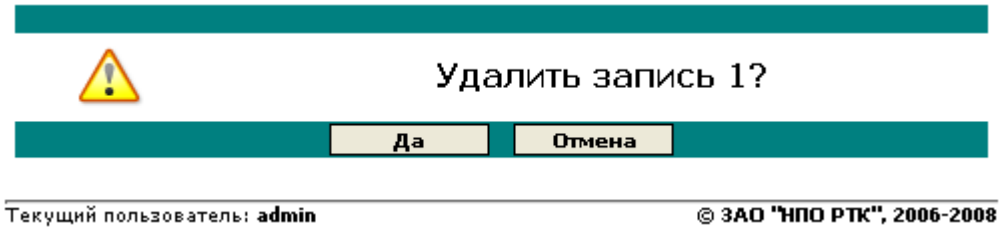

Рисунок 7.25

Очистка таблицы «Список Управления Доступом»

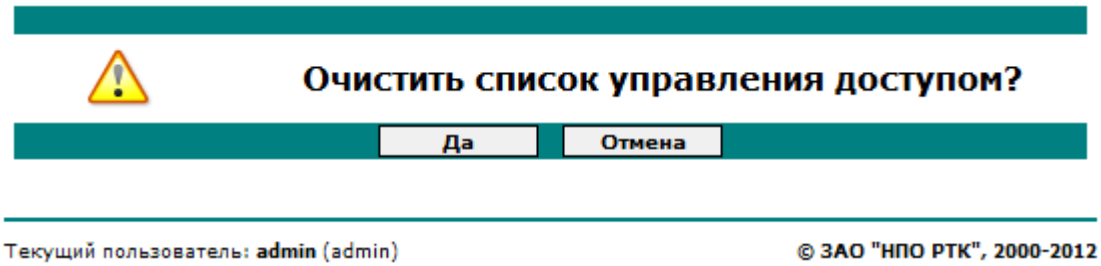

Рисунок 7.26

Окно настроек параметров фильтрующего интерфейса

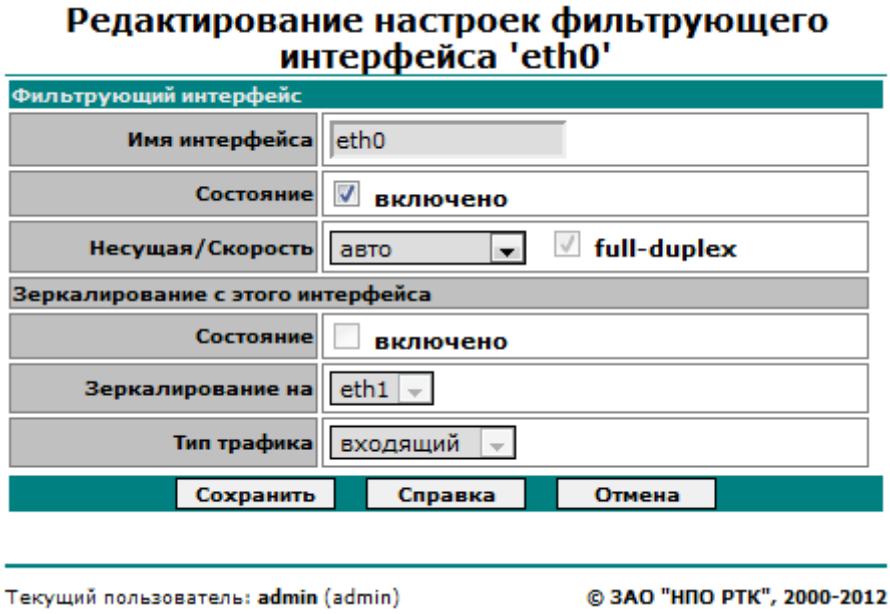

Рисунок 7.27

7.3.4. Настройка устройства для работы в системе фильтрации высокой готовности

Если в главном окне (рис.7.3) выбрать «Настройки», а в появившемся окне (рис. 7.6) выбрать «Горячий резерв», то на экране управляющего компьютера появится окно (рис.7.28) настроек устройства для работы в системе фильтрации высокой готовности (п.6.3). В представленном окне возможно выполнение следующих действий:

- редактирование настроек устройства для работы в системе фильтрации высокой готовности (режим «горячего резерва»);

- установить настройки горячего резерва по умолчанию;

- синхронизировать конфигурацию и правила фильтрации устройств, работающих в системе фильтрации высокой готовности.

Для редактирования настроек необходимо выбрать кнопку «Изменить». На экране появится окно (рис.7.29), в котором можно установить необходимые параметры устройства.

Окно настроек системы «горячего резерва»

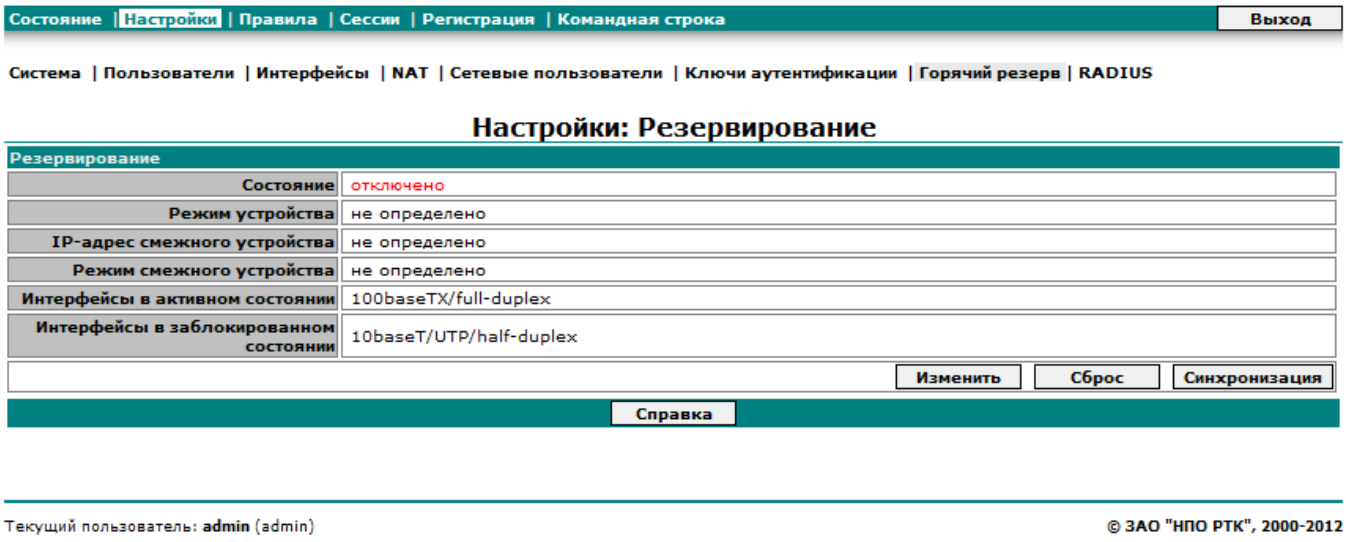

Рисунок 7.28

Окно редактирования настроек

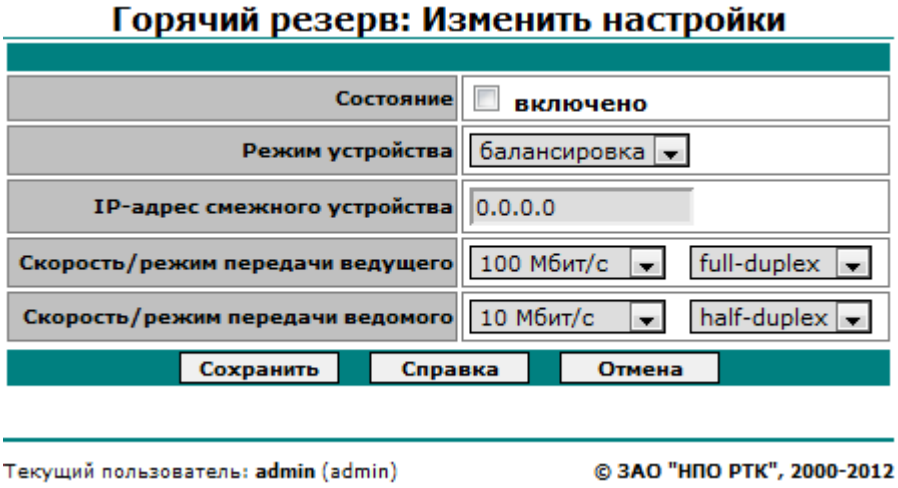

Рисунок 7.29

Для установки настроек горячего резерва по умолчанию необходимо выбрать кнопку «Сброс» и подтвердить установку параметров выбором «Да» в появившемся окне (рис. 7.30).

Для синхронизации конфигурации и правил фильтрации устройств, работающих в системе фильтрации высокой готовности, необходимо выбрать кнопку «Синхронизация», выбрать в появившемся окне (рис. 7.31) синхронизируемые параметры и подтвердить синхронизацию выбором «Синхронизация».

Значения устанавливаемых параметров и порядок настройки устройств, работающих в системе фильтрации высокой готовности представлены в п.6.3.

Установка параметров по умолчанию

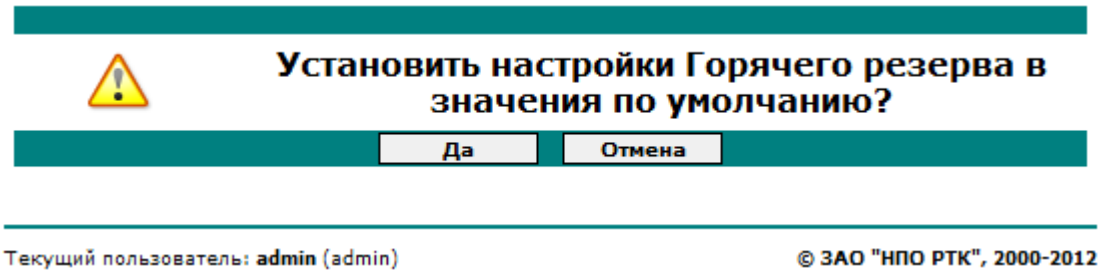

Рисунок 7.30

Синхронизация конфигурации и правил фильтрации

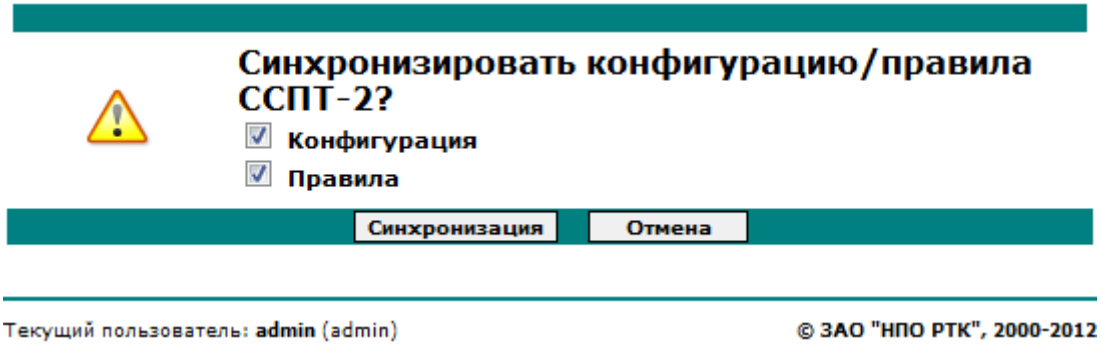

Рисунок 7.31

7.3.5. Настройка устройства для работы в режиме трансляции адресов (NAT)

Если в главном окне (рис.7.3) выбрать «Настройки», а в появившемся окне (рис. 7.6) выбрать «NAT», то на экране управляющего компьютера появится окно настроек для режима преобразования адресов (рис.7.32). В представленном окне возможно выполнение следующих действий:

- редактирование настроек NAT;
- редактирование и очистка правил переадресации NAT;
- настройка и редактирование ARP-таблиц.

Для редактирования настроек NAT необходимо выбрать кнопку «Изменить».

В появившемся окне (рис.7.33) можно произвести необходимые изменения настроек, для сохранения которых необходимо выбрать кнопку «Сохранить».

Для удаления настроек внешнего или внутреннего интерфейсов необходимо в соответствующей таблице (рис.7.32) выбрать кнопку «Удалить». На экране появиться окно запроса подтверждения команды (рис.7.34). После выбора «Да» появится сообщение об удалении настроек (рис.7.35).

Для редактирования правил переадресации NAT необходимо выбрать кнопку «Переадресация». Появившееся окно (рис.7.36) позволяет осуществить ввод нового правила переадресации (кнопка добавить) и очистку списка правил переадресации (кнопка «Очистить»).

В случае ввода нового правила в появившемся окне (рис.7.37) вводятся необходимые параметры и выбирается кнопка «Добавить».

При очистке списка правил, на экране появляется запрос на подтверждение очистки (рис.7.38), в котором можно выбрать «Да» и, тем самым очистить список, или «Отмена».

Окно настроек NAT

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка — Выход

Система | Пользователи | Интерфейсы | NAT | Сетевые пользователи | Ключи аутентификации | Горячий резерв | RADIUS

Настройки: NAT

Трансляция сетевых адресов	
Состояние	отключено
Регистрация отброшенных пакетов	отключено
Аутентификация сетевых пользователей	отключено
Тайм-аут неактивности сетевого пользователя (сек)	600
Диапазон портов	45000-60000
Внешний интерфейс	
Имя интерфейса	eth0
MAC-адрес	02:01:01:01:01:01
IP-адрес	не определено
Маска сети	не определено
Шлюз	не определено
Переадресация	отключено
	Удалить
Внутренний интерфейс	
Имя интерфейса	eth1
MAC-адрес	02:01:01:01:01:02
IP-адрес	не определено
Маска сети	не определено
	Удалить
DMZ	
Интерфейсы	
Переадресация	отключено
	Изменить / Переадресация / Таблица ARP

Справка

Текущий пользователь: **admin** (admin)

© ЗАО "НПО РТК", 2000-2012

Рисунок 7.32

Окно редактирования настроек NAT

Редактирование настроек NAT

Настройки трансляции сетевых адресов	
Состояние	☐ включено
Регистрация отброшенных пакетов	☐
Аутентификация сетевых пользователей	☐
Тайм-аут неактивности сетевого пользователя (сек)	600
Диапазон портов	45000 - 60000
Внешний интерфейс	
MAC-адрес	02:01:01:01:01:01
IP-адрес	0.0.0.0
Маска сети	0.0.0.0
Шлюз	0.0.0.0
Переадресация	☐
Внутренний интерфейс	
MAC-адрес	02:01:01:01:01:02
IP-адрес	0.0.0.0
Маска сети	0.0.0.0
DMZ	
Переадресация	☐

Сохранить | Справка | Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.33

Окно удаления настроек интерфейса

Удалить настройки внешнего интерфейса NAT?

Да | Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.34

Удаление настроек интерфейса

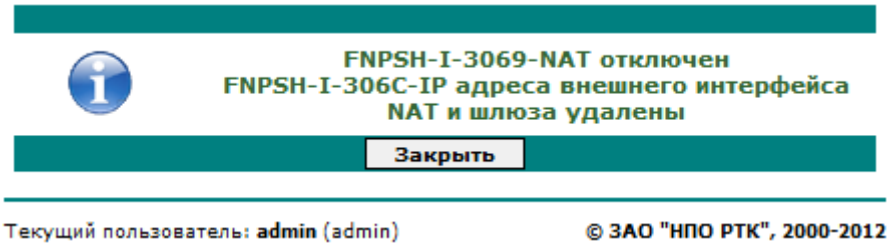

Рисунок 7.35

Окно настроек правил переадресации

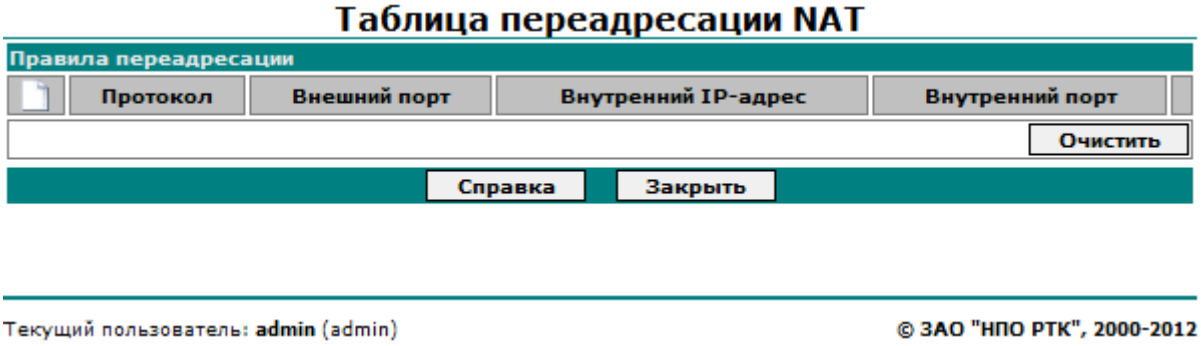

Рисунок 7.36

Окно добавления правила переадресации

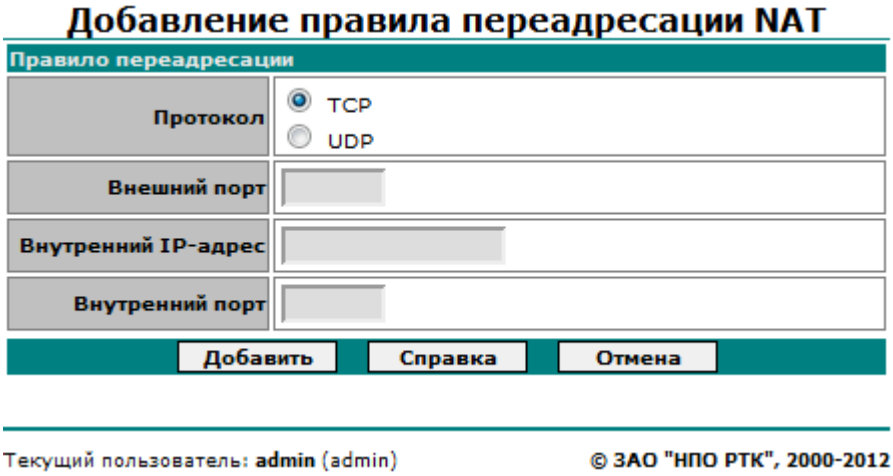

Рисунок 7.37

Очистка списка правил переадресации

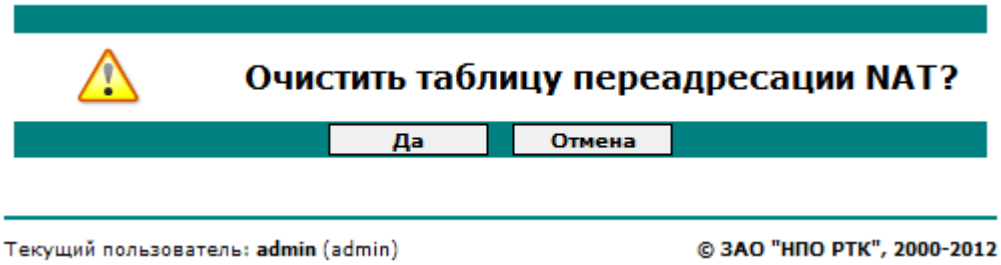

Рисунок 7.38

Для настройки и редактирования ARP-таблиц необходимо выбрать кнопку «Таблица ARP» (рис.7.32). В появившемся окне (рис.7.39) можно произвести необходимые изменения настроек. Для добавления записи в таблицу необходимо выбрать кнопку добавить.

Окно редактирования таблицы ARP

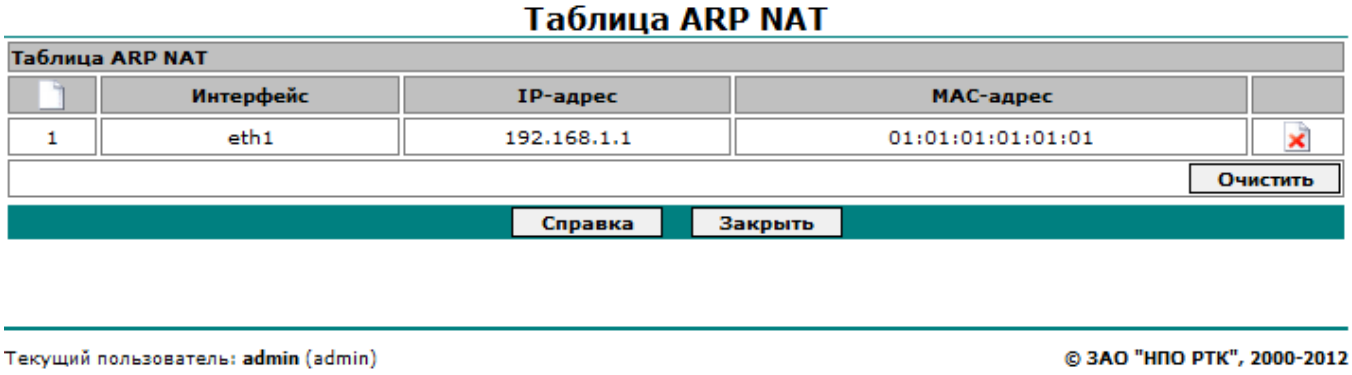

Рисунок 7.39

В появившемся окне (рис.7.40) вводятся необходимые параметры, для применения которых выбирается копка «Добавить». После чего на экране появится сообщение о добавлении записи (рис.7.41).

Окно добавления записи в таблицу ARP

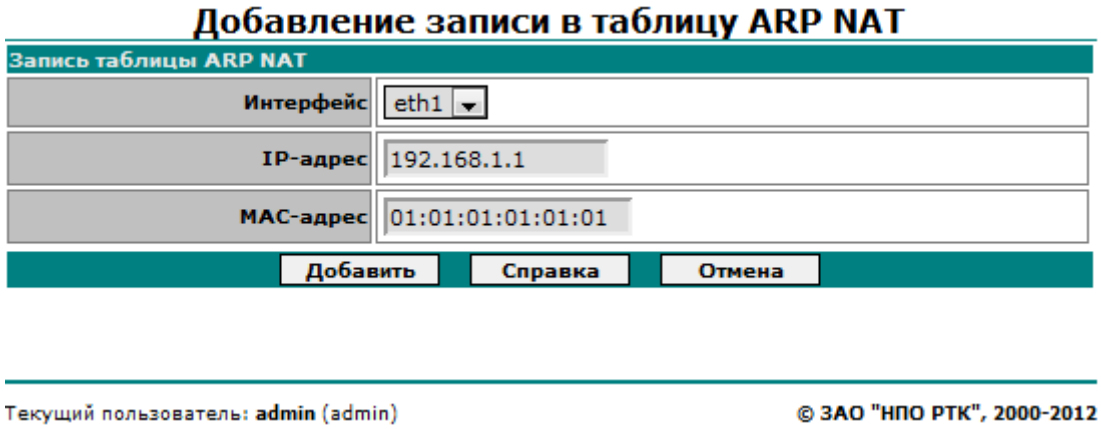

Рисунок 7.40

Добавление записи в таблицу ARP

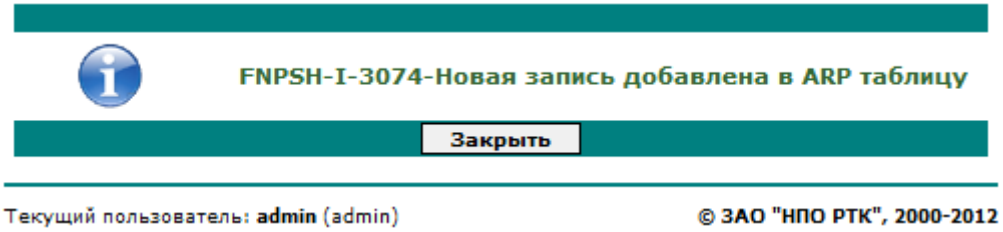

Рисунок 7.41

Для удаления записи в таблице необходимо выбрать кнопку удалить в соответствующей строке (рис.7.39). После чего на экране появится запрос на подтверждения команды (рис.7.42). Выбор «Да» приводит к удалению записи.

Удаление записи в таблице ARP

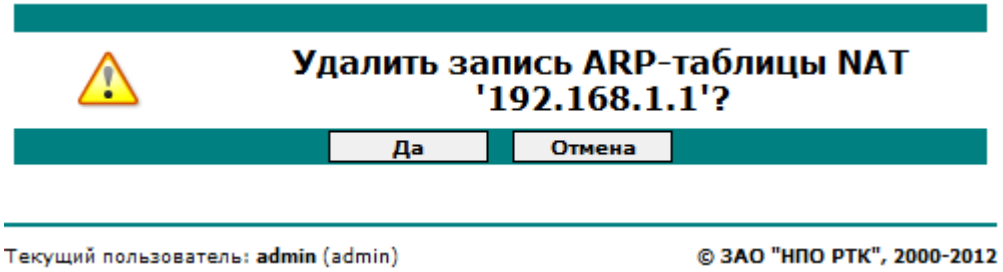

Рисунок 7.42

Для очистки таблицы необходимо выбрать кнопку «Очистить» (рис.7.39). После чего на экране появится запрос на подтверждения команды (рис.7.43). Выбор

«Да» приводит к удалению всех записей в таблице.

Очистка таблицы ARP

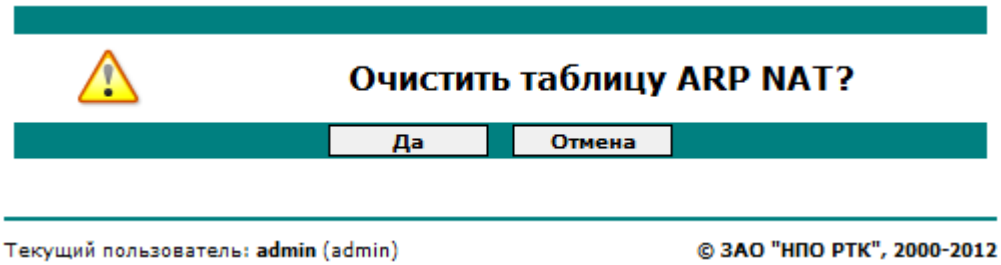

Рисунок 7.43

После выполнения действий по редактированию таблицы ARP на экране появляется сообщение о выполнении команды (рис.7.44).

Сообщение об очистке таблицы ARP

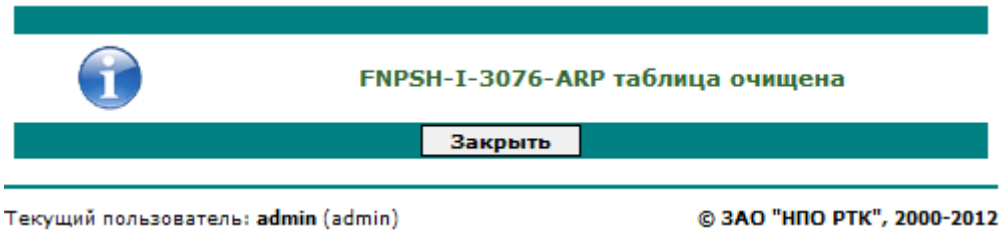

Рисунок 7.44

Значения устанавливаемых параметров и порядок настройки устройств, работающих в режиме NAT представлены в п.6.1.

7.3.6. Настройка устройства для идентификации пользователей через RADIUS - сервер

Если в главном окне (рис.7.3) выбрать «Настройки», а в появившемся окне (рис. 7.6) выбрать «RADIUS», то на экране управляющего компьютера появится окно настроек для режима идентификации пользователей через RADIUS – сервер (рис.7.45). Для редактирования настроек необходимо выбрать кнопку «Изменить».

В появившемся окне (рис.7.46) производится редактирование необходимых параметров и их сохранение (кнопка «Сохранить»). Порядок настройки подробно представлен в п. 4.1.1.

Окно настроек для аутентификации через RADIUS

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка — Выход

Система | Пользователи | Интерфейсы | NAT | Сетевые пользователи | Ключи аутентификации | Горячий резерв | RADIUS

Настройки: Аутентификация RADIUS

RADIUS	
Аутентификация RADIUS	отключено
Тайм-аут (сек)	5
Число повторов	3
Основной сервер	
IP-адрес	не определено
Секретный ключ	не определено
Порт	0
Запасной сервер	
IP-адрес	не определено
Секретный ключ	не определено
Порт	0

Изменить

Справка

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.45

Окно настроек для аутентификации через RADIUS

Редактирование настроек аутентификации RADIUS

RADIUS	
Тайм-аут (сек)	5
Число повторов	3
Основной сервер	
IP-адрес	
Секретный ключ	
Порт	0
Запасной сервер	
IP-адрес	
Секретный ключ	
Порт	0

Сохранить | Справка | Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.46

7.4. Правила фильтрации

7.4.1. Управление глобальными правилами и наборами правил

Для управления (введения, удаления или изменения) правилами фильтрации необходимо в главном окне (рис.7.3) выбрать «Правила». В появившемся окне (рис.7.47) находится основное меню по управлению правилами фильтрации. Которое позволяет ввести, удалить или отредактировать любое правило фильтрации любого типа.

Основное окно управления правилами фильтрации

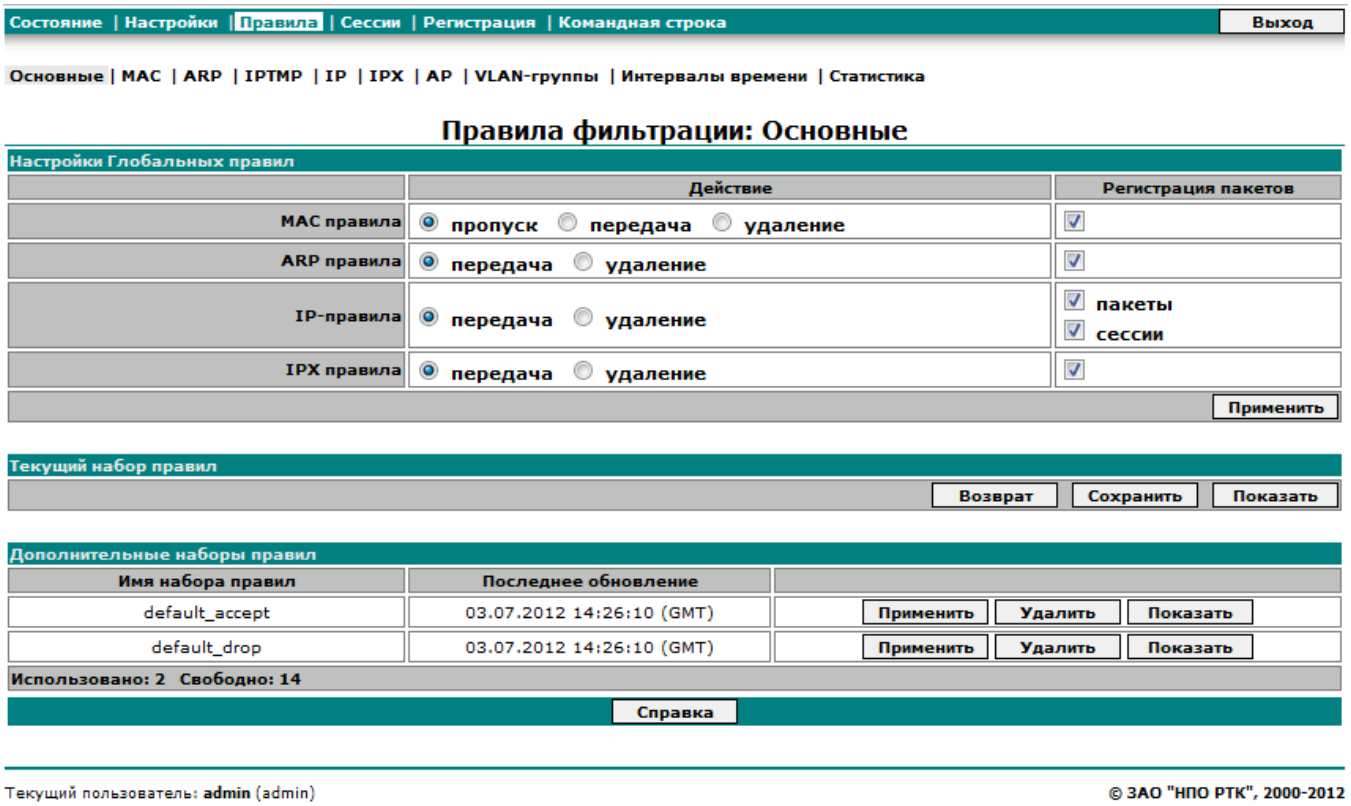

Рисунок 7.47

В основном окне возможно проведение следующих действий:

- редактирование глобальных правил фильтрации;

- сохранение и выгрузка на управляющий компьютер текущего набора правил фильтрации;

- установка в качестве текущего дополнительного набора правил, удаление дополнительного набора или его выгрузка на экран управляющего компьютера.

Редактирование глобальных правил (параметров «Действие» и «Регистрация пакетов») производится в таблице «Настройка Глобальных правил», применение заданных параметров осуществляется кнопкой «Применить». После чего на экран выводится сообщение о произведенных изменениях (рис.7.48).

Сообщение об изменении глобального IPX - правила

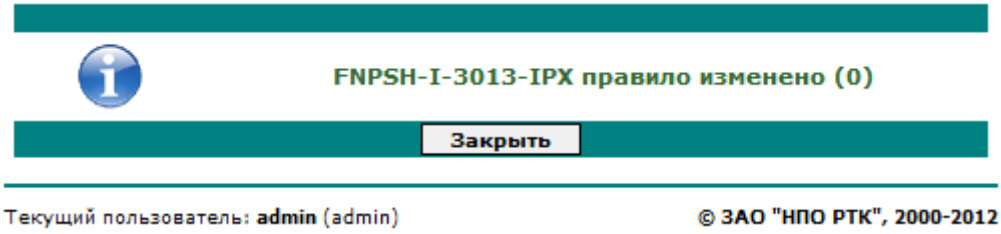

Рисунок 7.48

Сохранение и выгрузка на управляющий компьютер текущего набора правил фильтрации осуществляется, соответственно, кнопками «Сохранить» и «Выгрузить» в таблице «Текущий набор правил». При выборе кнопки «Сохранить» на экране появляется окно назначения имени набора правил (рис.7.49). Для сохранения текущего набора правил необходимо ввести имя набора и выбрать кнопку «Сохранить». На экране появится сообщение о выполнении команды сохранения (рис.7.50).

Сохранение текущего набора правил в списке дополнительных

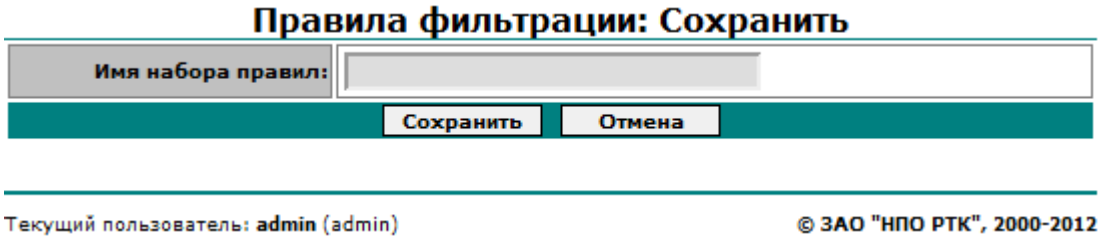

Рисунок 7.49

При выборе кнопки «Показать» на экране появляется окно с текущем набором правил (рис.7.51). Текущий набор правил может быть сохранен на управляющем компьютере.

Установка в качестве текущего дополнительного набора правил, удаление

дополнительного набора или его выгрузка на экран управляющего компьютера осуществляется, соответственно, кнопками «Применить», «Удалить» и «Выгрузить» в таблице «Дополнительные наборы правил».

Сообщение о сохранение текущего набора правил в качестве дополнительного

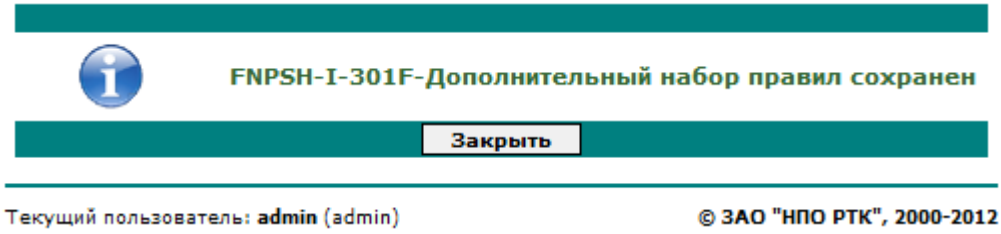

Рисунок 7.50

Выгрузка текущего набора правил

```
mac:0:pass:logpkt
arp:0:accept:logpkt
ip:0:accept:logpkt,logses
ipx:0:drop:logpkt
```

Рисунок 7.51

При выборе кнопки «Применить» на экране появляется сообщение о загрузке дополнительного набора правил в качестве текущего (рис.7.52).

При выборе кнопки «Выгрузить» на экране появляется окно с текущем набором правил (рис.7.53). Текущий набор правил может быть сохранен на управляющем компьютере.

При выборе кнопки «Удалить» на экране появляется запрос о подтверждении команды (рис.7.54). При выборе «Да» появляется сообщение об удалении дополнительного набора правил (рис.7.55).

Сообщение о применение дополнительного набора правил

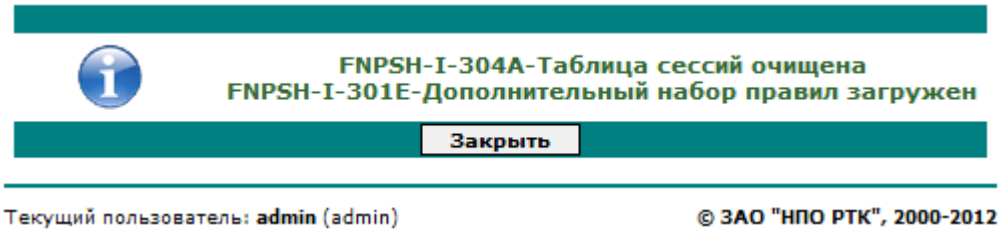

Рисунок 7.52

Выгрузка дополнительного набора правил

```
vlan:100:217:"Room-217 VLAN"
mac:0:accept:nolog
mac:100:accept:logpkt:0:1:12:00c0c0c0c0c0:00d0e0f0d0e0:active:testing...:any:any:any:noalarm
arp:0:accept:logpkt
ip:0:accept:logpkt,logses
ip:100:accept:logpkt,logses:1:0:0:tcp,udp:192.168.169.122:1024-
65535:192.168.169.126:53:any:any:any:any:any:any:active:"Laptop to DNS":any:defses:deftout:noapr:noalarm
ip:200:accept:logpkt,logses:1:0:0:tcp:192.168.169.122:1024-65535:any:80,8080:any:any:any:any:any:any:active:"Laptop to
WEB":100:defses:deftout:100:noalarm
ip:300:accept:logpkt,logses:0:1:0:tcp:89.110.227.0/24,195.208.113.128/27:1024-
65535:192.168.169.121:21:any:any:any:any:any:any:active:"Trusted networks to FTP":any:defses:deftout:noapr:noalarm
ipx:0:drop:nolog
ipx:100:drop:nolog:0::0:any:any:any:any:hello,rip:active::any:noalarm
time:12:any:21-31:any:any
time:100:feb:31:any:any
ap:100:drop:logpkt,logses:http:host=www.google.com:any:any:active:"Laptop deny www.google.com":noalarm
```

Рисунок 7.53

Удаление дополнительного набора правил

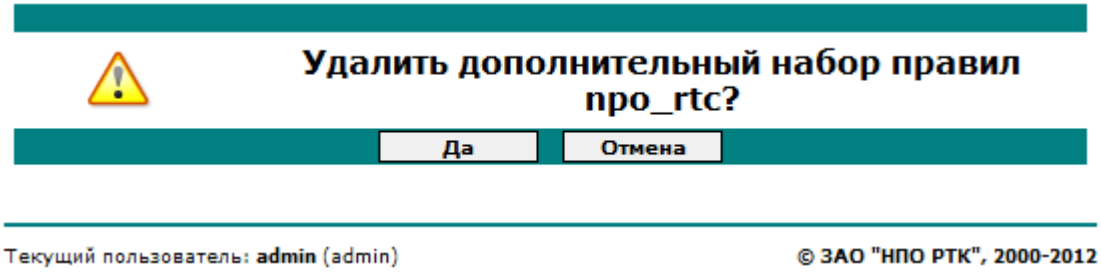

Рисунок 7.54

Сообщение об удалении дополнительного набора правил

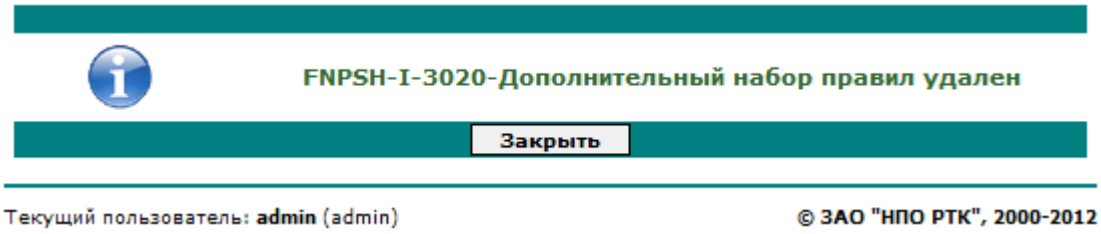

Рисунок 7.55

7.4.2. Управление MAC правилами

Для управления (введения, удаления или изменения) MAC правилами фильтрации необходимо в окне управления правилами фильтрации (рис.7.47) выбрать «MAC». В появившемся окне (рис.7.56) возможно проведение следующих действий по управлению MAC правилами:

- редактирование глобального MAC правила фильтрации (параметры «Действие» и «Регистрация пакетов»);

- установка нового, редактирование и удаление MAC правила фильтрации.

Таблица MAC правил фильтрации

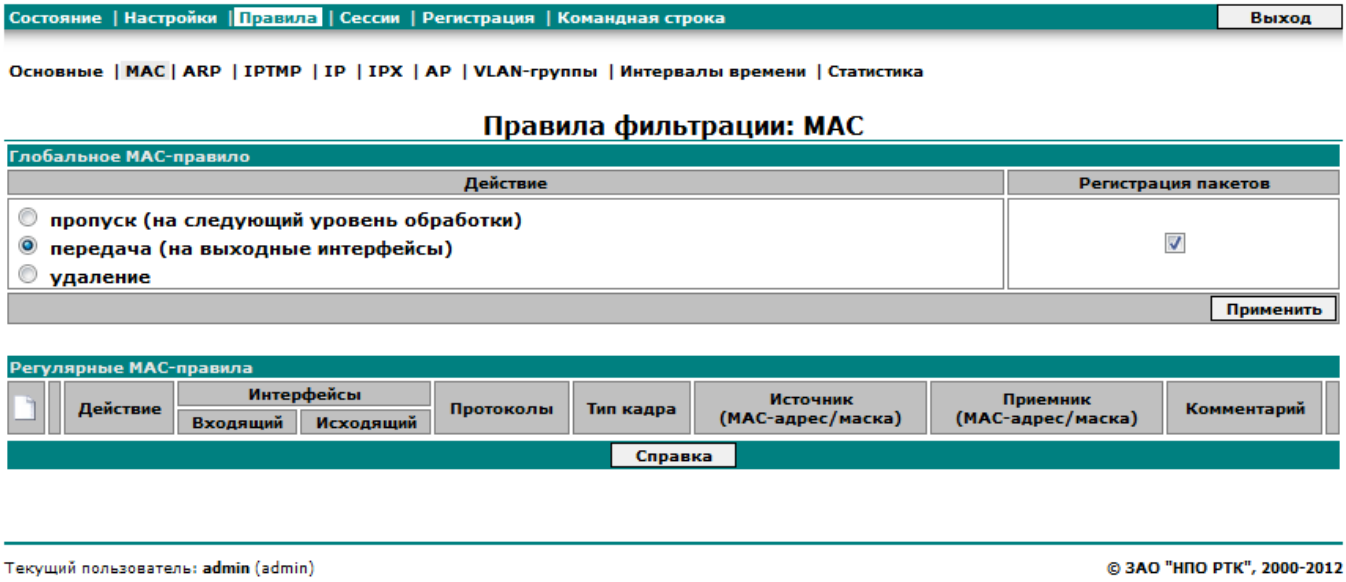

Рисунок 7.56

Редактирование глобального MAC правила производится в таблице «Глобальное MAC правило» выбором действия и/или установкой регистрации пакетов. Установка измененного глобального правила производится кнопкой «Применить» в той же таблице, при этом на экране появится сообщение об изменении правила (рис.7.57).

Сообщение о загрузке отредактированного глобального MAC правила

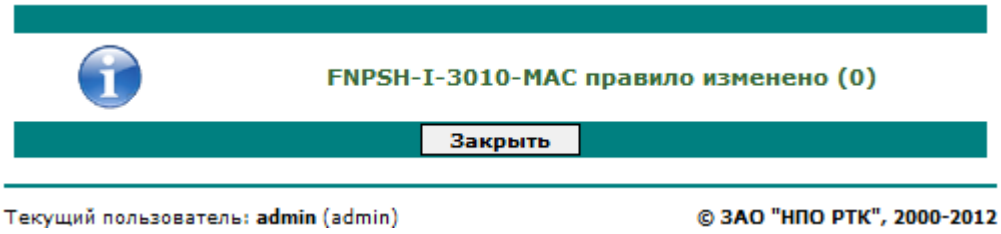

Рисунок 7.57

Для установки нового MAC правила необходимо выбрать кнопку в таблице «Регулярные MAC правила» (рис.7.56). На экране появится окно (рис.7.58) для ввода параметров устанавливаемого правила.

Добавление MAC правила фильтрации

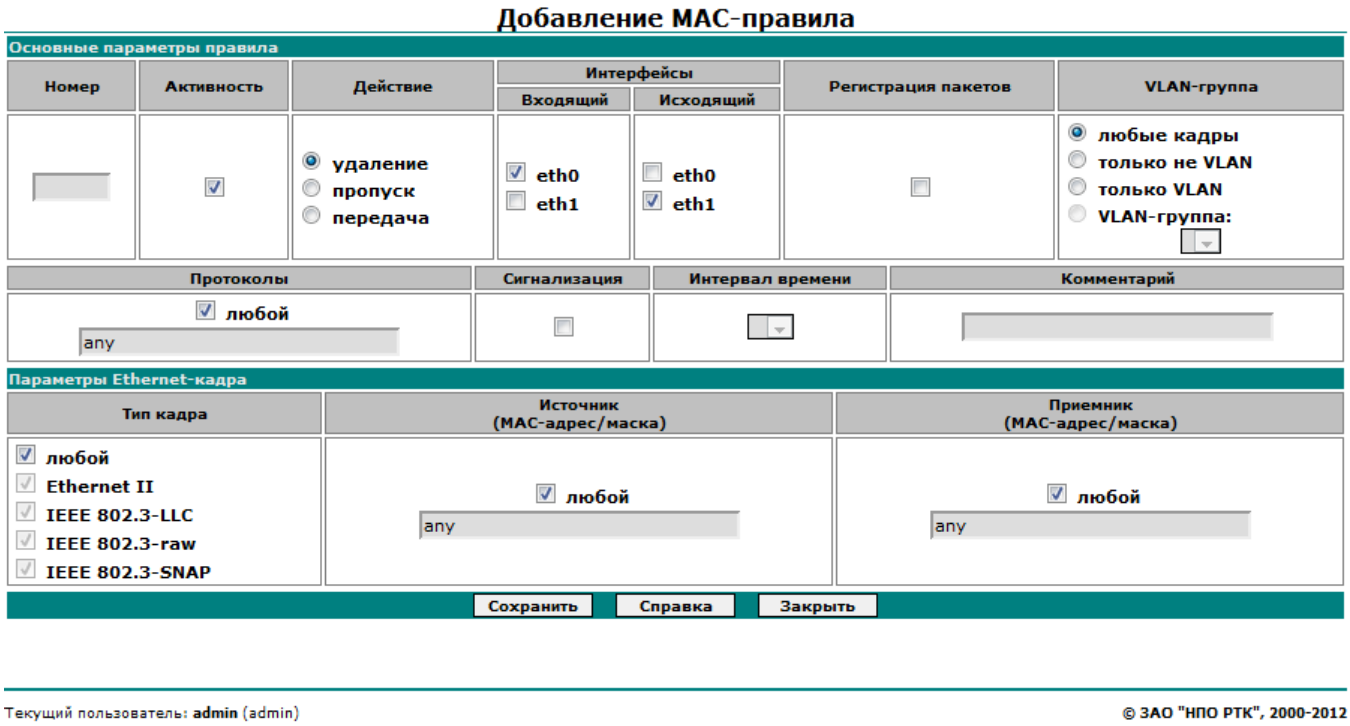

Рисунок 7.58

Для ввода нового правила в текущий набор правил необходимо установить нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.59).

Сообщение об установке нового MAC правила

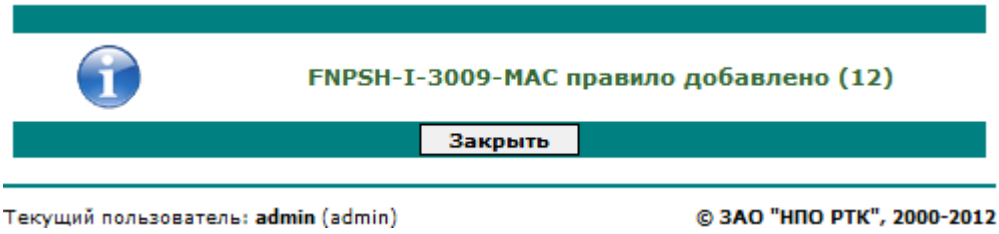

Рисунок 7.59

Для редактирования действующего MAC правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные MAC правила» (рис.7.56). На экране появится окно (рис.7.60) для редактирования выбранного MAC правила.

Редактирование MAC правила фильтрации

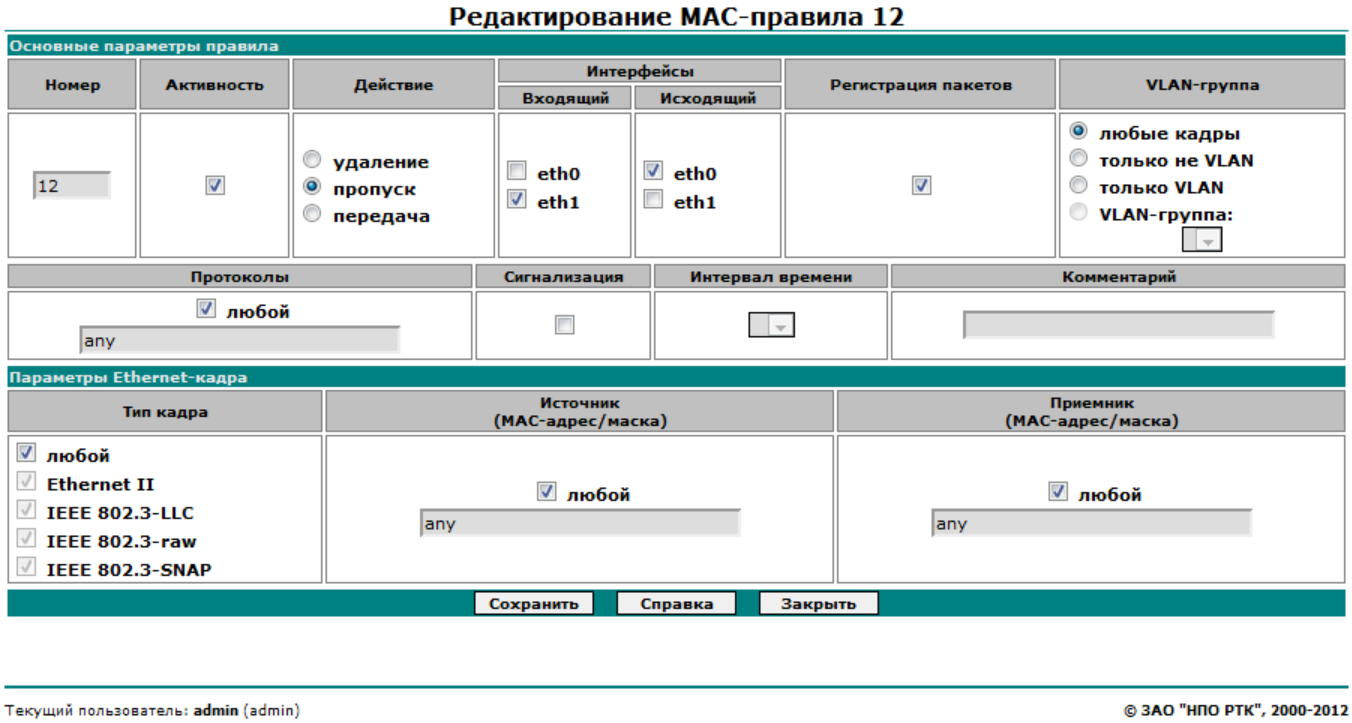

Рисунок 7.60

Для введения и сохранения изменения в действующем правиле необходимо отредактировать нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.61).

Сообщение об изменении MAC правила

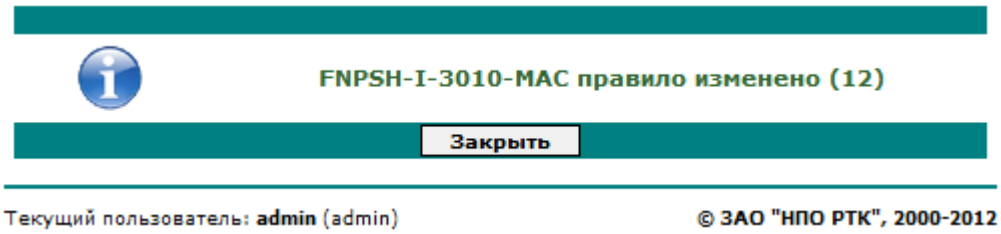

Рисунок 7.61

Для удаления действующего MAC правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные MAC правила» (рис.7.56). На экране появится запрос (рис.7.62) на подтверждение удаления выбранного MAC правила. Для удаления правила необходимо выбрать кнопку «Да», после чего на экране появится соответствующее сообщение (рис.7.63).

Удаление MAC правила

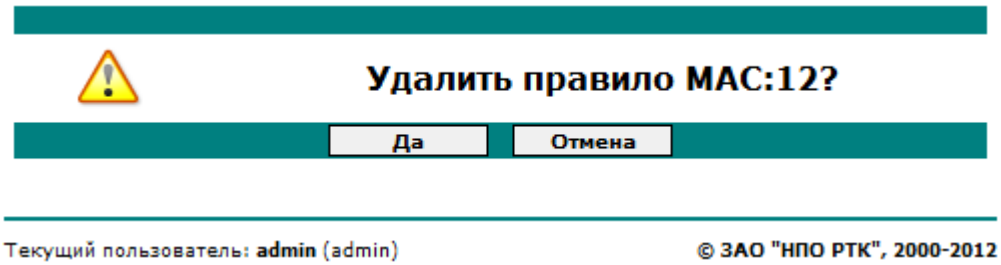

Рисунок 7.62

Сообщение об удалении MAC правила

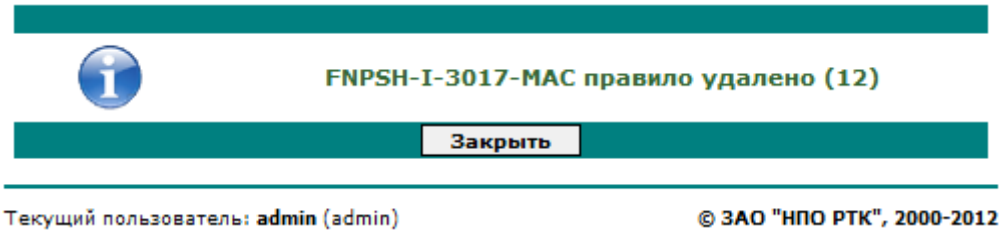

Рисунок 7.63

Редактирование параметра «Активность» (рис. 7.64) может производиться непосредственно в таблице «Регулярные MAC правила» (рис.7.56). При внесении

изменений в таблицу на экране появится соответствующее сообщение (рис.7.65).

Редактирование параметра «Активность»

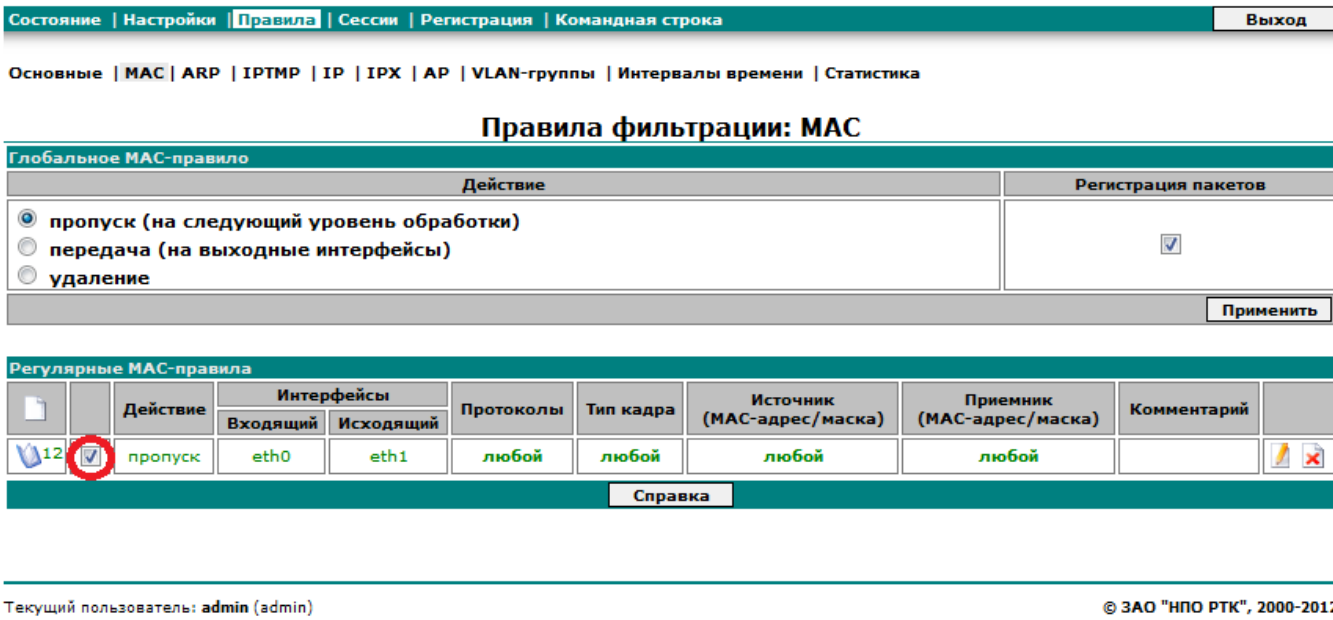

Рисунок 7.64

Сообщение об изменении MAC правила

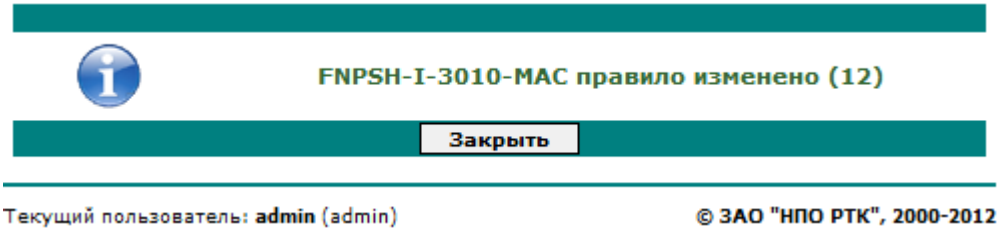

Рисунок 7.65

7.4.3. Управление ARP правилами

Для управления (введения, удаления или изменения) ARP правилами фильтрации необходимо в окне управления правилами фильтрации (рис.7.47) выбрать «ARP». В появившемся окне (рис.7.66) возможно проведение следующих действий по управлению ARP правилами:

- редактирование глобального ARP правила фильтрации (параметры «Действие» и «Регистрация пакетов»);

- установка нового, редактирование и удаление ARP правила фильтрации.

Таблица ARP правил фильтрации

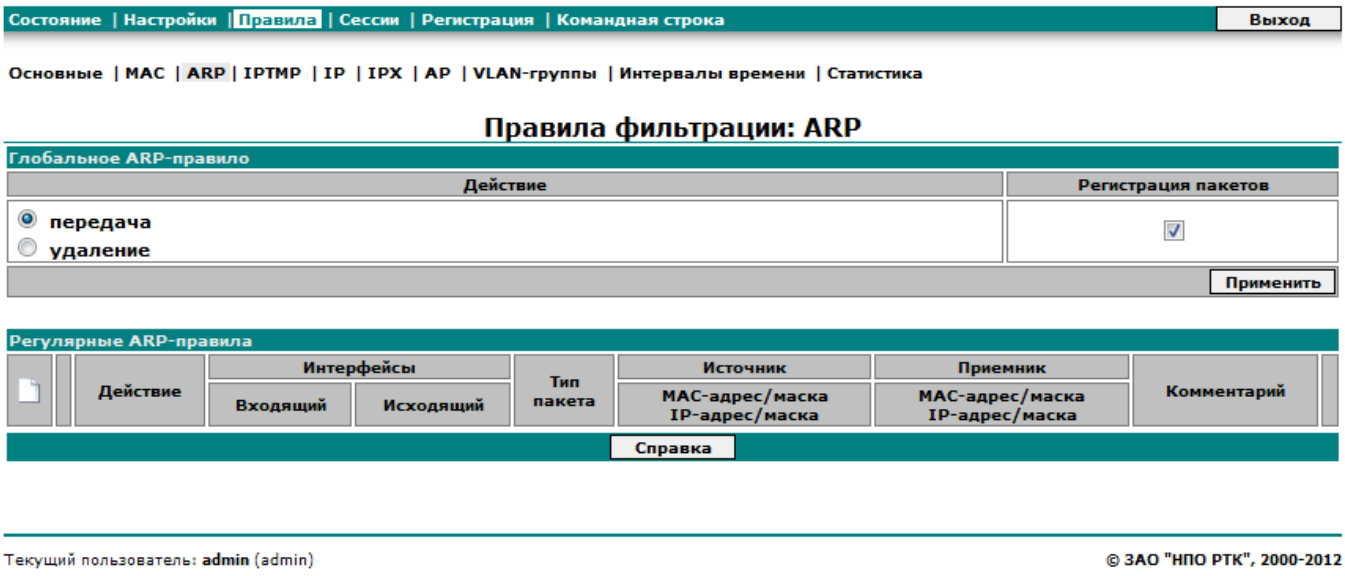

Рисунок 7.66

Редактирование глобального ARP правила производится в таблице «Глобальное ARP правило» выбором действия и/или установкой регистрации пакетов. Установка измененного глобального правила производится кнопкой «Применить» в той же таблице, при этом на экране появится сообщение об изменении правила (рис.7.67).

Для установки нового ARP правила необходимо выбрать кнопку в таблице «Регулярные ARP правила» (рис.7.66). На экране появится окно (рис.7.68) для ввода параметров устанавливаемого правила.

Сообщение о загрузке отредактированного глобального ARP правила

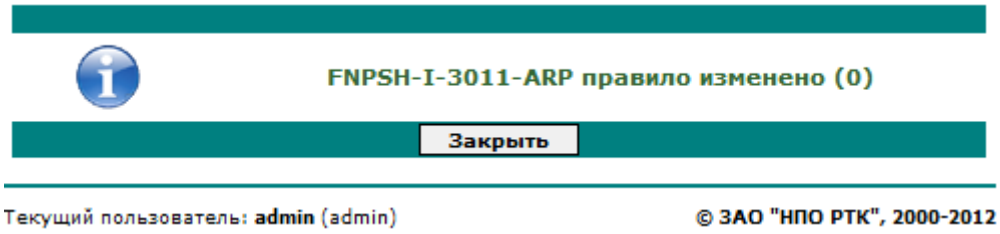

Рисунок 7.67

Добавление ARP правила фильтрации

Добавление ARP-правила

Основные параметры правила

Номер	Активность	Действие	Интерфейсы		Регистрация пакетов	VLAN-группа	Сигнализация	Интервал времени	Комментарий
			Входящий	Исходящий					
100	☑	◉ удаление ○ пропуск	☑ eth0 ☐ eth1	☐ eth0 ☑ eth1	☑	◉ любые кадры ○ только не VLAN ○ только VLAN ○ VLAN-группа:	☑		

Параметры ARP-пакета

Тип пакета	Источник		Приемник	
	MAC-адрес/маска	IP-адрес/маска	MAC-адрес/маска	IP-адрес/маска
☑ любой ☑ ARP-запрос ☑ ARP-ответ ☑ RARP-запрос ☑ RARP-ответ	☑ любой any	☑ любой any	☑ любой any	☑ любой any

Сохранить | Справка | Закрыть

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.68

Для ввода нового правила в текущий набор правил необходимо установить нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.69).

Сообщение об установке нового ARP правила

FNPSH-I-300A-ARP правило добавлено (100)

Закрыть

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.69

Для редактирования действующего ARP правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные ARP правила» (рис.7.66). На экране появится окно (рис.7.69) для редактирования выбранного ARP правила.

Редактирование ARP правила фильтрации

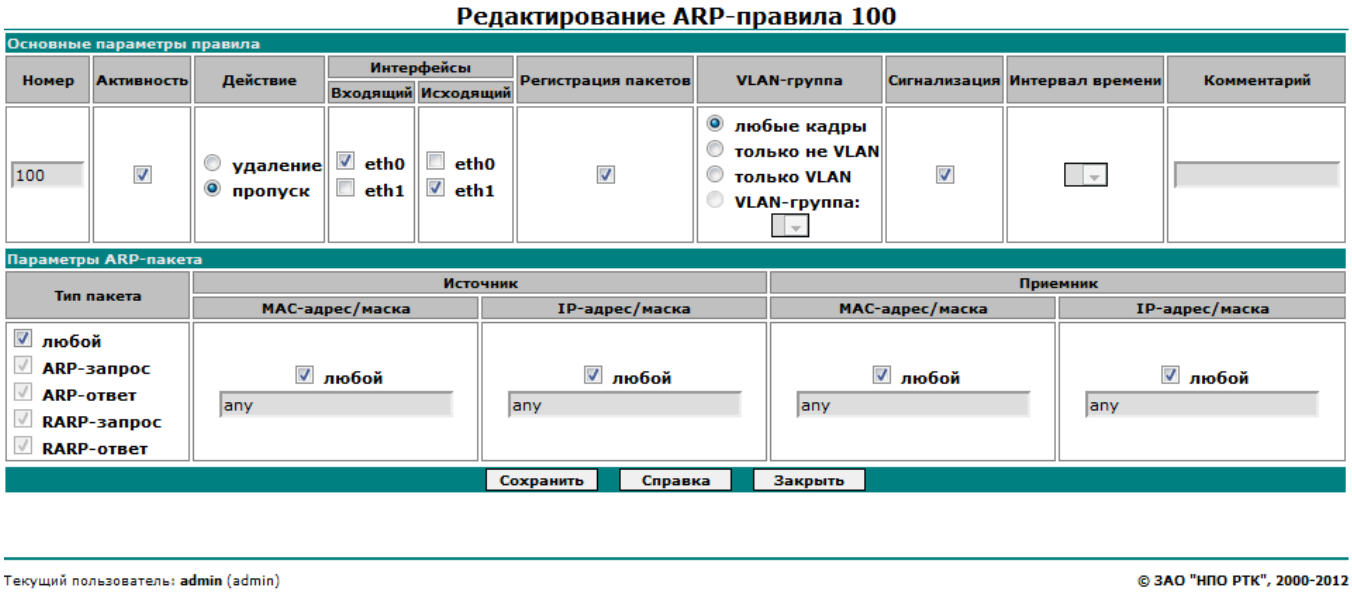

Рисунок 7.70

Для введения и сохранения изменения в действующем правиле необходимо отредактировать нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.71).

Сообщение об изменении ARP правила

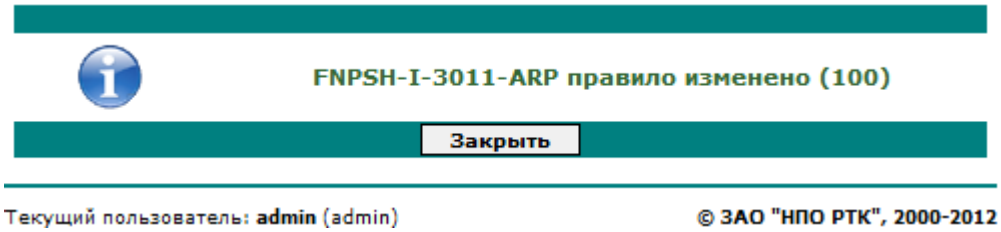

Рисунок 7.71

Для удаления действующего ARP правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные ARP правила» (рис.7.66). На экране появится запрос (рис.7.72) на подтверждение удаления выбранного ARP правила. Для удаления правила необходимо выбрать кнопку «Да», после чего на экране появится соответствующее сообщение (рис.7.73).

Удаление ARP правила

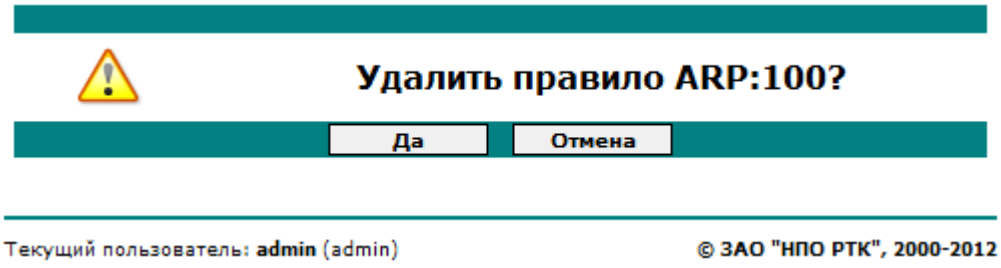

Рисунок 7.72

Сообщение об удалении ARP правила

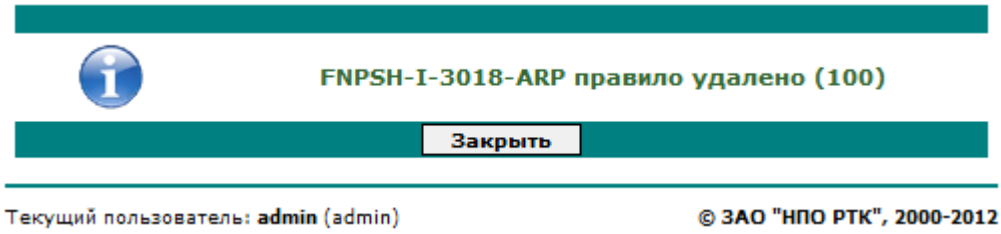

Рисунок 7.73

Редактирование параметра «Активность» (рис. 7.74) может производиться непосредственно в таблице «Регулярные ARP правила» (рис.7.66). При внесении изменений в таблицу на экране появится соответствующее сообщение (рис.7.75).

Редактирование параметра «Активность»

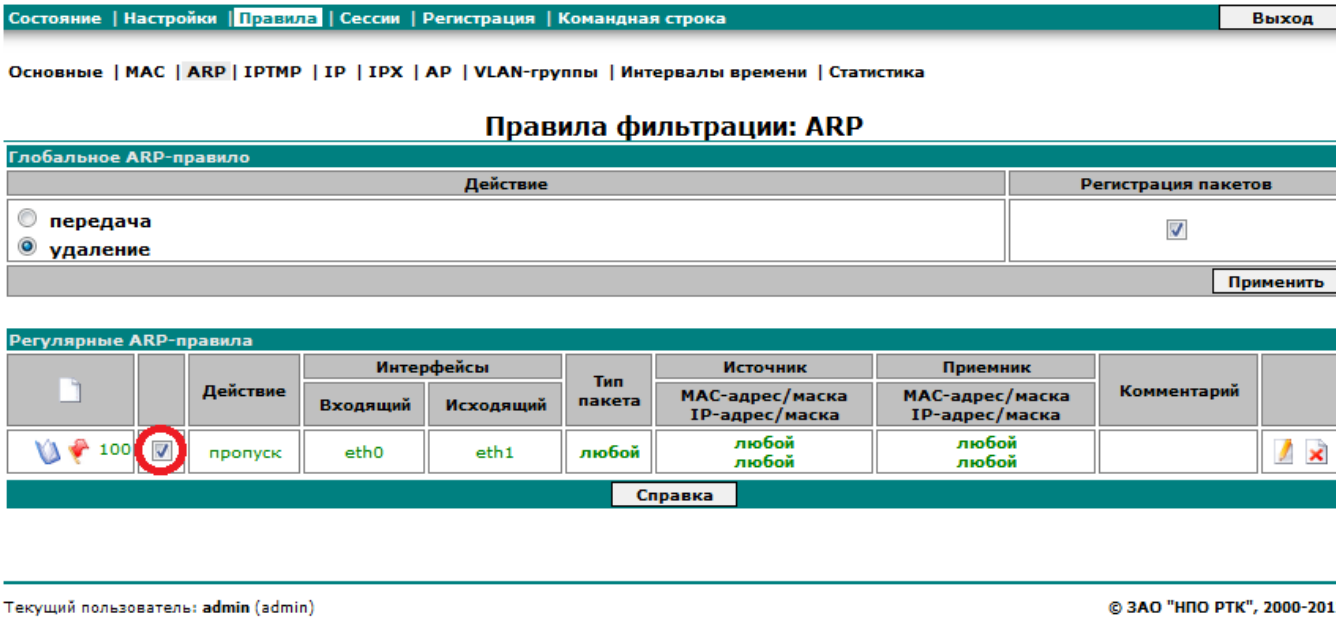

Рисунок 7.74

Сообщение об изменении ARP правила

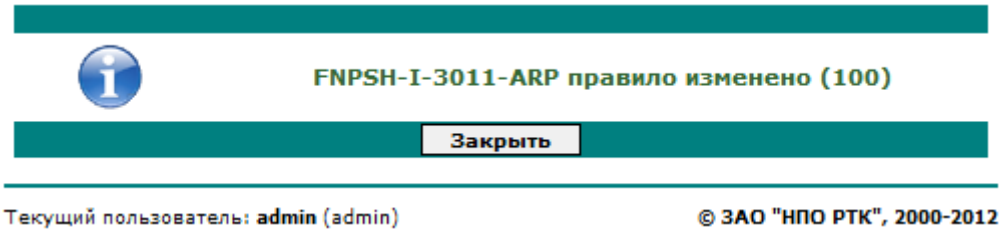

Рисунок 7.75

7.4.4. Управление IPX правилами

Для управления (введения, удаления или изменения) IPX правилами фильтрации необходимо в окне управления правилами фильтрации (рис.7.47) выбрать «IPX». В появившемся окне (рис.7.76) возможно проведение следующих действий по управлению IPX правилами:

- редактирование глобального IPX правила фильтрации (параметры «Действие» и «Регистрация пакетов»);
- установка нового, редактирование и удаление IPX правила фильтрации.

Таблица IPX правил фильтрации

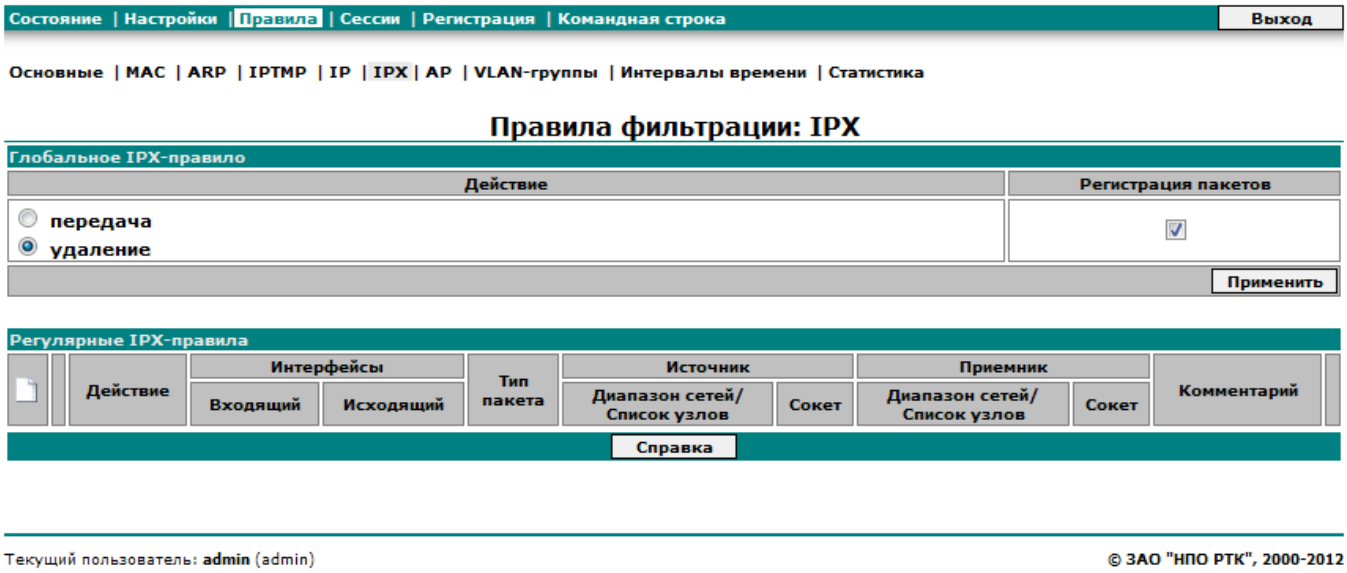

Рисунок 7.76

Редактирование глобального IPX правила производится в таблице «Глобаль-

ное IPX правило» выбором действия и/или установкой регистрации пакетов. Установка измененного глобального правила производится кнопкой «Применить» в той же таблице, при этом на экране появится сообщение об изменении правила (рис.7.77).

Для установки нового IPX правила необходимо выбрать кнопку в таблице «Регулярные IPX правила» (рис.7.76). На экране появится окно (рис.7.78) для ввода параметров устанавливаемого правила.

Сообщение о загрузке отредактированного глобального IPX правила

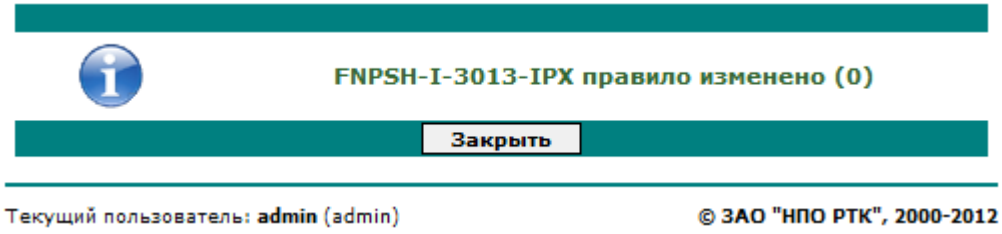

Рисунок 7.77

Добавление IPX правила фильтрации

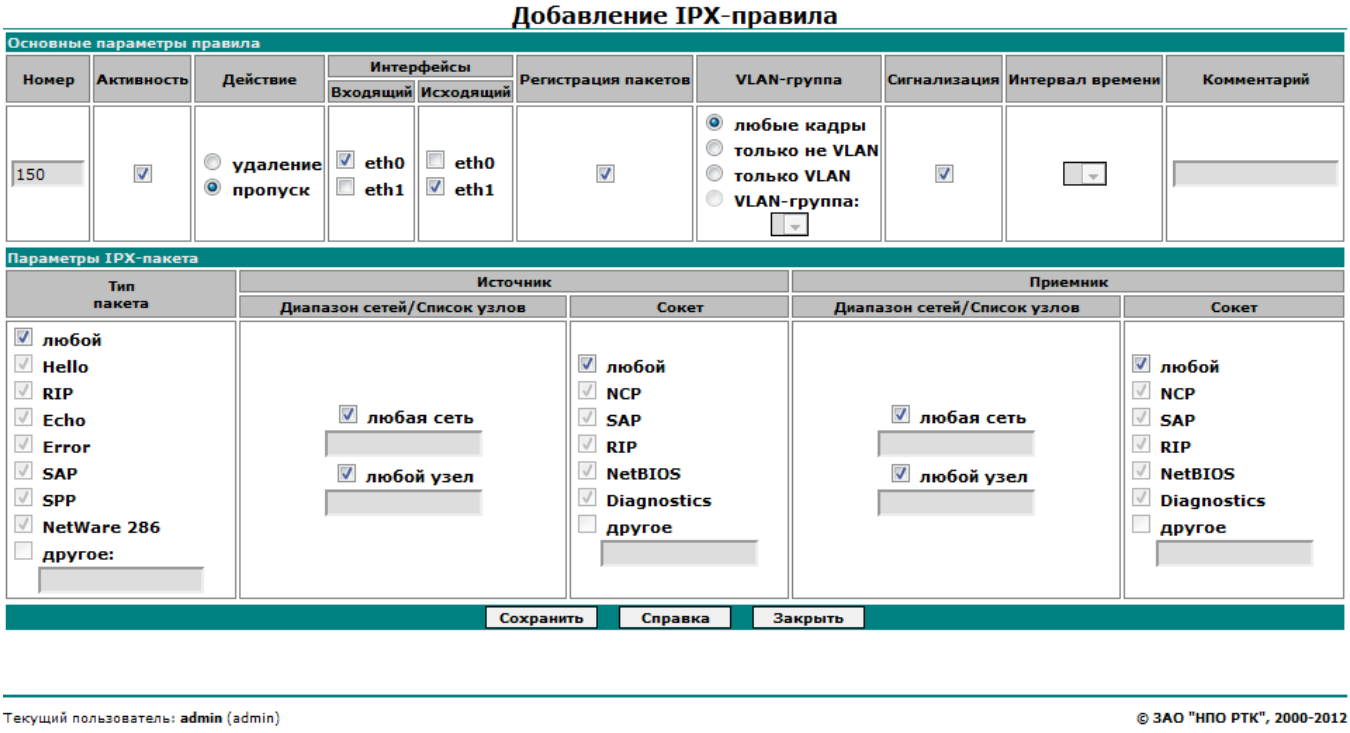

Рисунок 7.78

Для ввода нового правила в текущий набор правил необходимо установить нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.79).

Для редактирования действующего IPX правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные IPX правила» (рис.7.76). На экране появится окно (рис.7.80) для редактирования выбранного IPX правила.

Сообщение об установке нового IPX правила

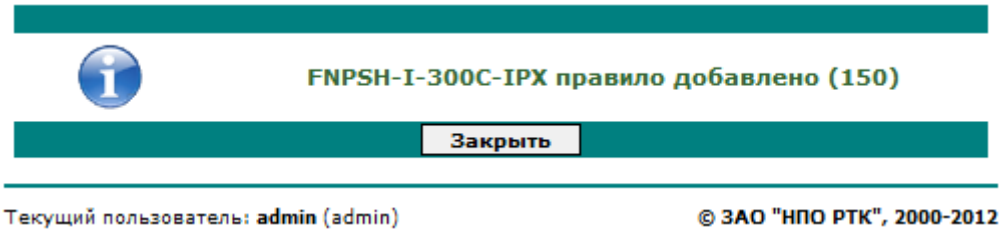

Рисунок 7.79

Редактирование IPX правила фильтрации

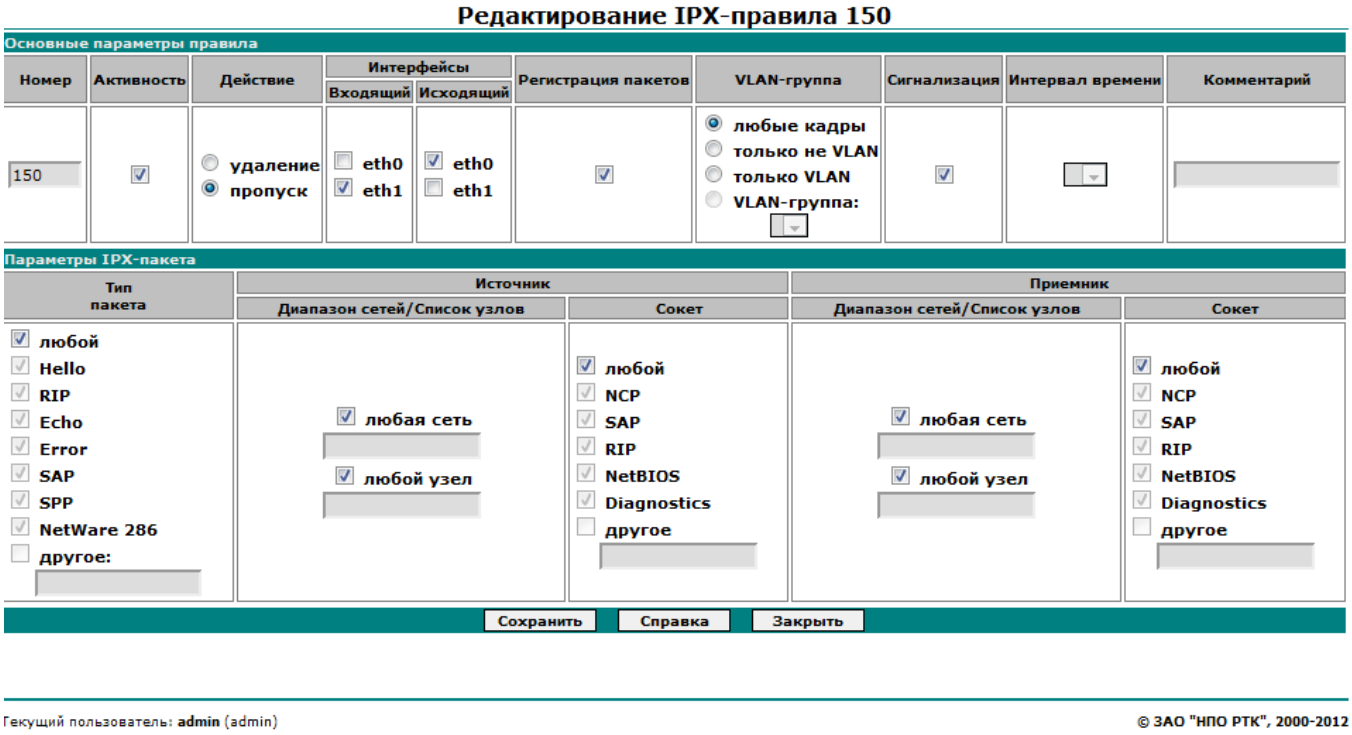

Рисунок 7.80

Для введения и сохранения изменения в действующем правиле необходимо отредактировать нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.81).

Для удаления действующего IPX правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные IPX правила» (рис.7.76). На экране появится запрос (рис.7.82) на подтверждение удаления выбранного IPX правила. Для удаления правила необходимо выбрать кнопку «Да», после чего на экране появится соответствующее сообщение (рис.7.80).

Сообщение об изменении IPX правила

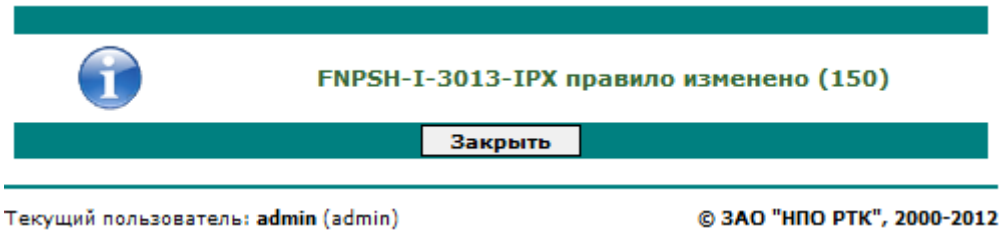

Рисунок 7.81

Удаление IPX правила

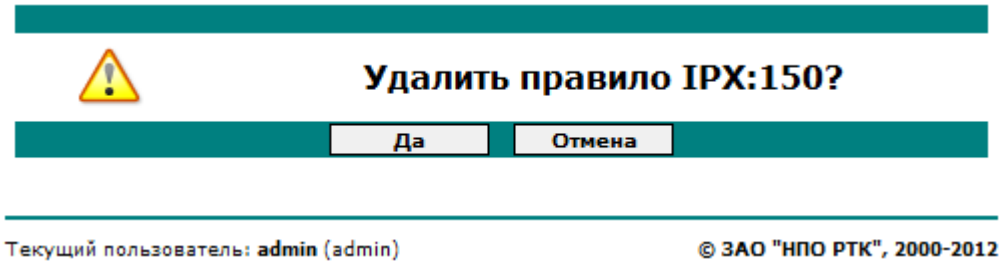

Рисунок 7.82

Сообщение об удалении IPX правила

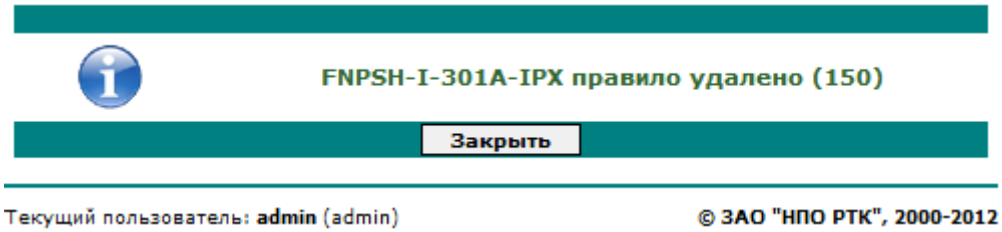

Рисунок 7.83

Редактирование параметра «Активность» (рис. 7.84) может производиться непосредственно в таблице «Регулярные IPX правила» (рис.7.76). При внесении изменений в таблицу на экране появится соответствующее сообщение (рис.7.85).

Редактирование параметра «Активность»

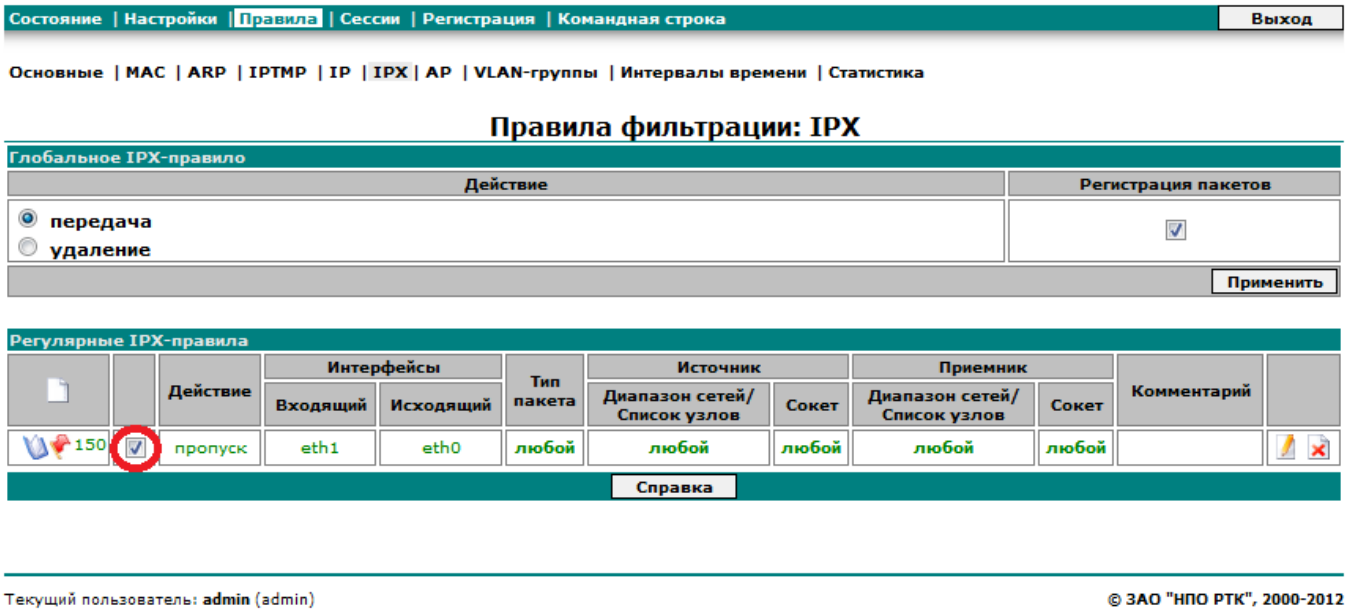

Рисунок 7.84

Сообщение об изменении IPX правила

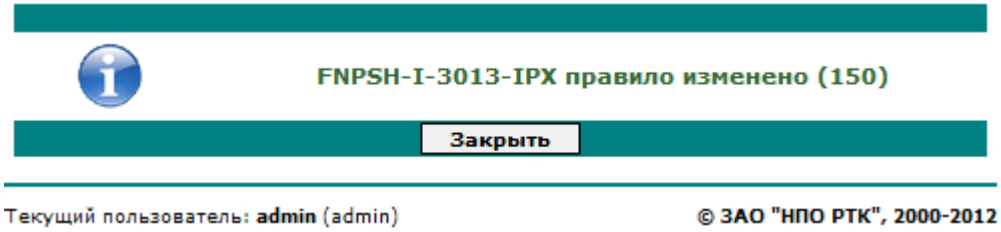

Рисунок 7.85

7.4.5. Управление IP правилами

Для управления (введения, удаления или изменения) IP правилами фильтрации необходимо в окне управления правилами фильтрации (рис.7.47) выбрать «IP». В появившемся окне (рис.7.86) возможно проведение следующих действий по управлению IP правилами:

- редактирование глобального IP правила фильтрации (параметры «Действие» и «Регистрация пакетов»);

- установка нового, редактирование и удаление IP правила фильтрации.

Таблица IP правил фильтрации

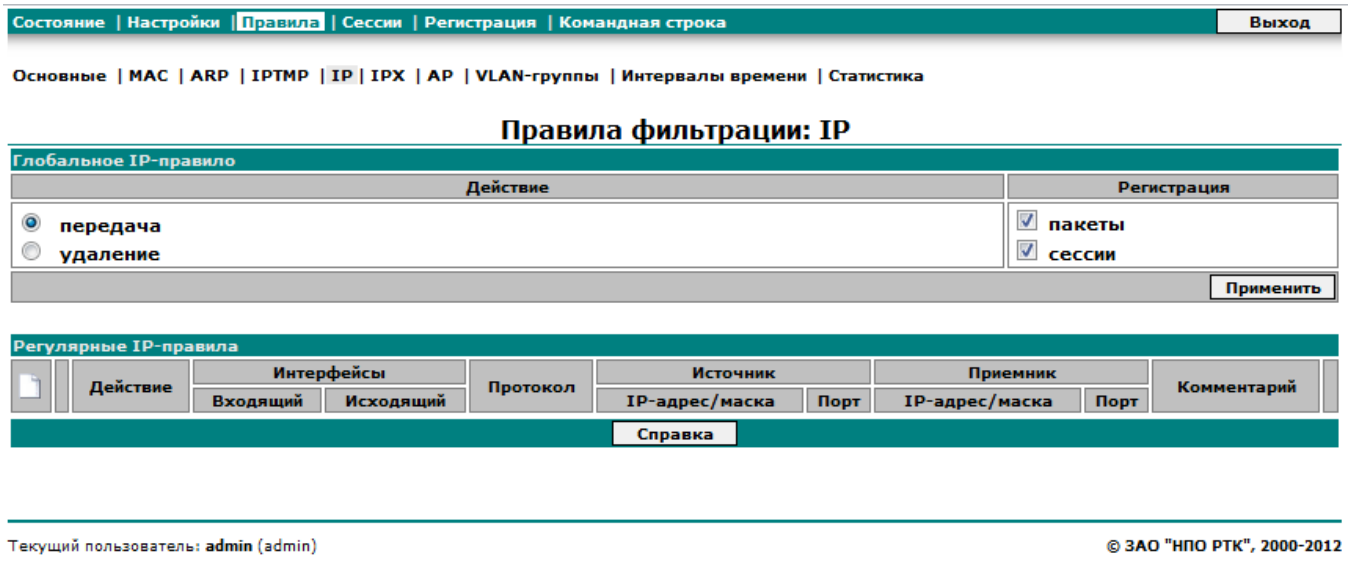

Рисунок 7.86

Редактирование глобального IP правила производится в таблице «Глобальное IP правило» выбором действия и/или установкой регистрации пакетов. Установка измененного глобального правила производится кнопкой «Применить» в той же таблице, при этом на экране появится сообщение об изменении правила (рис.7.87).

Для установки нового IP правила необходимо выбрать кнопку в таблице «Регулярные IP правила» (рис.7.86). На экране появится окно (рис.7.88) для ввода параметров устанавливаемого правила.

Сообщение о загрузке отредактированного глобального IP правила

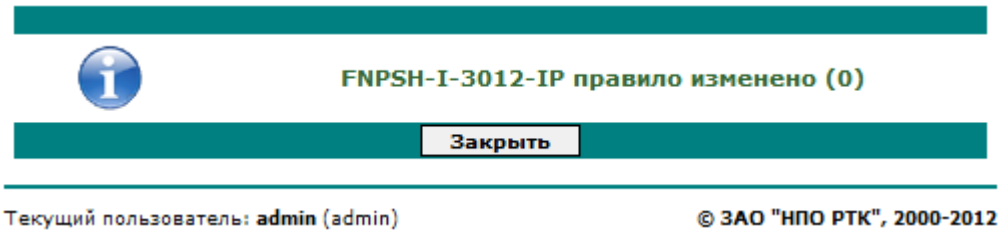

Рисунок 7.87

Добавление IP правила фильтрации

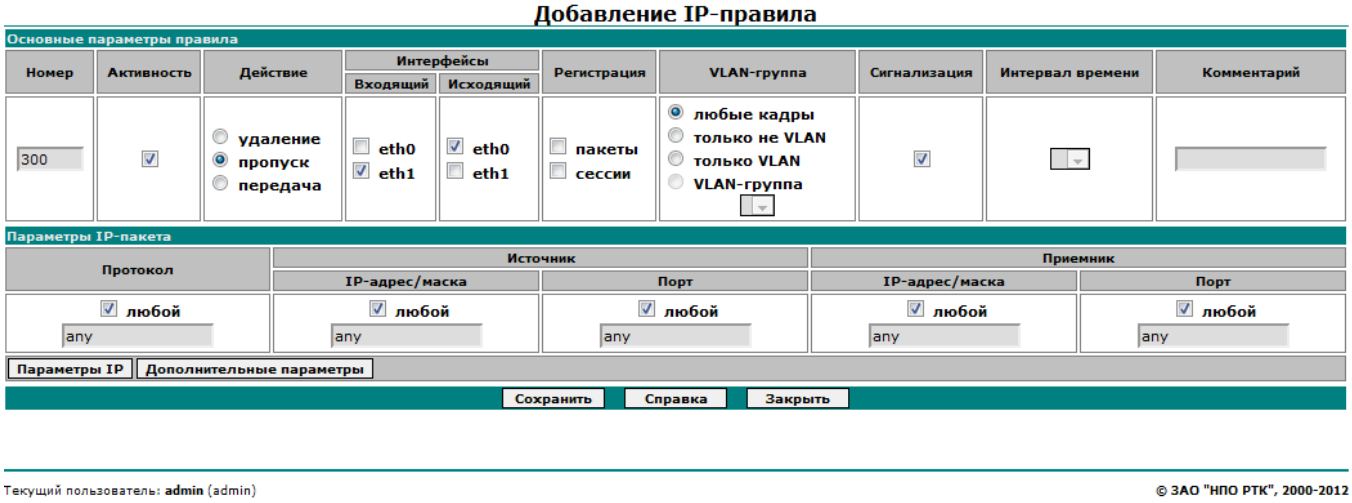

Рисунок 7.88

Для введения дополнительных параметров фильтрации по полям заголовка пакетов IP протокола необходимо выбрать кнопку «Параметры IP». Для введения дополнительных параметров фильтрации пакетов IP (ICMP сообщений) протокола и установок правила необходимо выбрать кнопку «Дополнительные параметры» (рис.7.88). В случае выбора этих кнопок, на экране появятся окна для ввода соответствующих параметров правила (рис. 7.89, 7.90).

Для ввода нового правила в текущий набор правил необходимо установить нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.91).

Добавление IP правила фильтрации

Параметры IP протокола

Флаг Precedence	Флаги TOS	Фрагментация IP-пакета	Максимальная длина IP-пакета	TTL
☑ любой ☐ Network Control ☐ Internetwork Control ☐ CRITIC/ECP4 ☐ Flash Override ☐ Flash ☐ Immediate ☐ Priority ☐ Routine	☑ любой delay: ○ да ○ нет ◉ любой throughput: ○ да ○ нет ◉ любой reliability: ○ да ○ нет ◉ любой cost: ○ да ○ нет ◉ любой ECN: ◉ любой ○ NOT ECT ○ ECT ○ CE ○ ECT CE	◉ любой ○ да ○ нет	☑ любой any	☑ любой any

Сохранить | Справка | Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.89

Добавление IP правила фильтрации

Дополнительные параметры протокола

Использование сессии	Тайм-аут сессии	Тип/код сообщения ICMP	Прикладные правила
◉ по умолчанию ○ да ○ нет	☑ по умолчанию deftout	☑ любой any	☐ использовать прикладные правила noapr

Сохранить | Справка | Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.90

Для редактирования действующего IP правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные IP правила» (рис.7.86). На экране появится окно (рис.7.92) для редактирования выбранного IP правила.

Сообщение об установке нового IP правила

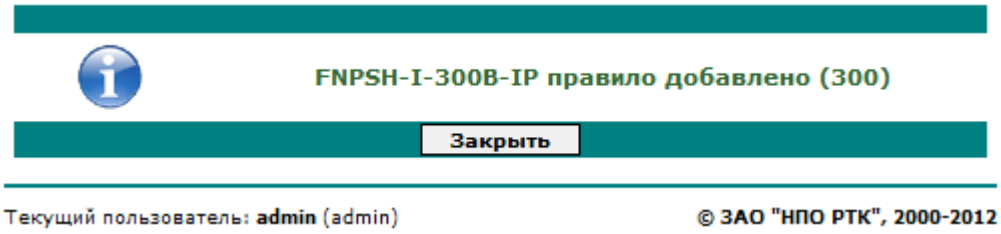

Рисунок 7.91

Редактирование IP правила фильтрации

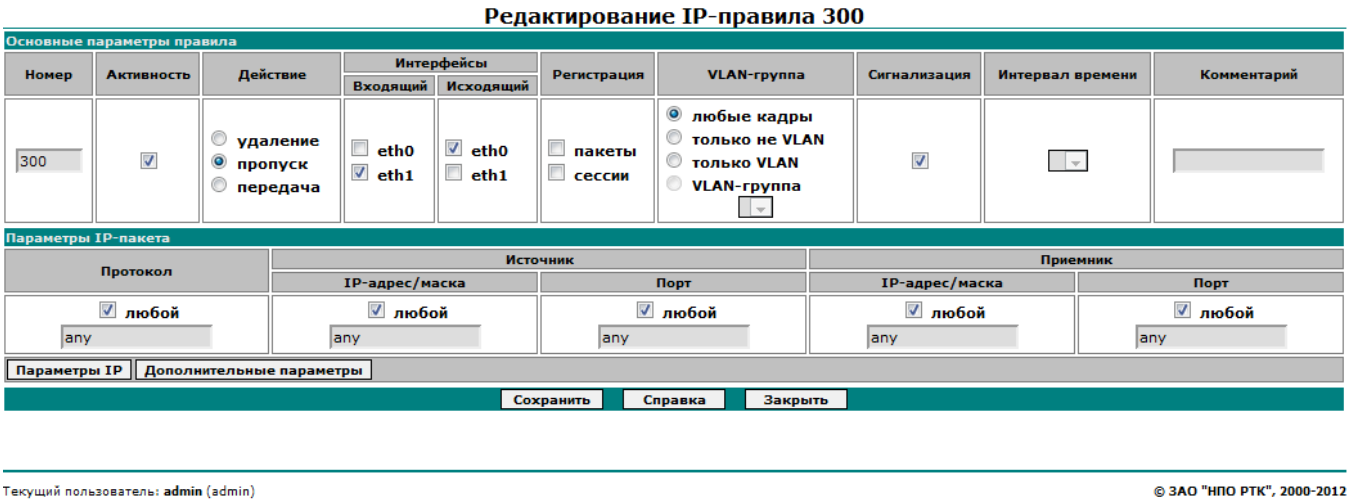

Рисунок 7.92

Так же как и в случае установки нового правила, здесь могут быть открыты окна с дополнительными параметрами (рис.7.89, 7.90).

Для введения и сохранения изменения в действующем правиле необходимо отредактировать нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.93).

Для удаления действующего IP правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные IP правила» (рис.7.86). На экране появится запрос (рис.7.94) на подтверждение удаления выбранного IP правила. Для удаления правила необходимо выбрать кнопку «Да», после чего на экране появится сообщение об удалении правила (рис.7.95).

Сообщение об изменении IP правила

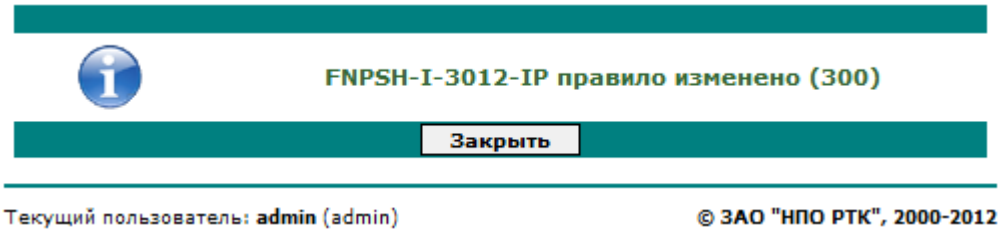

Рисунок 7.93

Удаление IP правила

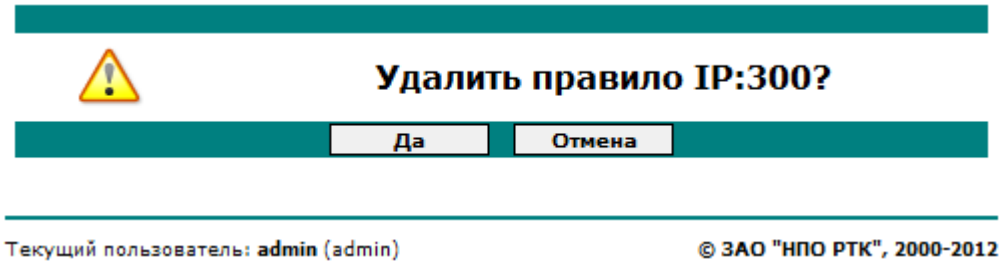

Рисунок 7.94

Сообщение об удалении IP правила

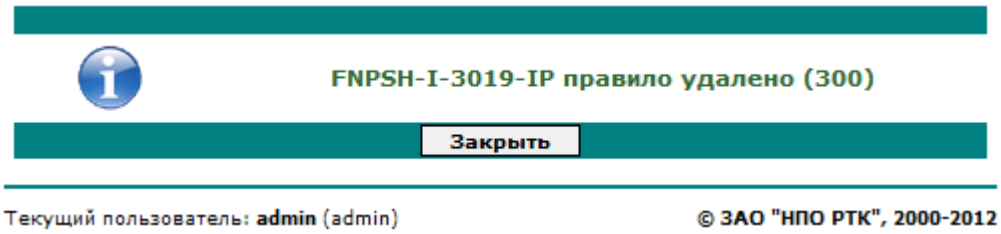

Рисунок 7.95

Редактирование параметра «Активность» (рис.7.96) может производиться непосредственно в таблице «Регулярные IP правила» (рис.7.86). При внесении изменений в таблицу на экране появится соответствующее сообщение (рис.7.97).

Редактирование параметра «Активность»

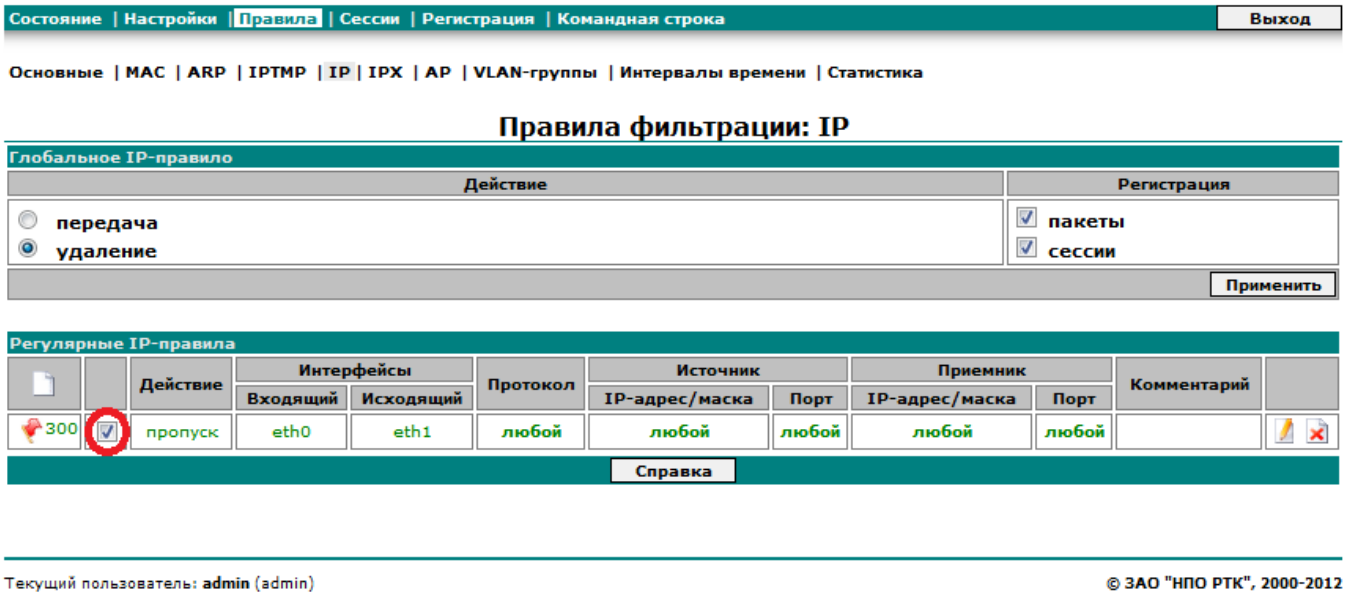

Рисунок 7.96

Сообщение об изменении IP правила

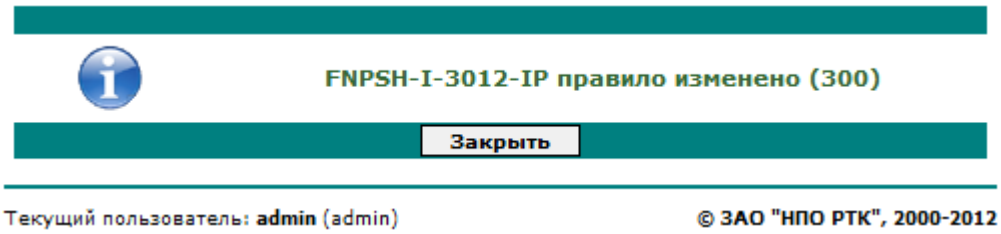

Рисунок 7.97

7.4.6. Управление временными IP правилами

Для управления (введения, удаления или изменения) временными IP правилами фильтрации (IPTMP) необходимо в окне управления правилами фильтрации (рис.7.47) выбрать «IPTMP». В появившемся окне (рис.7.98) возможно осуществление действий по установке нового, редактированию и удалению действующего IPTMP правила фильтрации.

Таблица IPTMP правил фильтрации

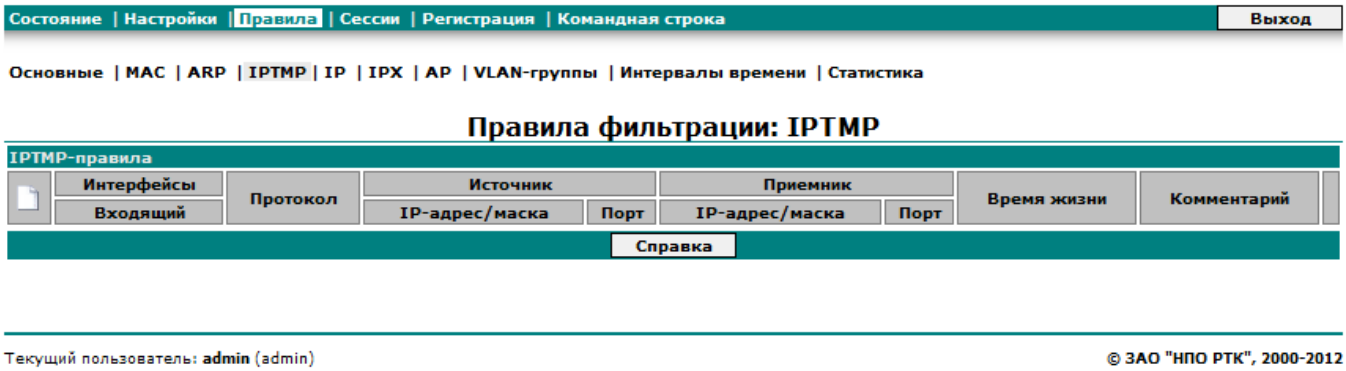

Рисунок 7.98

Для установки нового IPTMP правила необходимо выбрать кнопку в таблице « Правила IPTMP» (рис.7.93). На экране появится окно (рис.7.94) для ввода параметров устанавливаемого правила.

Для ввода нового правила в текущий набор правил необходимо установить нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.95).

Добавление IPTMP правила фильтрации

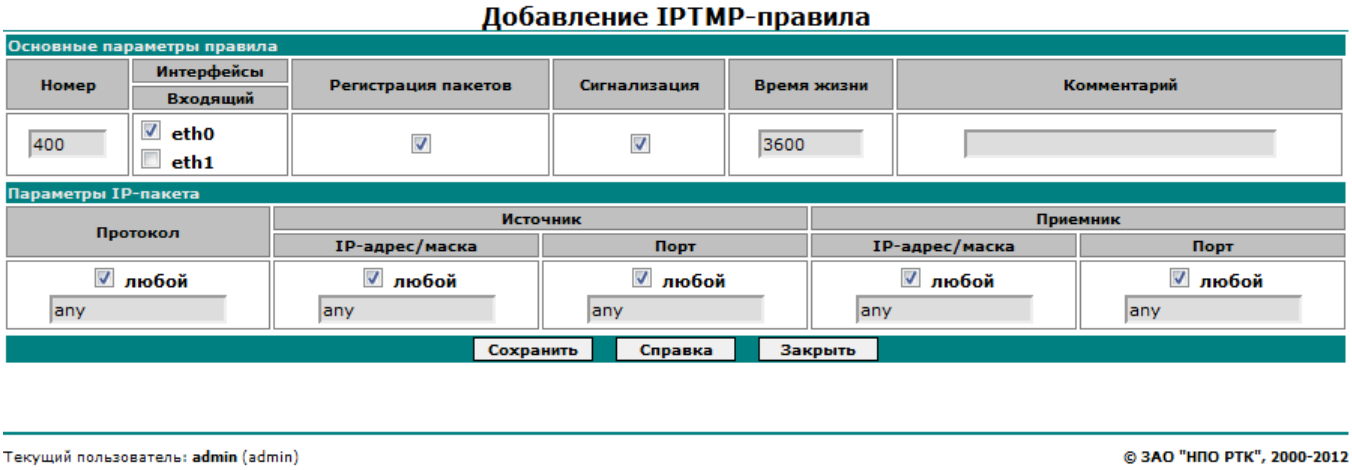

Рисунок 7.99

Сообщение об установке нового IPTMP правила

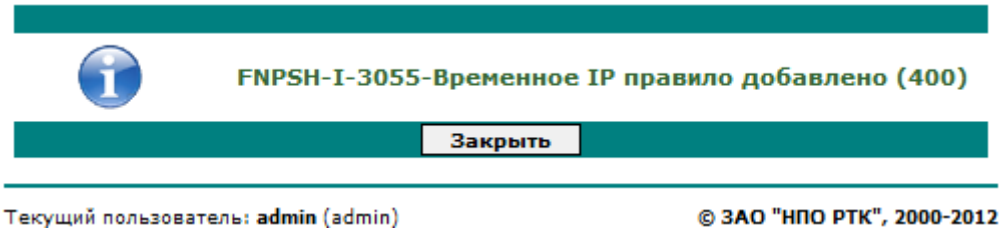

Рисунок 7.100

Для редактирования действующего IPTMP правила необходимо выбрать кнопку в соответствующей строке таблицы «Правила IPTMP» (рис.7.98). На экране появится окно (рис.7.101) для редактирования выбранного IPTMP правила.

Для введения и сохранения изменения в действующем правиле необходимо отредактировать нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.102).

Для удаления действующего IPTMP правила необходимо выбрать кнопку в соответствующей строке таблицы «Правила IPTMP» (рис.7.98). На экране появится запрос (рис.7.103) на подтверждение удаления выбранного IPTMP правила. Для удаления правила необходимо выбрать кнопку «Да», после чего на экране появится сообщение об удалении правила (рис.7.104).

Редактирование IPTMP правила фильтрации

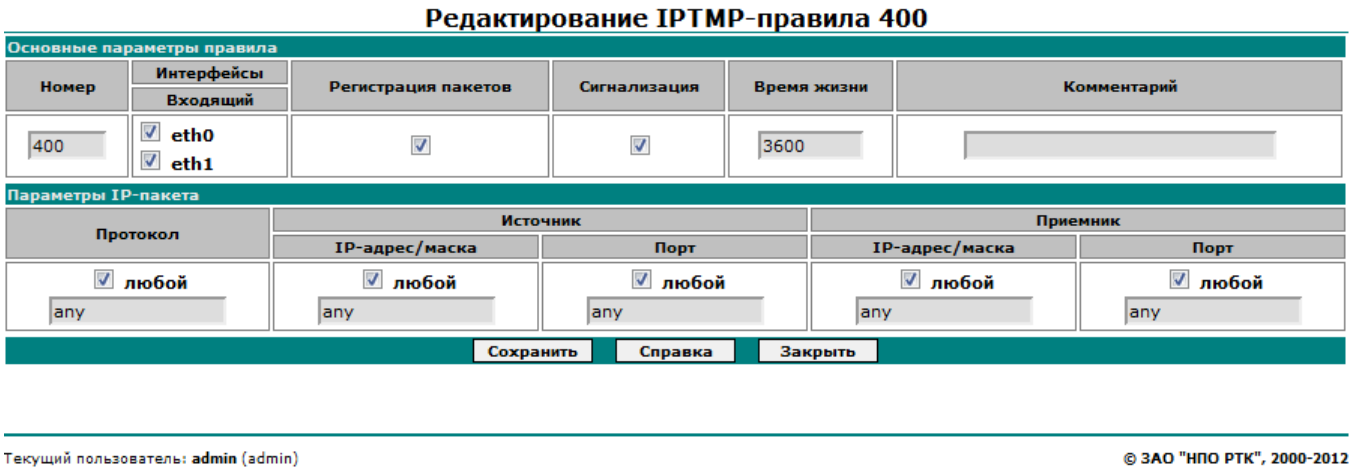

Рисунок 7.101

Сообщение об изменении IPTMP правила

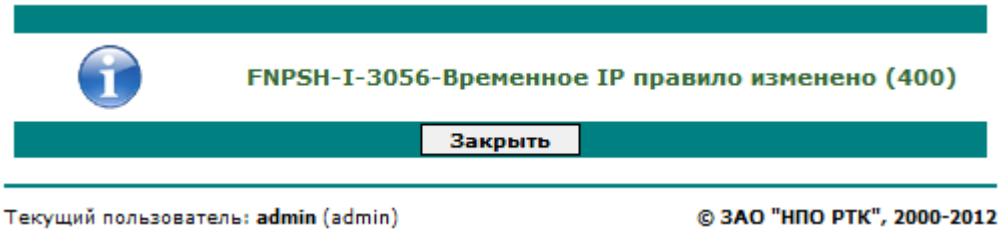

Рисунок 7.102

Удаление IPTMP правила

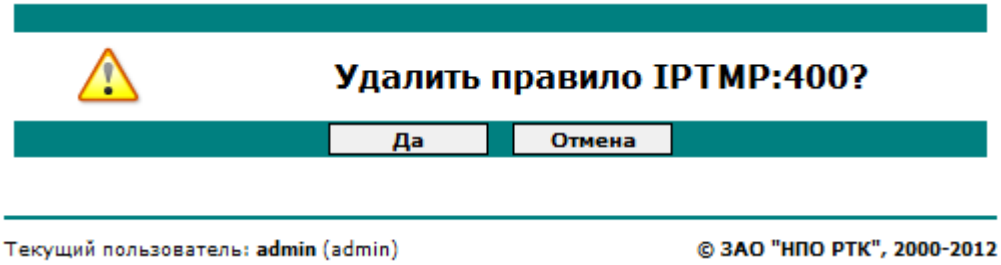

Рисунок 7.103

Сообщение об удалении IPTMP правила

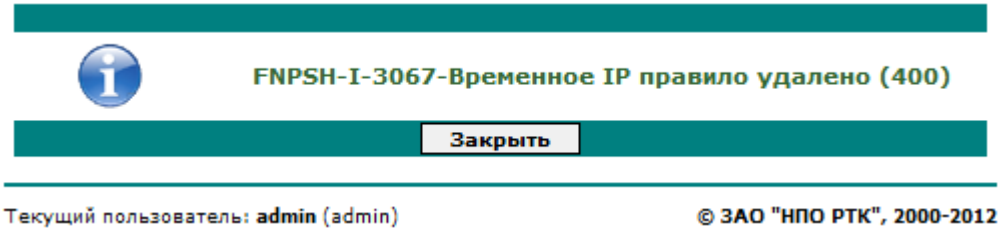

Рисунок 7.104

7.4.7. Управление правилами фильтрации прикладного уровня

Для управления (введения, удаления или изменения) правилами фильтрации прикладного уровня (АР) необходимо в окне управления правилами фильтрации (рис.7.47) выбрать «АР». В появившемся окне (рис.7.105) возможно осуществление действий по установке нового, редактированию и удалению действующего АР правила фильтрации.

Таблица AP правил фильтрации

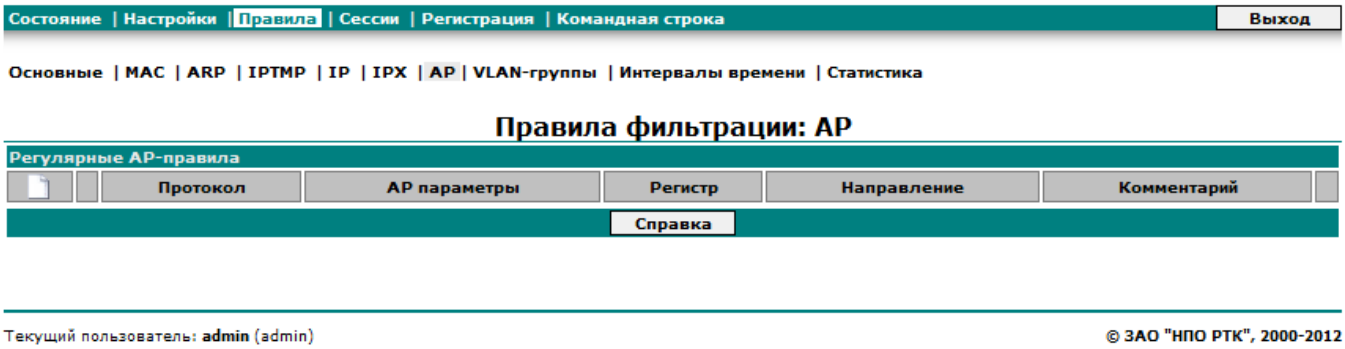

Рисунок 7.105

Для установки нового AP правила необходимо выбрать кнопку в таблице «Регулярные Прикладные правила» (рис.7.105). На экране появится окно (рис.7.106) для ввода параметров устанавливаемого правила.

Добавление AP правила фильтрации

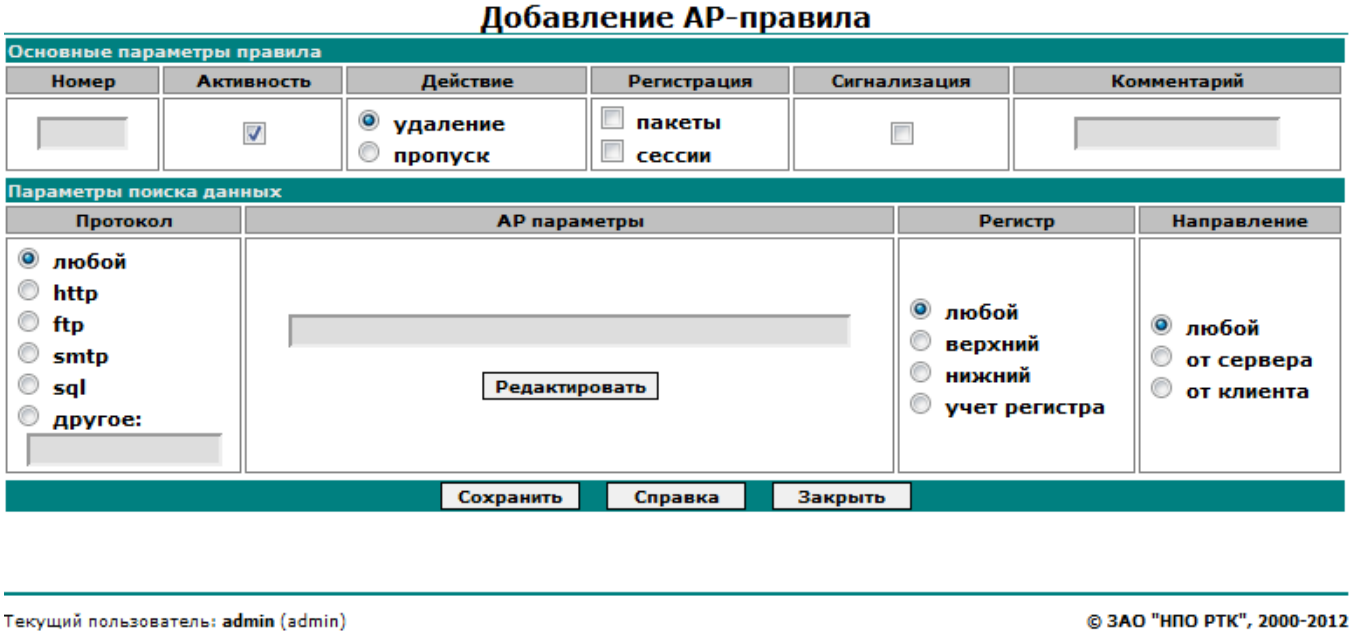

Рисунок 7.106

Для ввода нового правила в текущий набор правил необходимо установить нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.107). Дополнительные, не указанные на рисунке 7.106, контролируемые правилом параметры прикладных протоколов

вводятся в строку «Данные» в соответствии с синтаксисом, определенным в п.п.4.7.10-4.7.140.

Сообщение об установке нового АР правила

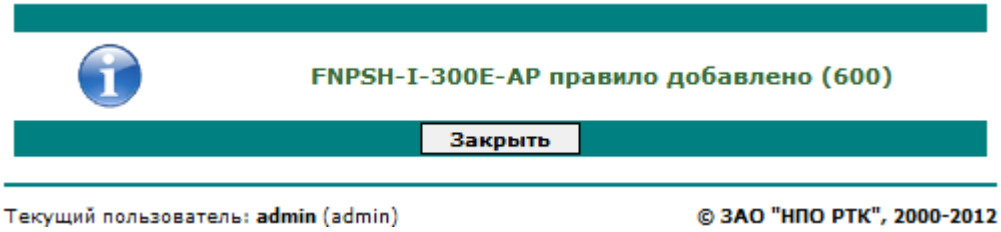

Рисунок 7.107

Для редактирования действующего АР правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные Прикладные правила» (рис.7.105). На экране появится окно (рис.7.108) для редактирования выбранного АР правила.

Редактирование АР правила фильтрации

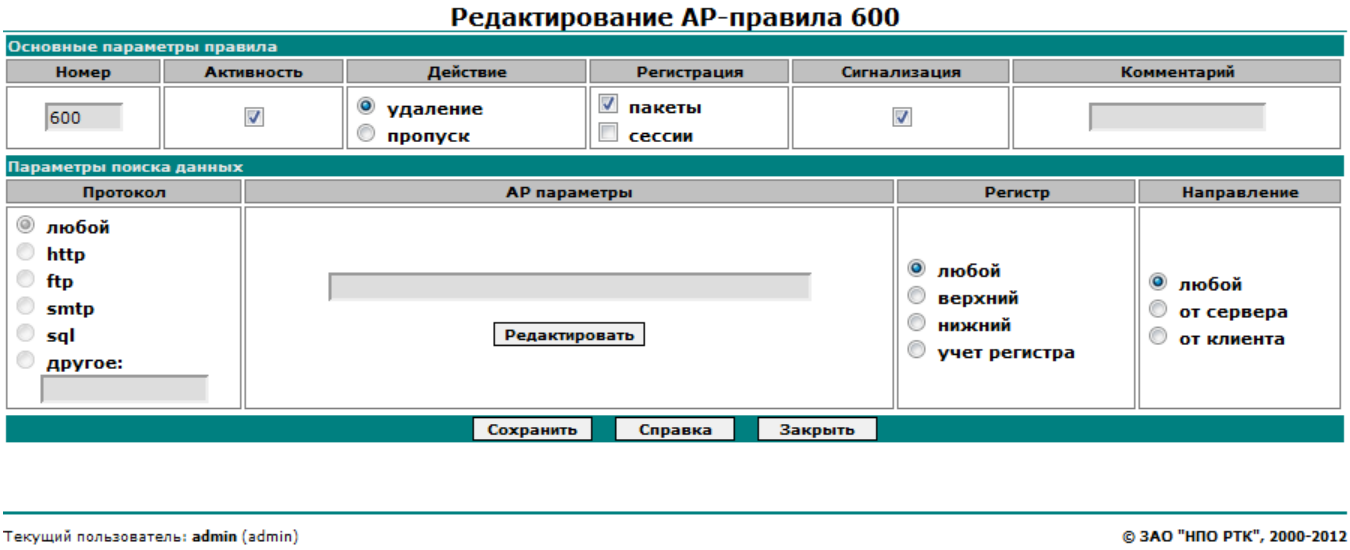

Рисунок 7.108

Для введения и сохранения изменения в действующем правиле необходимо отредактировать нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.109).

Для удаления действующего АР правила необходимо выбрать кнопку в соответствующей строке таблицы «Регулярные Прикладные правила» (рис.7.105). На экране появится запрос (рис.7.110) на подтверждение удаления выбранного АР правила. Для удаления правила необходимо выбрать кнопку «Да», после чего на экране появится сообщение об удалении правила (рис.7.111).

Сообщение об изменении АР правила

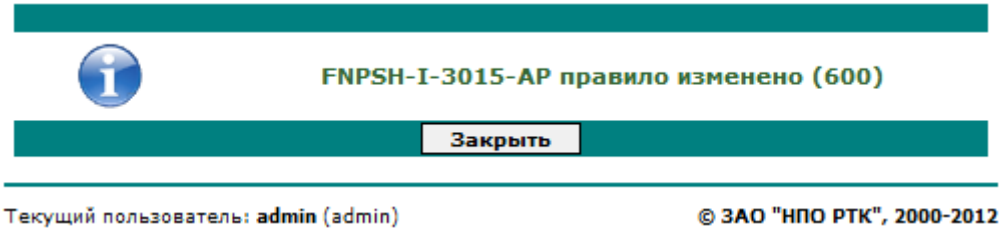

Рисунок 7.109

Удаление АР правила

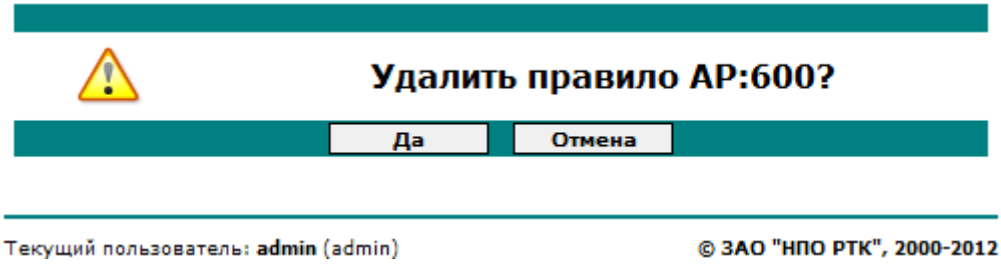

Рисунок 7.110

Сообщение об удалении АР правила

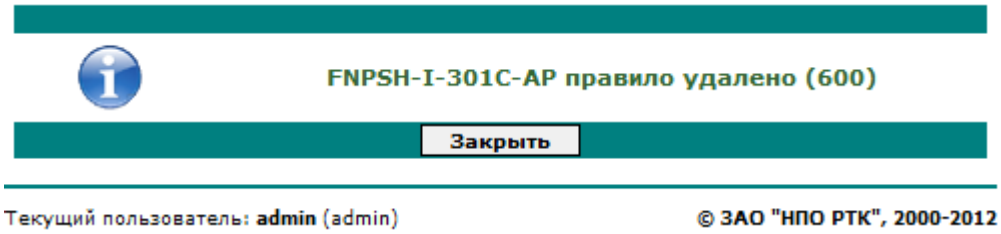

Рисунок 7.111

Редактирование параметра «Активность» (рис.7.112) может производиться непосредственно в таблице «Регулярные Прикладные правила» (рис.7.105). При внесении изменений в таблицу на экране появится соответствующее сообщение

(рис.7.109).

Редактирование параметра «Активность»

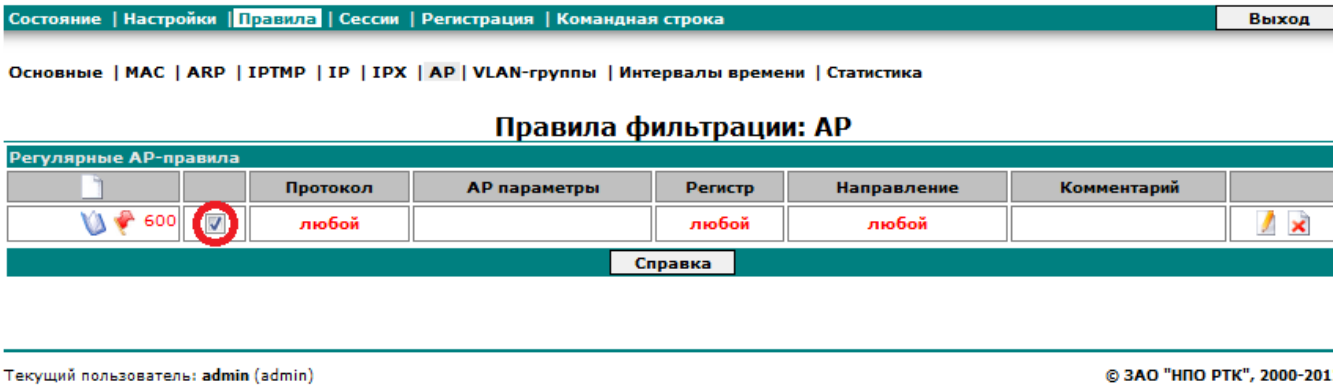

Рисунок 7.112

7.4.8. Управление группами VLAN

Для управления (введения, удаления или изменения) группами VLAN необходимо в окне управления правилами фильтрации (рис.7.47) выбрать «VLAN». В появившемся окне (рис.7.113) возможно осуществление действий по установке новой, редактированию и удалению установленной группы VLAN.

Таблица групп VLAN

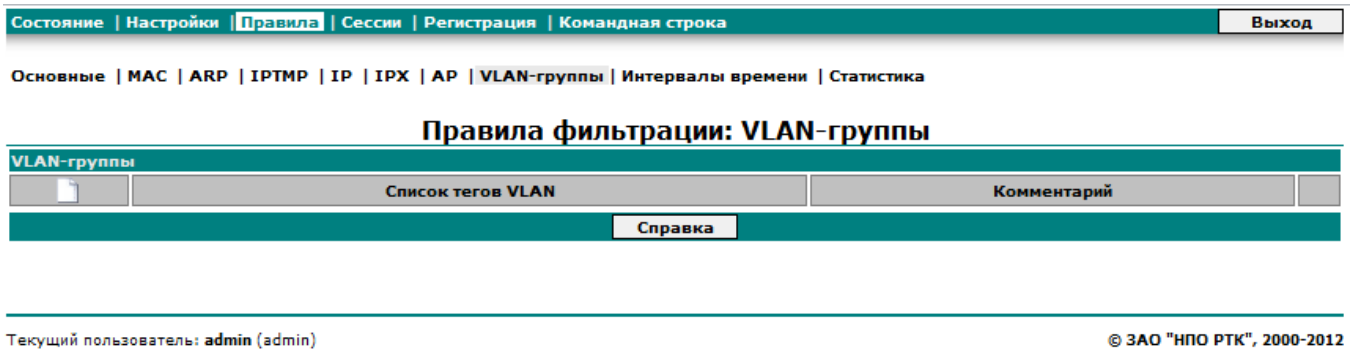

Рисунок 7.113

Для установки новой группы необходимо выбрать кнопку в таблице «Группы VLAN» (рис.7.113). На экране появится окно (рис.7.114) для ввода новой группы.

Добавление группы VLAN

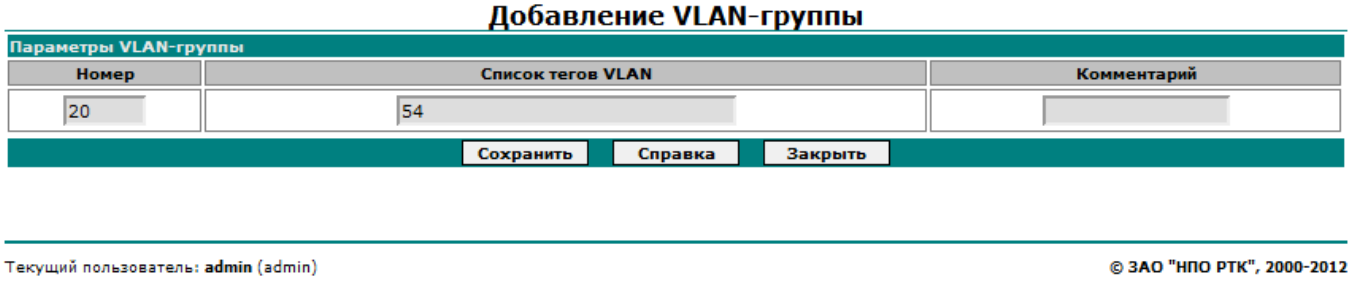

Рисунок 7.114

Для ввода новой группы необходимо установить нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.115).

Для редактирования установленной группы необходимо выбрать кнопку в соответствующей строке таблицы «Группы VLAN» (рис.7.113). На экране появится окно (рис.7.116) для редактирования выбранной группы.

Сообщение о добавлении группы VLAN

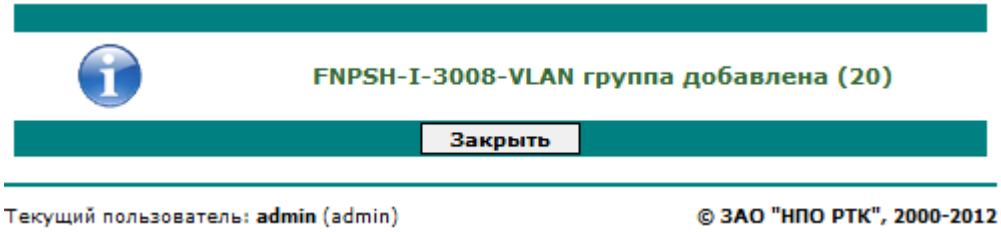

Рисунок 7.115

Редактирование группы VLAN

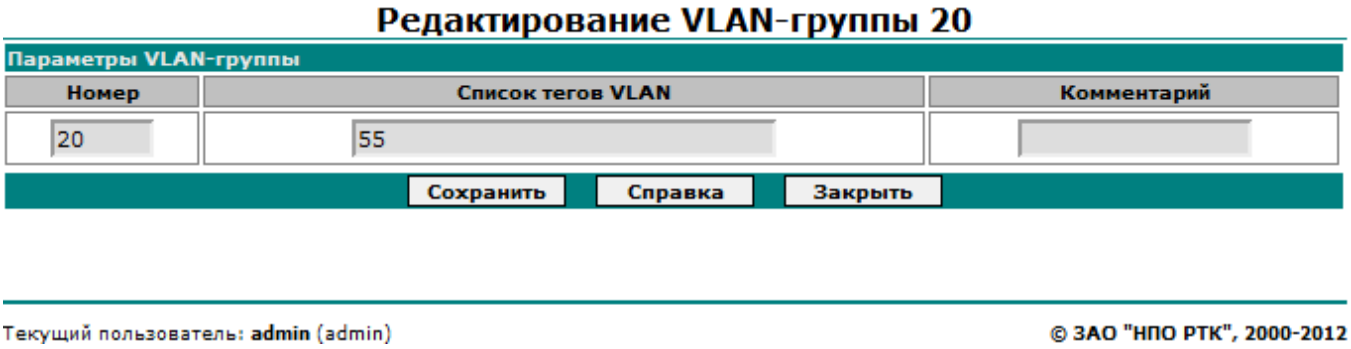

Рисунок 7.116

Для сохранения изменений необходимо отредактировать нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.117).

Сообщение об изменении группы VLAN

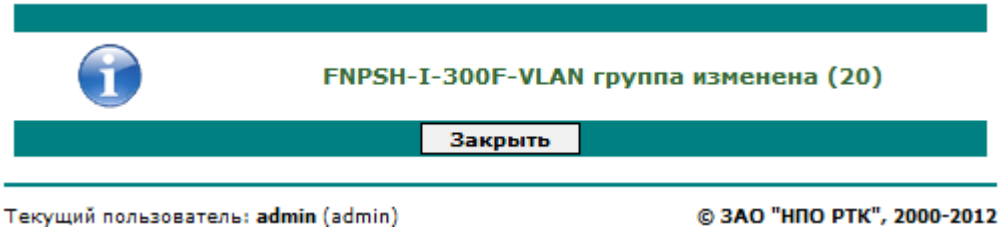

Рисунок 7.117

Для удаления установленной группы VLAN необходимо выбрать кнопку в соответствующей строке таблицы «Группы VLAN» (рис.7.113). На экране появится запрос (рис.7.118) на подтверждение удаления выбранной группы. Для удаления группы необходимо выбрать кнопку «Да», после чего на экране появится сообщение об удалении группы VLAN (рис.7.113).

Удаление группы VLAN

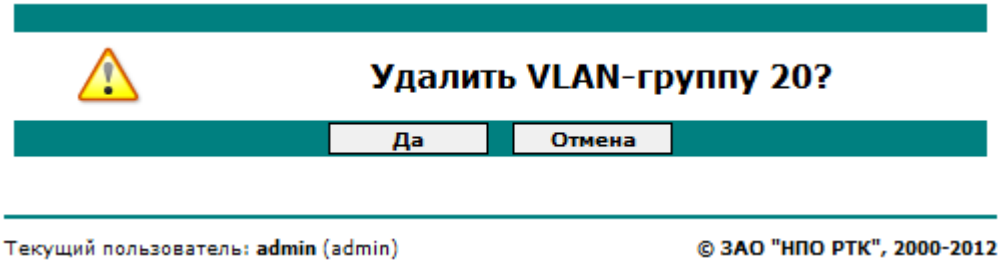

Рисунок 7.118

Сообщение об удалении группы VLAN

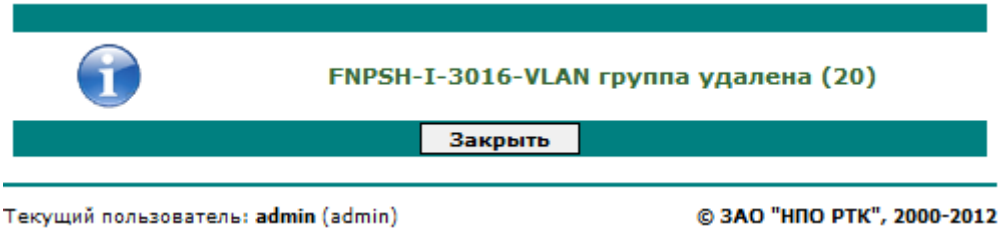

Рисунок 7.119

7.4.9. Управление интервалами времени

Для управления (введения, удаления или изменения) интервалами времени необходимо в окне управления правилами фильтрации (рис.7.47) выбрать «Интервалы времени». В появившемся окне (рис.7.114) возможно осуществление действий по установке новых, редактированию и удалению установленных интервалов времени.

Таблица интервалов времени

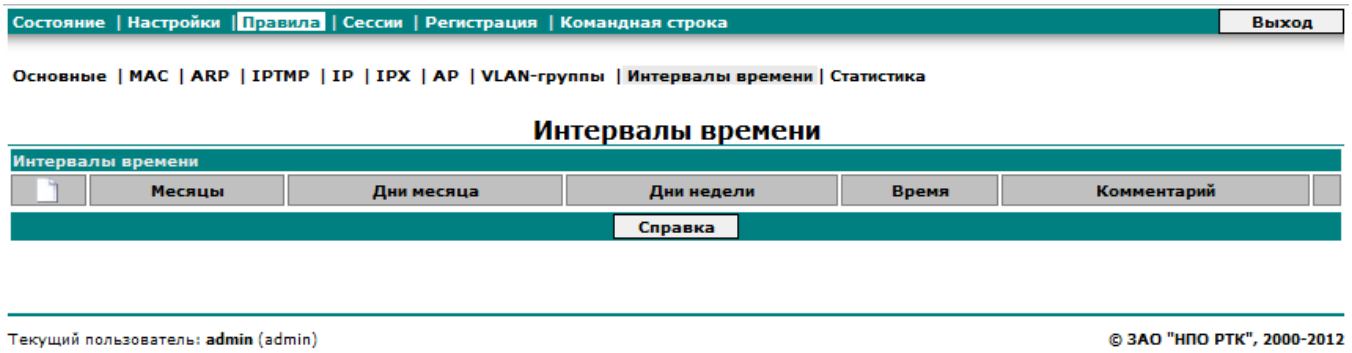

Рисунок 7.120

Для установки нового интервала необходимо выбрать кнопку в таблице «Интервалы времени» (рис.7.120). На экране появится окно (рис.7.121) для ввода нового интервала времени.

Добавление интервала времени

Рисунок 7.121

Для ввода нового интервала необходимо установить нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.122).

Сообщение о добавлении интервала времени

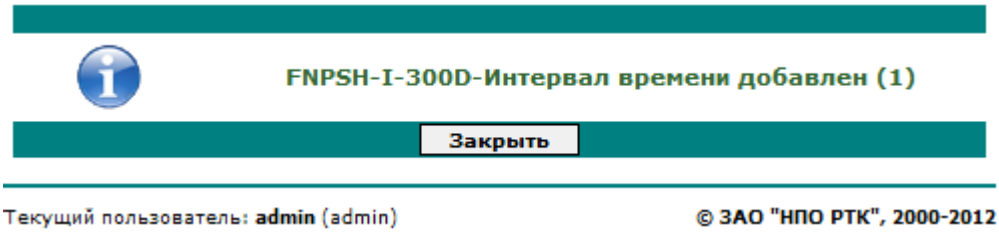

Рисунок 7.122

Для редактирования установленного интервала времени необходимо выбрать кнопку в соответствующей строке таблицы «Интервалы времени» (рис.7.120). На экране появится окно (рис.7.123) для редактирования выбранного интервала.

Для сохранения изменений необходимо отредактировать нужные параметры (п.4.7) и выбрать кнопку «Сохранить», после чего на экране появится соответствующее сообщение (рис.7.118).

Для удаления установленного интервала времени необходимо выбрать кнопку в соответствующей строке таблицы «Интервалы времени» (рис.7.120). На экране появится запрос (рис.7.125) на подтверждение удаления выбранного интервала. Для удаления интервала необходимо выбрать кнопку «Да», после чего на экране появится сообщение об удалении интервала времени (рис.7.126).

Редактирование интервала времени

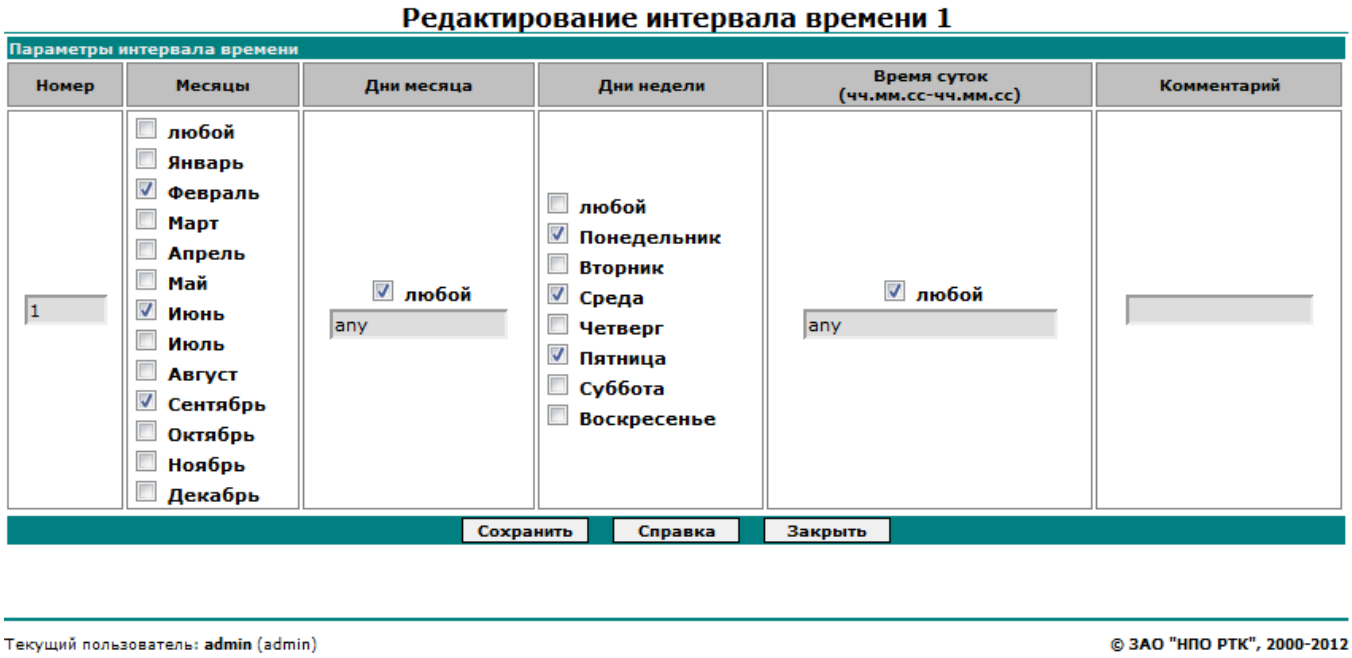

Рисунок 7.123

Сообщение об изменении интервала времени

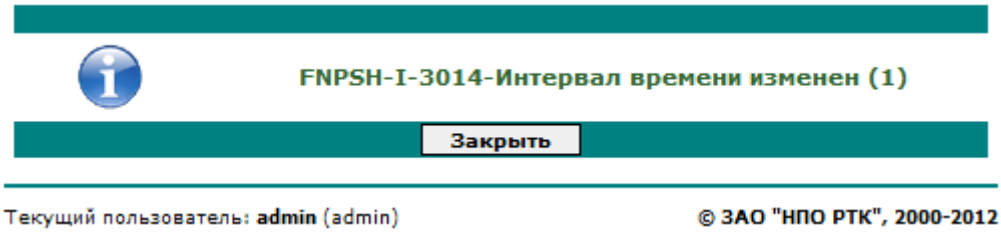

Рисунок 7.124

Удаление интервала времени

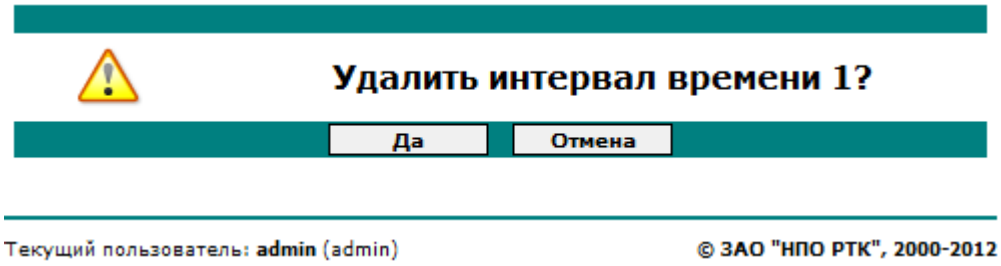

Рисунок 7.125

Сообщение об удалении интервала времени

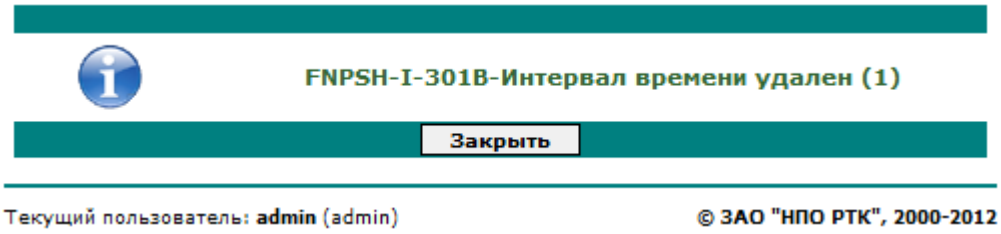

Рисунок 7.126

7.4.10. Возврат к предыдущему состоянию правил фильтрации и статистика использования правил

Для возврата к предыдущему состоянию (перед последним проведенным изменением) правил фильтрации осуществляется выбором в окне управления правилами фильтрации (рис.7.47) слова «Возврат». На экране появится запрос (рис.7.127) на подтверждение выполнения этой команды. Для ее выполнения необходимо выбрать кнопку «Да». На экране появится сообщение о возврате (рис.7.128).

Возврат к предыдущему набору правил фильтрации

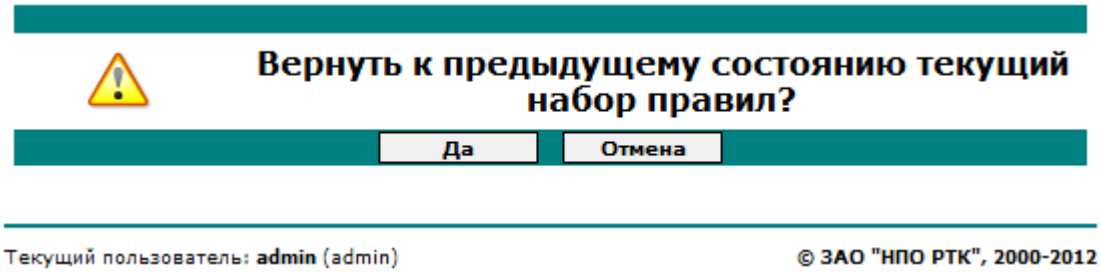

Рисунок 7.127

Сообщение о возврате к предыдущему набору правил фильтрации

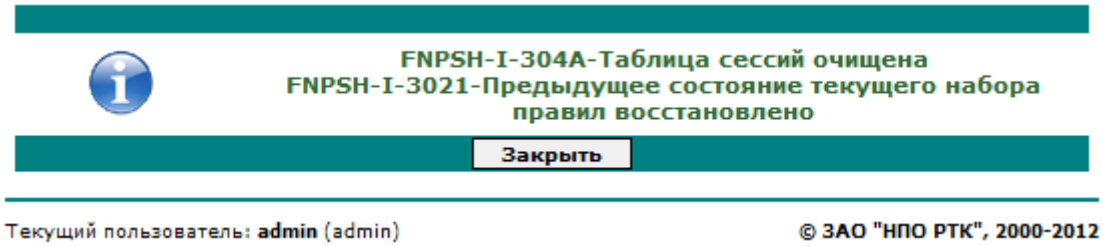

Рисунок 7.128

Для просмотра статистики использования установленных правил фильтрации

необходимо в окне управления правилами фильтрации (рис.7.47) выбрать слово «Статистика». На экране появится таблица использования правил фильтрации (рис.7.129).

Для очистки таблицы необходимо выбрать кнопку «Очистить». На экране появится запрос (рис.7.130) на подтверждение выполнения этой команды. Для ее выполнения необходимо выбрать кнопку «Да». На экране появится сообщение об очистке таблицы (рис.7.125).

Статистика использования правил фильтрации

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка Выход

Основные | MAC | ARP | IPTMP | IP | IPX | AP | VLAN-группы | Интервалы времени | Статистика

Правила фильтрации: Статистика использования

Использование правил

Правило	Последнее изменение	Пакеты	Байты
mac:0	11.07.2012, 13:13:36	0	0
mac:12	11.07.2012, 13:13:36	0	0
arp:0	11.07.2012, 13:13:36	0	0
arp:100	11.07.2012, 13:13:36	0	0
ip:0	11.07.2012, 13:13:36	0	0
ipx:0	11.07.2012, 13:13:36	0	0

Очистить Справка

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.129

Удаление статистических данных

Очистить статистику использования правил?

Да Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.130

Сообщение об очистки таблицы

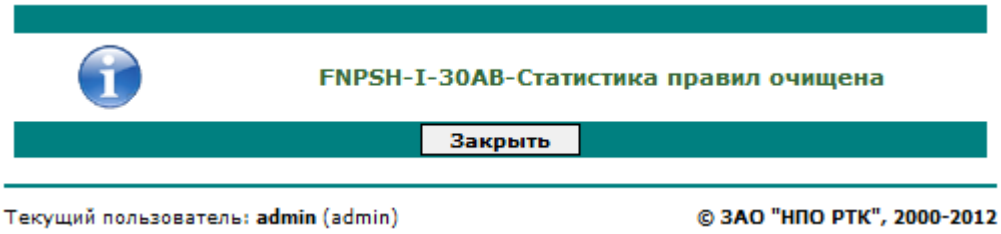

Рисунок 7.131

7.5. Управление сессиями

Для управления сессиями необходимо в главном окне (рис.7.3) выбрать «Сессии». На экране управляющего компьютера появится окно настроек сессий (рис. 7.132)

Окно настроек сессий

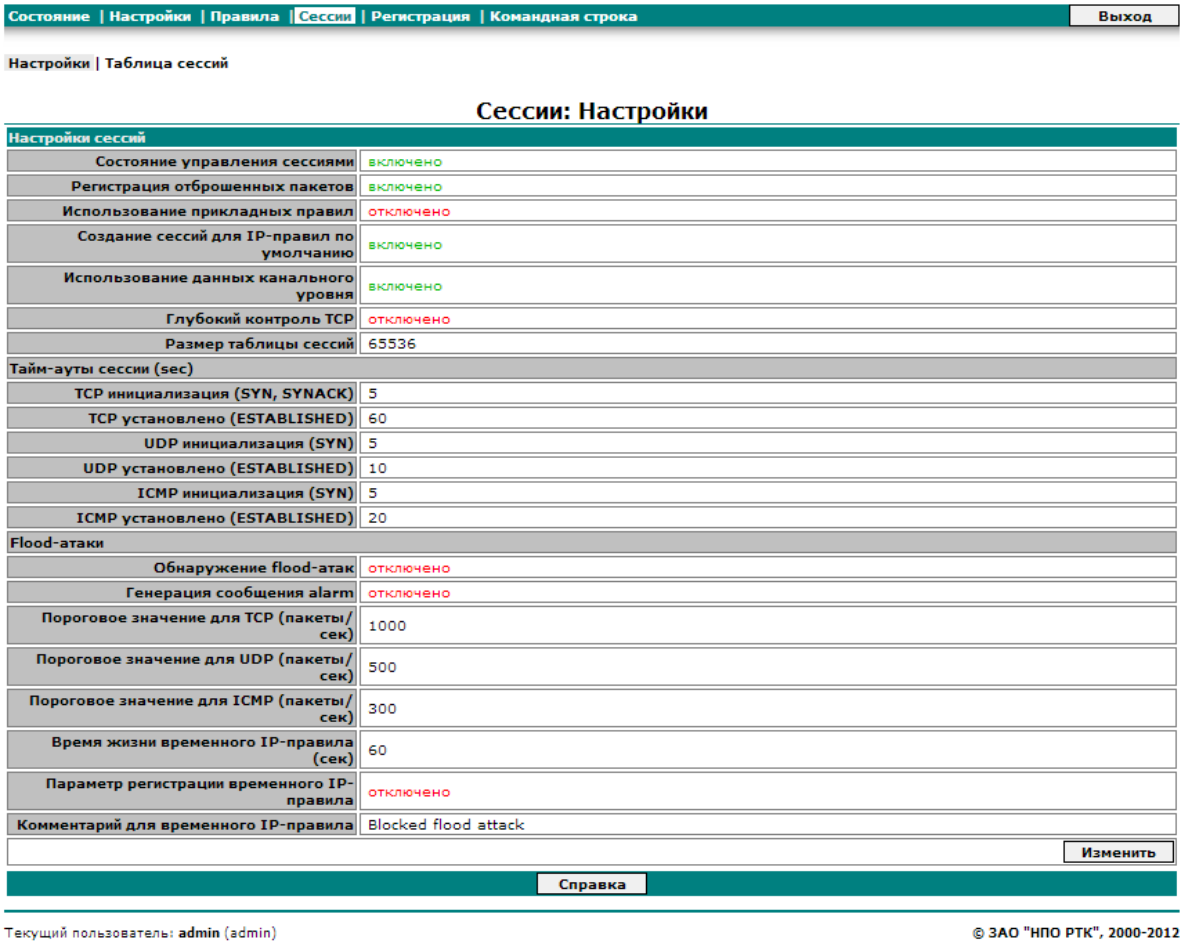

Рисунок 7.132

Выбор кнопки «Изменить» позволяет изменить параметры настроек сессий в появившемся окне (рис.7.133). Для применения измененных настроек необходимо выбрать кнопку «Сохранить». После чего на экране появится окно сообщения о произведенных изменениях (рис.7.134).

Окно редактирования настроек сессий

Редактирование настроек сессий

Настройки сессий

Управление сессиями	☑
Регистрация отброшенных пакетов	☑
Использование прикладных правил	☐
Создание сессий для IP-правил по умолчанию	☑
Использование данных канального уровня	☑
Глубокий контроль TCP	☐
Размер таблицы сессий	65536
Тайм-ауты сессии (sec)	
TCP инициализация (SYN, SYNACK)	5
TCP установлено (ESTABLISHED)	60
TCP завершение (FIN, FINACK, FINFINACK)	5
UDP инициализация (SYN)	5
UDP установлено (ESTABLISHED)	10
ICMP инициализация (SYN)	5
ICMP установлено (ESTABLISHED)	20

Flood-атаки	
Обнаружение flood-атак	☐
Генерация сообщения alarm	☐
Пороговое значение для TCP (пакеты/сек)	1000
Пороговое значение для UDP (пакеты/сек)	500
Пороговое значение для ICMP (пакеты/сек)	300
Время жизни временного IP-правила (сек)	60
Параметр регистрации временного IP-правила	☐
Комментарий для временного IP-правила	Blocked flood attacl

Сохранить | Справка | Отмена

Текущий пользователь: admin (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.133

Сообщение о введенных изменениях

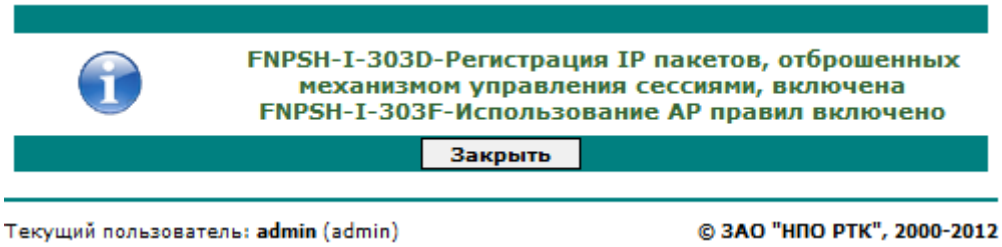

Рисунок 7.134

Подробное описание настроек сессий представлено в п. 6.1.2. Все настройки, при использовании WEB – интерфейса выполняются выбором соответствующих кнопок и записью необходимых параметров.

Для просмотра таблицы незавершенных сессий необходимо в окне настроек сессий выбрать «Сессии». На экране управляющего компьютера появится окно с таблицей сессий (рис. 7.135)

Таблица сессий

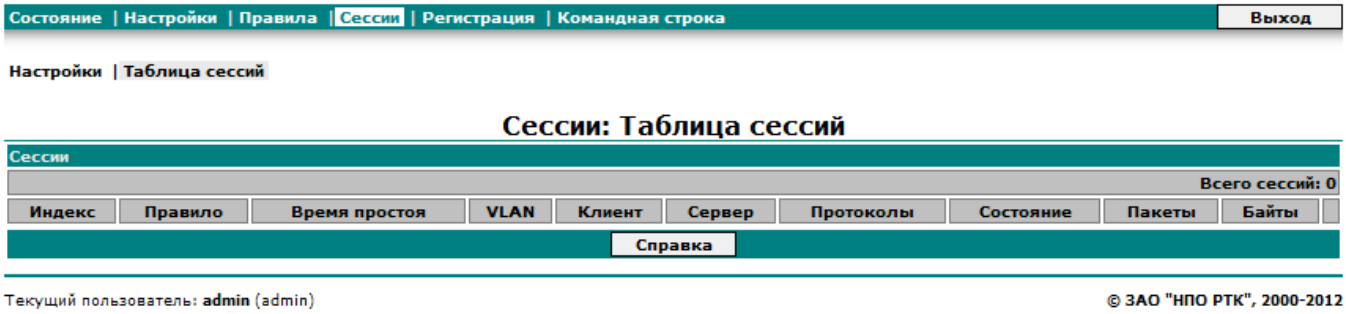

Рисунок 7.135

7.6. Регистрация

Для настройки параметров регистрации и просмотра журналов, и управления ими необходимо в главном окне (рис.7.3) выбрать «Регистрация». На экране управляющего компьютера появится окно настроек параметров регистрации (рис. 7.136)

Окно настроек параметров регистрации

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка Выход

Настройки | События | Пакеты | Сессии | Системные сообщения | Очистка файлов регистрации

Регистрация: Настройки

Настройки подсистемы регистрации	
Регистрация пакетов	включено
Регистрация пакетов, удаленных сессиями	отключено
Регистрация пакетов, удаленных NAT	отключено
Системная регистрация обновлений NTP	включено
FTP	
Выгрузка файлов регистрации по FTP	отключено
FTP сервер	не установлен
FTP путь	не установлен
FTP вход	не установлен
SYSLOG	
Выгрузка файлов регистрации по SYSLOG	отключено
SYSLOG сервер	не установлен

Очистка FTP Изменить

Справка

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.136

Для изменения настроек необходимо выбрать кнопку «Изменить». На экране управляющего компьютера появится окно (рис.7.137)

Параметры, устанавливаемые при настройке подсистемы, и их значения определены в разделе 5.

Окно редактирования настроек параметров подсистемы регистрации

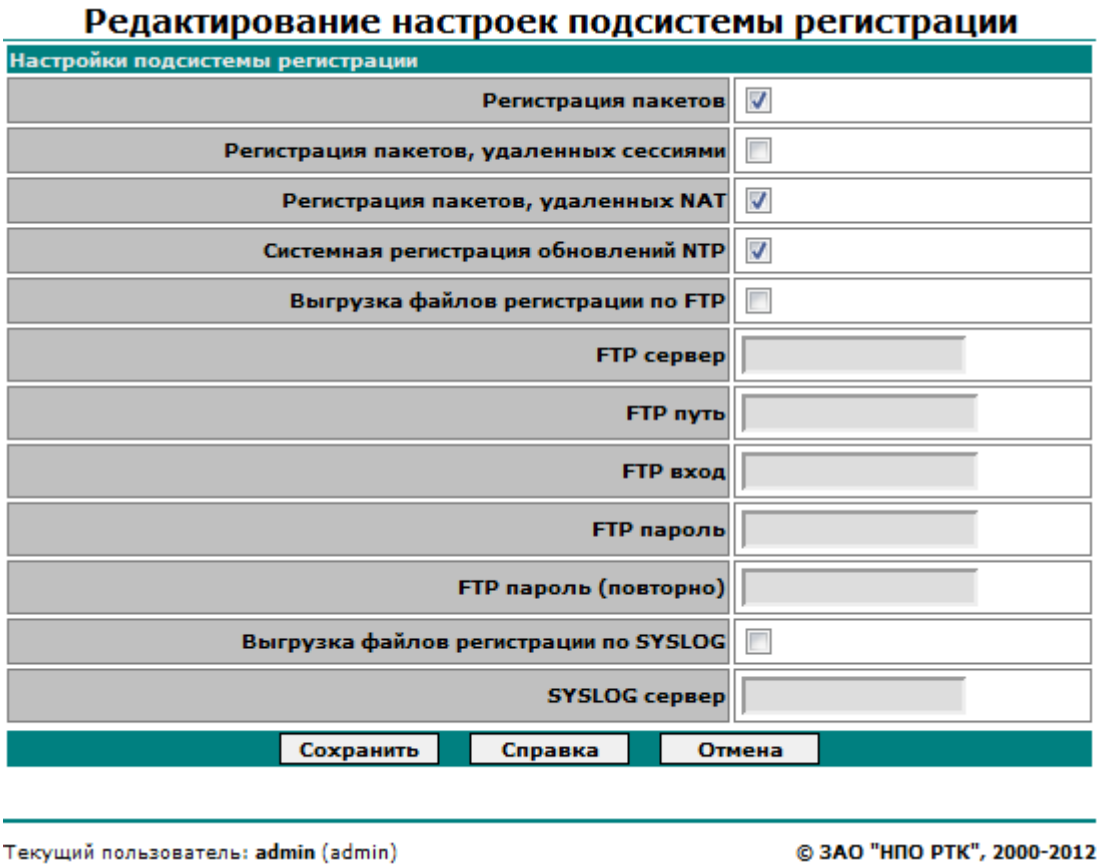

Рисунок 7.137

Для сохранения измененных настроек необходимо выбрать кнопку «Сохранить». После чего на экране появится окно сообщения о произведенных изменениях (рис.7.138).

Сообщение о произведенных изменениях

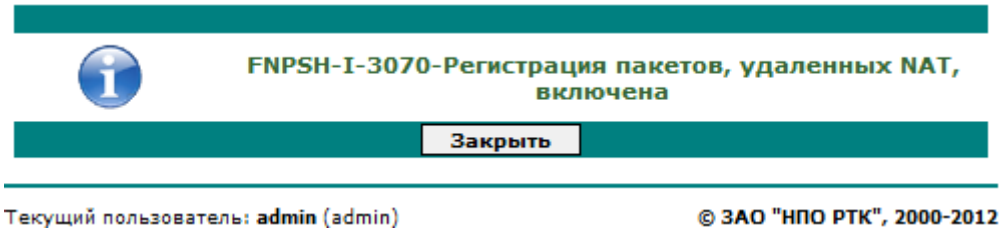

Рисунок 7.138

Для просмотра зарегистрированных событий необходимо в окне настроек параметров регистрации (рис.7.136) выбрать «События». На экране управляющего компьютера появится окно (рис.7.139) выбора параметров просмотра событий.

Окно выбора параметров просмотра событий

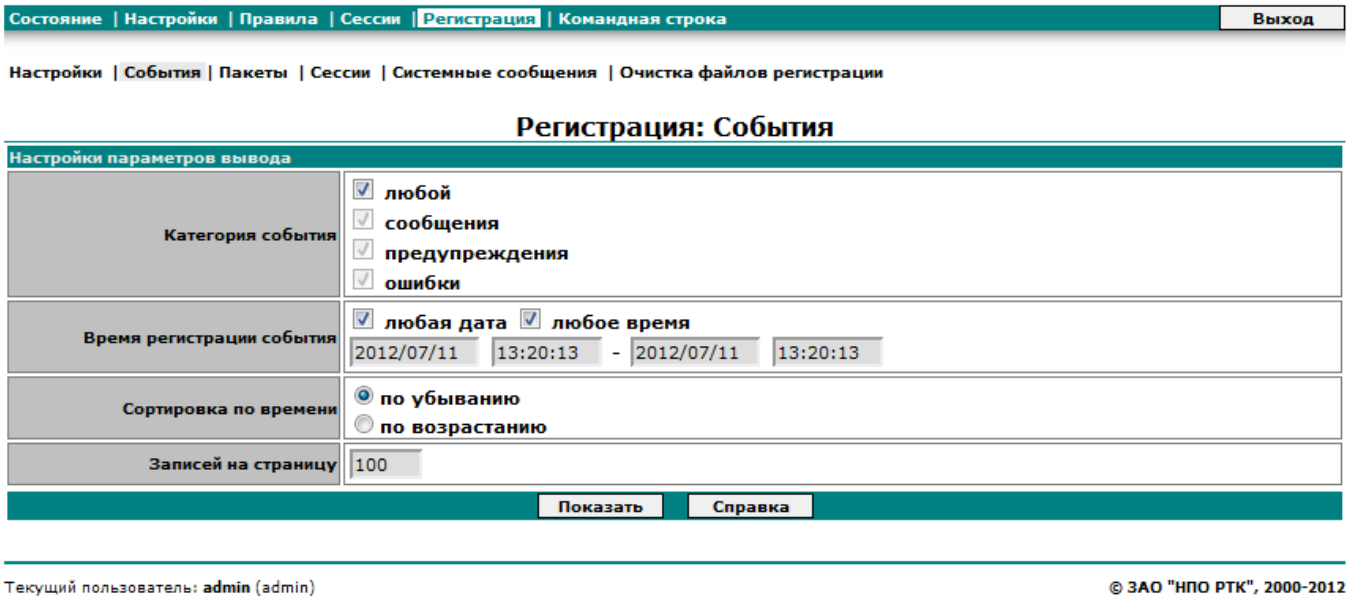

Рисунок 7.139

В этом окне выбираются параметры, по которым необходимо произвести выборку зарегистрированных событий. По умолчанию задается просмотр всех зарегистрированных событий. После установке необходимых значений необходимо выбрать кнопку «Показать». На экране управляющего компьютера появится окно (рис.7.140) с зарегистрированной информацией выбранных событий.

Для просмотра зарегистрированных пакетов необходимо в окне настроек параметров регистрации (рис.7.136) выбрать «Пакеты». На экране управляющего компьютера появится окно (рис.7.141) выбора параметров просматриваемых пакетов.

В этом окне выбираются параметры, по которым необходимо произвести выборку зарегистрированных пакетов. По умолчанию задается просмотр всех зарегистрированных пакетов. После установке необходимых значений параметров просмотра необходимо выбрать кнопку «Показать». На экране управляющего компьютера появится окно (рис.7.142) с зарегистрированной информацией выбранных пакетов.

Окно просмотра выбранных событий

Регистрация: Список событий

Закрыть

Найдено записей: 4303, Страница 1 из 44
Первая 1 2 3 4 5 6 7 8 9 10 Следующая Последняя

Номер	Время	Информация	Пользователь
1	11.07.2012 13:18:48, GMT	I-1209: Включение регистрации NAT	admin, 10.8.0.14
2	11.07.2012 13:17:39, GMT	I-1101: Выход пользователя - Средство группового управления; read	admin, 192.168.78.103
3	11.07.2012 13:17:37, GMT	I-1100: Вход пользователя - Средство группового управления; read	admin, 192.168.78.103
4	11.07.2012 13:17:24, GMT	I-1050: Выключение фильтрации на прикладном уровне	admin, 10.8.0.14
5	11.07.2012 13:17:24, GMT	I-104E: Выключение регистрации пакетов, отброшенных механизмом управления сессиями	admin, 10.8.0.14
6	11.07.2012 13:16:46, GMT	I-104F: Включение фильтрации на прикладном уровне	admin, 10.8.0.14
7	11.07.2012 13:16:46, GMT	I-104D: Включение регистрации пакетов, отброшенных механизмом управления сессиями	admin, 10.8.0.14
8	11.07.2012 13:15:27, GMT	I-102F: Сброс статистики в правилах - все правила	admin, 10.8.0.14
9	11.07.2012 13:15:00, GMT	I-102F: Сброс статистики в правилах - все правила	admin, 10.8.0.14
10	11.07.2012 13:13:38, GMT	I-1016: Откат к предыдущему состоянию набора правил	admin, 10.8.0.14
11	11.07.2012 13:13:36, GMT	I-1058: Очистка таблицы сессий	admin, 10.8.0.14
12	11.07.2012 13:12:39, GMT	I-1101: Выход пользователя - Средство группового управления; read	admin, 192.168.78.103
13	11.07.2012 13:12:37, GMT	I-1100: Вход пользователя - Средство группового управления; read	admin, 192.168.78.103
14	11.07.2012 13:12:30, GMT	I-1012: Удаление правила фильтрации - интервал времени 1	admin, 10.8.0.14

Рисунок 7.140

Окно выбора параметров просмотра пакетов

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка Выход

Настройки | События | Пакеты | Сессии | Системные сообщения | Очистка файлов регистрации

Регистрация: Пакеты

Настройки параметров вывода

Действие	
Интерфейсы Вх.	
Интерфейсы Вых.	
Правило	
Тип кадра Ethernet	
Протокол	
Номер сессии	
MAC-адрес источника	
MAC-адрес приемника	
MAC-адрес	
IP-адрес источника	
IP-адрес приемника	
IP-адрес	
Порт источника	
Порт приемника	
Порт	
Время регистрации пакета	☑ любая дата ☑ любое время 2012/07/11 13:21:36 - 2012/07/11 13:21:36
Сортировка по времени	◉ по убыванию ○ по возрастанию
Записей на страницу	100

Показать Справка

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.141

Окно просмотра выбранных (удаленных) пакетов

Регистрация: Пакеты

Закрыть

Список пакетов

Найдено записей: 7341, Page 1 of 74
Первая 1 2 3 4 5 6 7 8 9 10 Следующая Последняя

Время	Действие	Правила	Интерфейсы	Протокол	Источник	Приемник	
03. 04. 2008 10:35:47. 398408, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	
03. 04. 2008 10:35:45. 396489, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	
03. 04. 2008 10:35:43. 394517, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	
03. 04. 2008 10:35:40. 777079, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.121 : 138 (netbios-dgm)	192.168.169.255 : 138 (netbios-dgm)	
03. 04. 2008 10:35:40. 643115, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	
03. 04. 2008 10:35:39. 777383, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	
03. 04. 2008 10:35:39. 777089, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.121 : 138 (netbios-dgm)	192.168.169.255 : 138 (netbios-dgm)	
03. 04. 2008 10:35:38. 777103, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.121 : 138 (netbios-dgm)	192.168.169.255 : 138 (netbios-dgm)	
03. 04. 2008 10:35:37. 777105, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.121 : 138 (netbios-dgm)	192.168.169.255 : 138 (netbios-dgm)	
03. 04. 2008 10:35:36. 277469, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	
03. 04. 2008 10:35:36. 277409, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	
03. 04. 2008 10:35:36. 277111, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.121 : 138 (netbios-dgm)	192.168.169.255 : 138 (netbios-dgm)	
03. 04. 2008 10:35:34. 777464, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	
03. 04. 2008 10:35:34. 777401, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	
03. 04. 2008 10:35:34. 777104, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.121 : 138 (netbios-dgm)	192.168.169.255 : 138 (netbios-dgm)	
03. 04. 2008 10:35:33. 277454, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	IP / UDP	192.168.169.125 : 138 (netbios-dgm)	192.168.169.127 : 138 (netbios-dgm)	

Рисунок 7.142

Для просмотра всей информации по зарегистрированному пакету, необходимо в соответствующей строке выбрать значок . На экране управляющего компьютера появится окно (рис.7.143) с подробной информацией по выбранном пакете.

Для просмотра зарегистрированных сессий необходимо в окне настроек параметров регистрации (рис.7.136) выбрать слово «Сессии». На экране управляющего компьютера появится окно (рис.7.144) выбора параметров просматриваемых сессий. В этом окне выбираются параметры, по которым необходимо произвести выборку зарегистрированных сессий. По умолчанию задается просмотр всех зарегистрированных сессий. После установки необходимых значений необходимо выбрать кнопку «Показать». На экране управляющего компьютера появится окно (рис.7.145) с зарегистрированной информацией выбранных сессий.

Окно просмотра полной информации о пакете

Регистрация: Детальная информация о пакете

Информация о пакете

Время	Действие	Правила	Интерфейсы	Номер сессии	NAT	Ошибка	Состояние сессии
03. 04. 2008 10:35:47. 398408, MSD	accept	mac:0, ip:0	Internal -> External, DMZ	2			установление соединения - принят первый пакет

Кадр Ethernet

Тип кадра	Протокол	VLAN	MAC-адрес источника	MAC-адрес приемника
Ethernet II	IP/UDP		00:05:5d:e6:0a:bf	ff:ff:ff:ff:ff:ff

IP

TOS	IP флаги (Delay, Throughput, Reliability)	Длина сегмента	Идентификатор	Фрагментация (MF, DF, Offset)	TTL	Протокол	Контрольная сумма	IP-адрес источника	IP-адрес приемника
Routine	Normal, Normal, Normal	214	0xe0a0	0, 0, 0	64	17 (udp)	0xc528	192.168.169.125	192.168.169.127

UDP

Порт источника	Порт приемника	Длина дейтаграммы	Контрольная сумма
138 (netbios-dgm)	138 (netbios-dgm)	194	0x9037

Прикладные данные

```
11 0A 37 29 C0 A8 A9 7D 00 8A 00 AC 00 00 20 45
46 45 4D 45 4E 43 41 43 41 43 41 43 41 43 41 43
41 43 41 43 41 43 41 43 41 43 41 43 41 41 41 00
20 46 48 45 50 46 43 45 4C 45 48 46 43 45 50 46
46 46 41 43 41 43 41 43 41 43 41 43 41 43 41 42
4F 00 FF 53 4D 42
```

```
. . % . . . . . . . . . . . -
. - . - . + ) + ) + ) + ) + ) +
) + ) + ) + ) + ) + ) + ) ) ) .
. . 0 - 2 . + - . - 0 . + - 2 .
. . ) + ) + ) + ) + ) + ) + ) *
. . . 5 . *
```

Закрыть

Текущий пользователь: **admin** © ЗАО "НПО РТК", 2006-2008

Рисунок 7.143

Окно выбора параметров просмотра сессий

Настройки | События | Пакеты | Сессии | Системные сообщения | Очистка файлов регистрации

Регистрация: Сессии

Параметры просмотра

Номер сессии	
Интерфейс клиента	
Интерфейс сервера	
IP-адрес клиента	
IP-адрес сервера	
IP-адреса	
Транспортный протокол	
Прикладной протокол	
Порт клиента	
Порт сервера	
Порт	
Время регистрации сессий	☑ любая дата ☑ любое время 2008/04/03 06:41:34 - 2008/04/03 06:41:34
Сортировка по времени	◉ по убыванию ○ по возрастанию
Записей на страницу	100

Показать Справка

Текущий пользователь: **admin** © ЗАО "НПО РТК", 2006-2008

Рисунок 7.144

Окно просмотра зарегистрированных TCP сессий

Регистрация: Сессии

Закрыть

Сессии

Найдено записей: 1411, Страница 1 из 15
Первая 1 2 3 4 5 6 7 8 9 10 Следующая Последняя

Номер	Время	Правила	Клиент	Сервер	Протоколы	
134	03.04.2008 10:41:02.309137, MSD	ip:0	Internal:192.168.169.121:138 (netbios-dgm)	External,DMZ:192.168.169.255:138 (netbios-dgm)	17 (udp)	
2	03.04.2008 10:41:02.309065, MSD	ip:0	Internal:192.168.169.125:138 (netbios-dgm)	External,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
134	03.04.2008 10:40:32.306071, MSD	ip:0	Internal:192.168.169.121:138 (netbios-dgm)	External,DMZ:192.168.169.255:138 (netbios-dgm)	17 (udp)	
2	03.04.2008 10:39:42.301053, MSD	ip:0	Internal:192.168.169.125:138 (netbios-dgm)	External,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
134	03.04.2008 10:38:52.296061, MSD	ip:0	Internal:192.168.169.121:137 (netbios-ns)	External,DMZ:192.168.169.255:137 (netbios-ns)	17 (udp)	
134	03.04.2008 10:35:52.278094, MSD	ip:0	Internal:192.168.169.121:138 (netbios-dgm)	External,DMZ:192.168.169.255:138 (netbios-dgm)	17 (udp)	
2	03.04.2008 10:35:52.278026, MSD	ip:0	Internal:192.168.169.125:138 (netbios-dgm)	External,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
2	03.04.2008 10:34:42.271015, MSD	ip:0	Internal:192.168.169.125:138 (netbios-dgm)	External,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
1	03.04.2008 10:32:02.254994, MSD	ip:0	External:192.168.169.126:138 (netbios-dgm)	Internal,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
134	03.04.2008 10:30:42.247040, MSD	ip:0	Internal:192.168.169.121:138 (netbios-dgm)	External,DMZ:192.168.169.255:138 (netbios-dgm)	17 (udp)	
2	03.04.2008 10:30:42.246983, MSD	ip:0	Internal:192.168.169.125:138 (netbios-dgm)	External,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
2	03.04.2008 10:29:32.239977, MSD	ip:0	Internal:192.168.169.125:138 (netbios-dgm)	External,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
134	03.04.2008 10:28:32.233979, MSD	ip:0	Internal:192.168.169.121:138 (netbios-dgm)	External,DMZ:192.168.169.255:138 (netbios-dgm)	17 (udp)	
134	03.04.2008 10:25:32.216008, MSD	ip:0	Internal:192.168.169.121:138 (netbios-dgm)	External,DMZ:192.168.169.255:138 (netbios-dgm)	17 (udp)	
2	03.04.2008 10:25:32.215946, MSD	ip:0	Internal:192.168.169.125:138 (netbios-dgm)	External,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
2	03.04.2008 10:24:12.207936, MSD	ip:0	Internal:192.168.169.125:138 (netbios-dgm)	External,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
134	03.04.2008 10:20:22.184972, MSD	ip:0	Internal:192.168.169.121:138 (netbios-dgm)	External,DMZ:192.168.169.255:138 (netbios-dgm)	17 (udp)	
2	03.04.2008 10:20:22.184906, MSD	ip:0	Internal:192.168.169.125:138 (netbios-dgm)	External,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	
1	03.04.2008 10:20:12.183908, MSD	ip:0	External:192.168.169.126:138 (netbios-dgm)	Internal,DMZ:192.168.169.127:138 (netbios-dgm)	17 (udp)	

Рисунок 7.145

Для просмотра всей информации по какой либо сессии, необходимо в соответствующей строке выбрать значок . На экране управляющего компьютера появится окно (рис.7.146) с подробной информацией по выбранной сессии.

Окно просмотра параметров выбранной сессии

Регистрация: Детальная информация о сессии

Сессия 134 подробно	
Время создания	03.04.2008 10:40:41.775433, MSD
Время закрытия	03.04.2008 10:41:02.309137, MSD
Причина закрытия	Тайм-аут неактивности
Состояние сессии	установление соединения - принят первый пакет
Правила	ip:0
Интерфейс клиента	Internal
Интерфейс сервера	External, DMZ
VLAN	-1
IP адрес клиента	192.168.169.121
IP адрес сервера	192.168.169.255
Транспортный протокол	17 (udp)
Порт клиента	138 (netbios-dgm)
Порт сервера	138 (netbios-dgm)
Прикладной протокол	netbios-dgm
Прикладные данные	
Счетчик пакетов клиент/сервер	8/0
Счетчик байт клиент/сервер	1520/0

Закрыть

Текущий пользователь: **admin** © ЗАО "НПО РТК", 2006-2008

Рисунок 7.146

Для просмотра зарегистрированных системных сообщений необходимо в окне настроек параметров регистрации (рис.7.136) выбрать «Системные сообщения». На экране управляющего компьютера появится окно (рис.7.147) просмотра системных сообщений.

Окно просмотра системных сообщений

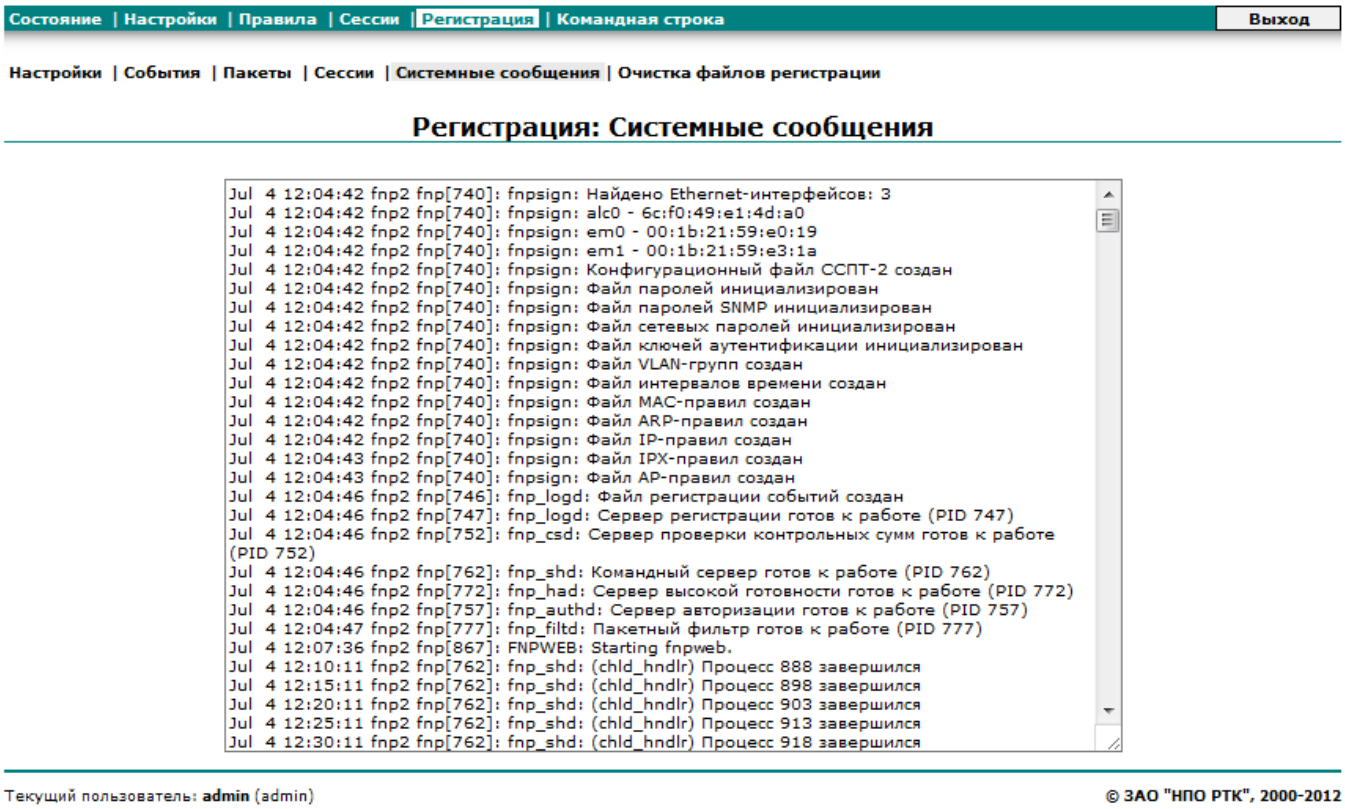

Рисунок 7.147

Для очистки файлов регистрации пакетов и/или сессий необходимо в окне настроек параметров регистрации (рис.7.136) выбрать «Очистка файлов регистрации». На экране управляющего компьютера появится окно (рис.7.148) выбора очищаемого файла.

Окно выбора очищаемого файла

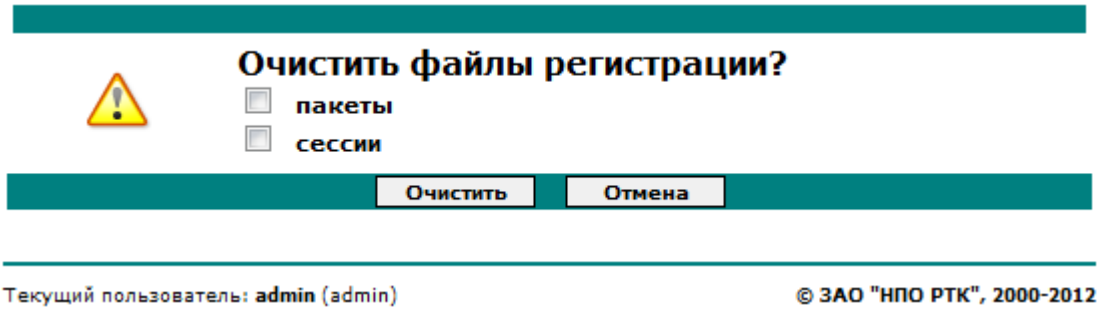

Рисунок 7.148

После выбора очищаемого файла (или файлов) выбирается кнопка «Очистить». На экране управляющего компьютера появится окно (рис.7.149), подтверждающее выполнение операции очистки.

Окно подтверждения очистки файла регистрации пакетов

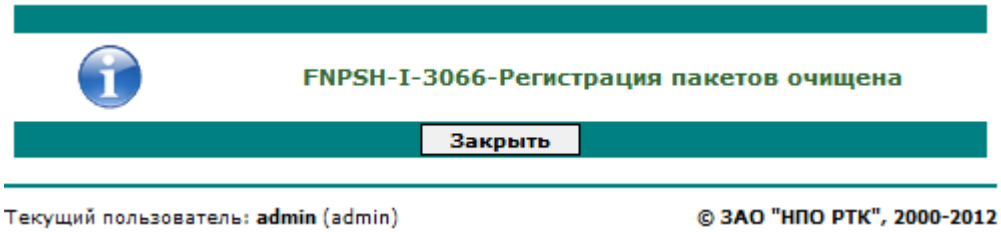

Рисунок 7.149

7.7. Аутентификацией входящих и исходящих запросов

Для включения функции аутентификации входящих и исходящих запросов необходимо в главном окне (рис.7.3) выбрать «Настройки: NAT» (рис.7.32), нажать кнопку «Изменить» и в появившемся окне поставить галочку напротив функции «Аутентификация сетевых пользователей» (рис.7.150). Затем нажать «Сохранить».

Для работы функции аутентификации необходимо, чтобы сетевой пользователь был зарегестрирован на ССПТ. Для того, чтобы зарегестрировать сетевого пользователя, необходимо в окне «Настройки» (рис.7.6) перейти к закладке «Сетевые пользователи» (рис.7.151). Для добавления нового сетевого пользователя необходимо нажать . На экране появится окно (рис.7.152) для добавления нового сетевого пользователя. После внесения всех необходимых данных необходимо нажать кнопку «Сохранить». Для редактирования существующего сетевого пользователя необходимо нажать . В появившемся окне (рис.7.153) необходимо внести все необходимые изменения, после чего нажать кнопку «Сохранить». Для удаления сетевого пользователя необходимо нажать .

Сетевые пользователи, работающий в данный момент через ССПТ-2 отображаются в таблице «Активные сетевые пользователи».

Аутентификация сетевых пользователей

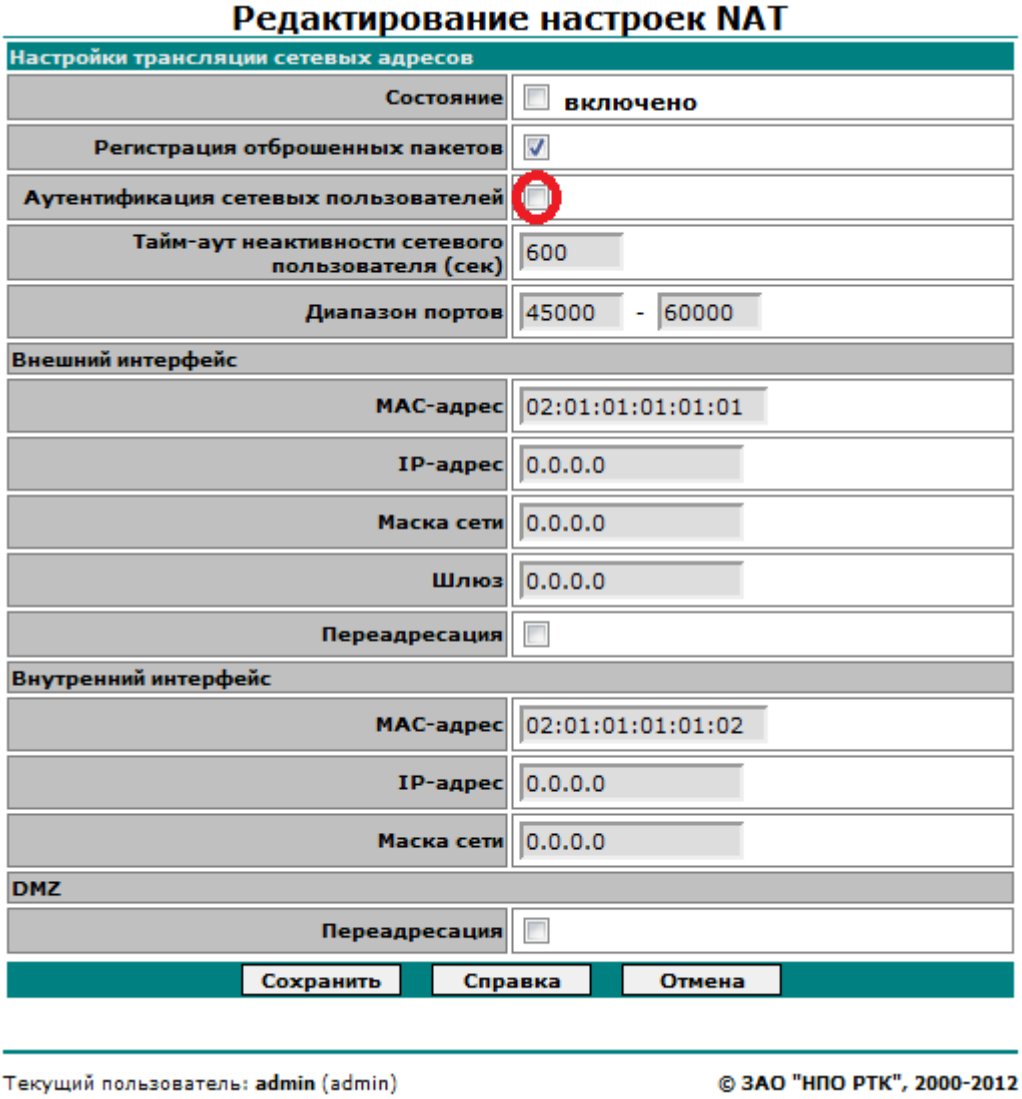

Рисунок 7.150

Настройки: Сетевые пользователи

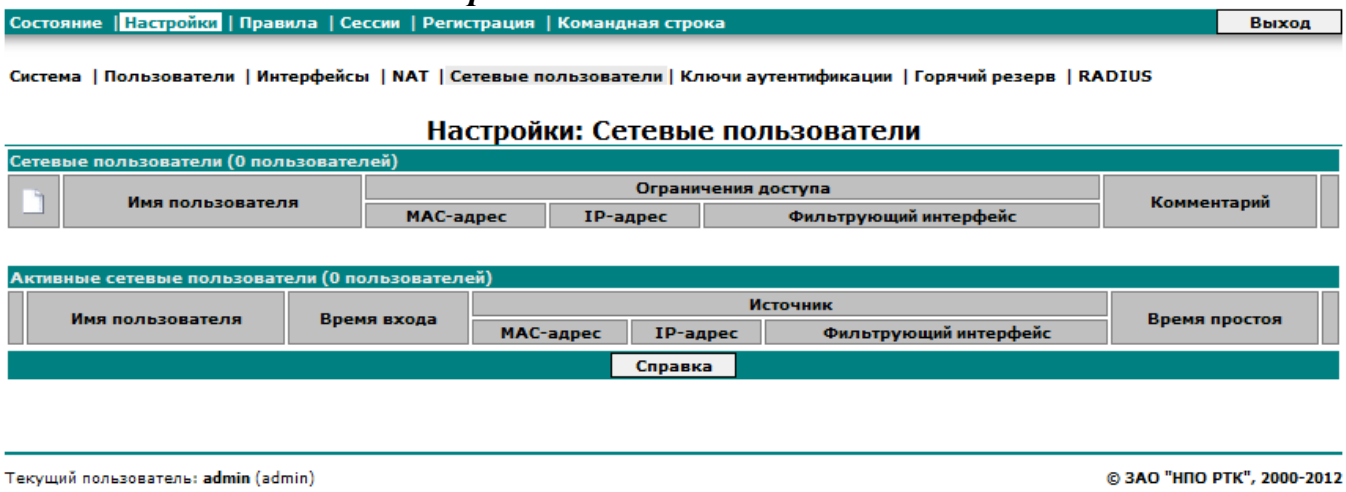

Рисунок 7.151

Добавление нового сетевого пользователя

Добавить нового сетевого пользователя

Параметры сетевого пользователя	
Имя пользователя	
Активность	☑
MAC-адрес	☑ любой
IP-адрес	☑ любой
Фильтрующие интерфейсы	☑ любой ☑ eth0 ☑ eth1
Комментарий	
Пароль	
Пароль (повторно)	

Сохранить | Справка | Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.152

Редактирование сетевого пользователя

Изменить сетевого пользователя

Параметры сетевого пользователя	
Имя пользователя	vvs
Активность	☑
MAC-адрес	☑ любой
IP-адрес	☑ любой
Фильтрующие интерфейсы	☑ любой ☑ eth0 ☑ eth1
Комментарий	
Пароль	
Пароль (повторно)	

Сохранить | Справка | Отмена

Текущий пользователь: **admin** (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.153

Для работы функции аутентификации входящих и исходящих запросов также необходимо сетевому пользователю получить ключи аутентификации, привязанные к ip-адресу компьютера, на котором работает пользователь (рис.7.154). Для этого необходимо на ССПТ-2 сгенерировать ключи аутентификации для каждого сетевого пользователя и установить их на рабочий компьютер пользователя. Скачивание ключей с ССПТ-2 производится с помощью утилиты fnpld. Для добавления нового ключа аутентификации необходимо нажать . В появившемся окне (рис.7.155) необходимо ввести ip-адрес, для которого будут сгенерированы открытый и закрытый ключи аутентификации. После того, как ip-адрес введен необходимо нажать кнопку «Сохранить». Для обновления ключа аутентификации необходимо нажать . В появившемся окне (рис.7.156) нажать кнопку «Обновить». Для удаления ключей аутентификации необходимо нажать . В появившемся окне (рис.7.157) нажать «Да».

Окно получения ключей аутентификации

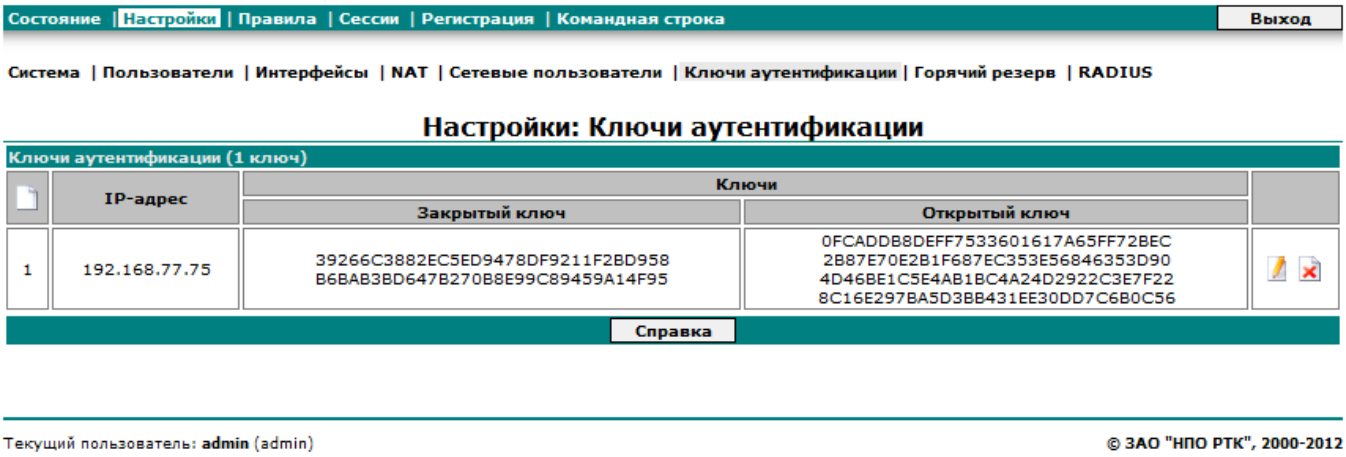

Рисунок 7.154

Окно добавление нового ключа аутентификации

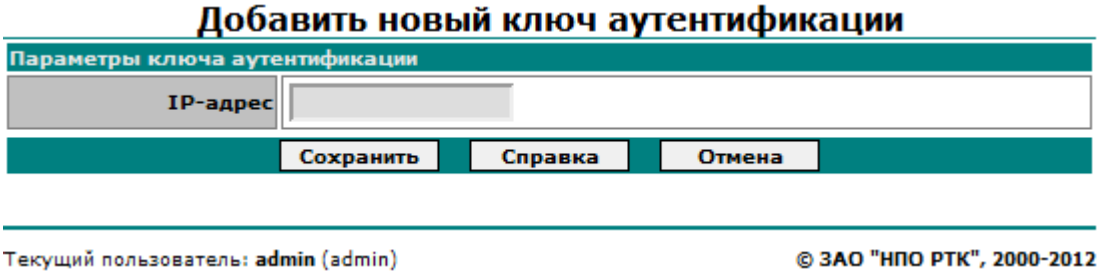

Рисунок 7.155

Окно обновления ключа аутентификации

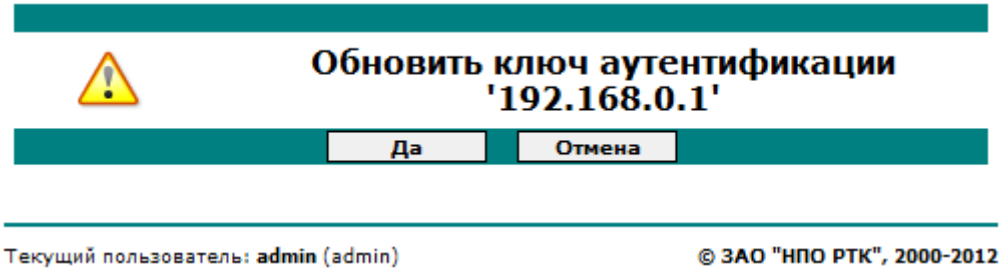

Рисунок 7.156

Окно удаления ключа аутентификации

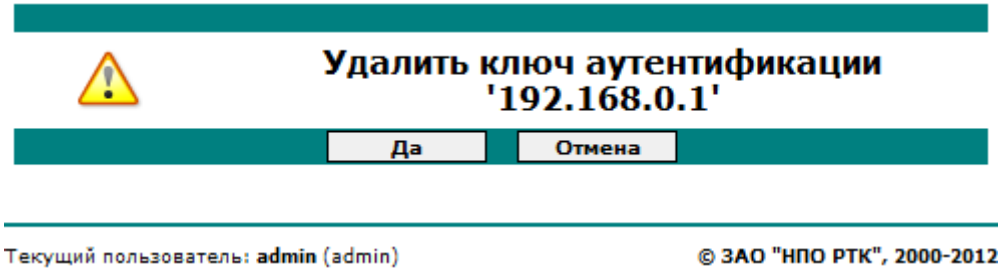

Рисунок 7.157

Функция аутентификации входящих и исходящих запросов работает только при включенном режиме трансляции сетевых адресов (NAT).

7.8. Остановка процесса фильтрации и выход из системы

Для остановки процесса фильтрации необходимо выбрать кнопку «Выключить» в главном окне (рис.7.3). На экране появится запрос на подтверждение команды (рис.7.158).

Остановка процесса фильтрации

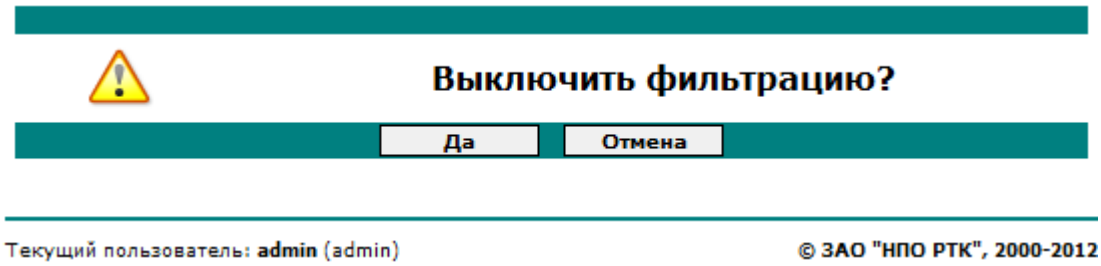

Рисунок 7.158

Если выбрать кнопку «Да», то процесс фильтрации будет отключен (рис.7.159, 7.160).

Сообщение об остановке процесса фильтрации

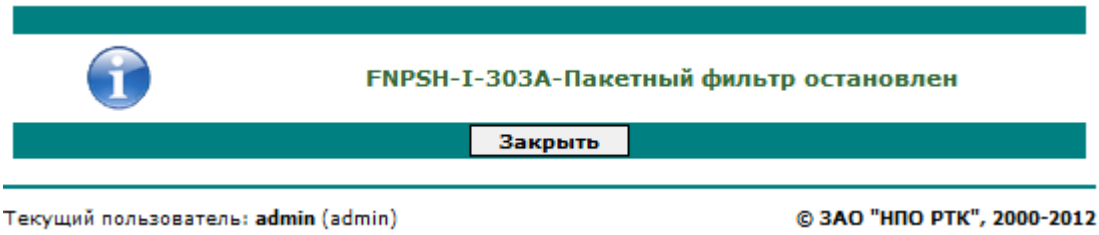

Рисунок 7.159

Главное окно при остановленной фильтрации

Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка Выход

Система | Фильтрация

Состояние: Системная информация

Системная информация	
Центральный процессор	Pentium(R) Dual-Core CPU E5400 @ 2.70GHz
Ядер ЦПУ	2
Объем памяти	1063124992
Версия ПО ССПТ-2	FNP2_SNAPSHOT_1_3-p1.2 (Jul 3 2012)
Всего интерфейсов	3
Фильтрующие интерфейсы	2: eth0, eth1
Тайм-аут неактивности пользователя (сек)	600
Управляющий интерфейс	
IP-адрес	192.168.78.5
Маска сети	255.255.255.0
Несущая/Скорость	100baseTX/full-duplex
Состояние процессов	
Пакетная фильтрация	Включить
Контроль целостности	
Авторизация	
Регистрация	
Резервирование	
Удаленное администрирование	
SNMP интерфейс	
Управление устройством	
	Останов/Перезагрузка

Справка

Текущий пользователь: admin (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.160

Для запуска процесса фильтрации необходимо выбрать кнопку «Старт» в главном окне (рис.7.160). На экране появится запрос на подтверждение команды (рис.7.161).

Запрос на возобновление процесса фильтрации

Включить фильтрацию?

Да Отмена

Текущий пользователь: admin (admin) © ЗАО "НПО РТК", 2000-2012

Рисунок 7.161

Если выбрать кнопку «Да», то процесс фильтрации будет запущен

(рис.7.162), а главное окно примет прежний вид.

Сообщение о возобновлении процесса фильтрации

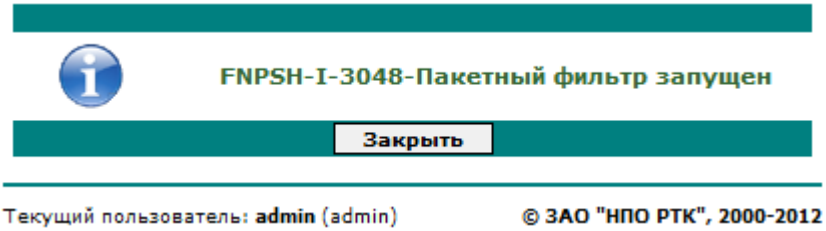

Рисунок 7.162

Для штатного выхода из системы и прекращения управления изделием по WEB интерфейсу необходимо в главном окне выбрать кнопку «Выход» (рис.7.3, 7.160). На экране появится запрос на подтверждение команды (рис.7.163).

Запрос на прекращение управления изделием по WEB интерфейсу

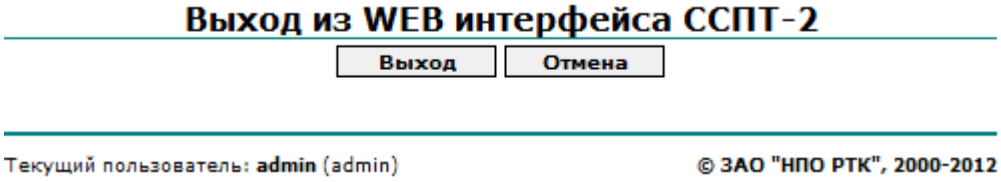

Рисунок 7.163

Если выбрать кнопку «Да», то управление изделием будет прервано, а на экране появится приглашение к входу в систему (рис.7.1).

Лист регистрации изменений

Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в докум.*	*№ докум.*	*Входящий № сопроводительного докум. и дата*	*Подп*	*Дата*
	измененных	*замененных*	*новых*	*аннулированных*					

№ изм.	**Подпись**	**Дата**