ZENATOR R Rt

Руководство оператора

ИСКП.30334-01 34 01

Листов 46

2022

АННОТАЦИЯ

Данный документ является руководством оператора для Zenator R Rt (программного обеспечения граничного маршрутизатора на аппаратной платформе с архитектурой x86), далее по тексту – Zenator R Rt или программа.

Документ описывает назначение, условия и порядок функционирования Zenator R Rt, а также действия оператора при запуске и во время выполнения программы.

Настоящее руководство входит в состав эксплуатационной документации и рассчитано на пользователя, имеющего навыки работы в операционной системе (ОС) Linux.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Zenator R Rt выполняет функции программного обеспечения (ПО) граничного маршрутизатора.

1.2. Zenator R Rt обеспечивает явное задание скорости интерфейса Ethernet (10/100/1000), режима работы (half duplex, full duplex), автосогласование.

1.3. Zenator R Rt обеспечивает явную настройку максимального размера полезного блока данных (MTU) на сетевых интерфейсах, в том числе и на туннельных.

1.4. Zenator R Rt обеспечивает функционирование по протоколу IPv4 и IPv6.

1.5. Zenator R Rt обеспечивает вывод в интерфейс управления статистики по сетевым интерфейсам (тип/количество ошибок, тип/количество переданных/принятых пакетов).

1.6. Zenator R Rt имеет возможность назначения и (или) изменения MAC-адреса на своих интерфейсах и подынтерфейсах.

1.7. Zenator R Rt обеспечивает поддержку loopback-интерфейсов.

1.8. Zenator R Rt обеспечивает возможность назначения нескольких IP-адресов на своих интерфейсах и подынтерфейсах.

1.9. Zenator R Rt обеспечивает статическое и динамическое заполнение таблицы MAC-адресов с помощью протокола разрешения адресов (ARP).

1.10. Zenator R Rt имеет возможность функционирования как ARP-proxy.

1.11. Zenator R Rt обеспечивает:

– производительность не менее 3000000 пакетов/с (таблицы фильтрации пустые, настройки приоритезации отсутствуют, длина пакета 64 байта);

– производительность не менее 2000000 пакетов/с (при заполненной таблице маршрутизации – 1000 маршрутов, заполненной таблице фильтрации – 1000 записей и настроенной приоритезации – 1000 классов, длина пакета 64 байта).

1.12. Для локального управления в Zenator R Rt используется выделенный порт RS-232/Ethernet.

1.13. В Zenator R Rt реализована поддержка групповой передачи данных «multicast routing».

1.14. Zenator R Rt обеспечивает обработку Jumbo Frames (более 9000 байт) на всех интерфейсах, кроме выделенного порта управления.

1.15. В Zenator R Rt обеспечивается статическая маршрутизация пакетов.

1.16. Zenator R Rt обеспечивает функционирование по протоколам динамической маршрутизации:

– протокол маршрутизации (RIPv2);

– протокол маршрутизации для IPv6 (RIPng);

– протокол динамической маршрутизации (OSPFv3);

– пограничный межсетевой протокол (BGPv4).

Примечание. Блокировка протоколов динамической маршрутизации обеспечивается программным способом.

1.17. Zenator R Rt обеспечивает настройку таймеров OSPFv3.

1.18. Zenator R Rt обеспечивает маршрутизацию на основе политик (policy-routing).

1.19. Zenator R Rt обеспечивает возможность балансировки нагрузки при наличии нескольких маршрутов с одинаковой метрикой.

1.20. В Zenator R Rt реализована возможность автоматического переключения на резервный канал по сетевому протоколу, объединяющему группу маршрутизаторов в один виртуальный маршрутизатор (VRRP).

1.21. Zenator R Rt обеспечивает функционирование по протоколу управления групповой передачей данных (IGMPv3);

1.22. Zenator R Rt обеспечивает перераспределение маршрутной информации:

– между протоколами внутренних маршрутизаторов (IGP) маршрутизации;

– между IGP и BGP;

– статических маршрутов в протоколы динамической маршрутизации.

1.23. Zenator R Rt обеспечивает настройку маршрутизации выделенных IP-потоков в туннели PPPoE и PPTP как с клиентской, так и с серверной стороны туннеля.

1.24. Zenator R Rt обеспечивает функционирование туннелей по протоколам:

– туннельный протокол типа «точка-точка» в стандартной, незащищенной сети (PPTP);

– сетевой протокол канального уровня передачи кадров PPP через Ethernet (PPPoE);

– протокол туннелирования сетевых пакетов (GRE);

– протокол туннелирования «IP over IP» (IPIP).

1.25. Zenator R Rt обеспечивает функционирование туннельного протокола протокола типа «точка-точка» (PPP).

1.26. Zenator R Rt поддерживает протокол туннелирования второго уровня L2TP.

1.27. Zenator R Rt обеспечивает функционирование защищенной виртуальной частной сети (VPN) на основе OpenVPN.

1.28. Zenator R Rt обеспечивает фильтрацию фрагментированных пакетов.

1.29. Zenator R Rt обеспечивает фильтрацию на всех интерфейсах (реальных и виртуальных).

1.30. Zenator R Rt поддерживает правила фильтрации при перераспределении маршрутной информации.

1.31. Zenator R Rt обеспечивает возможность снятия бита DF на сетевых интерфейсах.

1.32. Zenator R Rt обеспечивает возможность изменения значения максимального размера полезного блока данных (MSS) в TCP-пакетах для предотвращения Path MTU Discovery Black Hole.

1.33. Zenator R Rt обеспечивает фильтрацию входящего, исходящего и пересылаемого трафика.

1.34. Zenator R Rt обеспечивает маркировку и перемаркировку кадров/пакетов в трех битах в теге 802.1Q Ethernet-кадра и поле «ToS» (TOS/DSCP) заголовка IP по следующим критериям:

– порт (TCP/UDP) отправителя;
– порт (TCP/UDP) получателя;
– IP-адрес отправителя;
– IP-адрес получателя;
– MAC-адрес отправителя;
– значение поля «Протокол» заголовка IP;
– значение поля «ToS» (TOS/DSCP) заголовка IP;
– длина пакетов;
– значение трех битов в теге 802.1Q Ethernet-кадра;
– совокупность указанных критериев.

1.35. Zenator R Rt обеспечивает функционирование клиента сервиса доменных имён (DNS) и кэширующего DNS-сервера.

1.36. В Zenator R Rt реализована фильтрация IP-пакетов в соответствии с заданными правилами фильтрации на основе:

– сетевых интерфейсов;

– порта (TCP/UDP) отправителя;

– порта (TCP/UDP) получателя;

– IP-адреса отправителя;

– IP-адреса получателя;

– MAC-адреса отправителя;

– флагов заголовков сегмента TCP;

– значения поля «Протокол» заголовка IP;

– значения поля «ToS» (TOS/DSCP) заголовка IP;

– состояния соединений;

– прикладных протоколов с использованием регулярных выражений;

– мандатных меток, с возможностью преобразования форматов;

– совокупности указанных критериев.

1.37. Zenator R Rt обеспечивает средства расширенной сетевой диагностики.

1.38. Zenator R Rt обеспечивает запрашивающие хосты IP-адресами и другими конфигурационными параметрами с помощью протокола динамической конфигурации хоста (DHCP).

1.39. Zenator R Rt обеспечивает возможность автоматического разделения одного физического сетевого интерфейса на несколько логических подынтерфейсов.

1.40. В Zenator R Rt реализована возможность ограничения числа одновременных соединений с одного IP-адреса.

1.41. В Zenator R Rt реализована возможность поддержки добавления/удаления мандатных меток безопасности в поле опций IP-заголовка.

1.42. Zenator R Rt обеспечивает три базовые концепции трансляции адресов:

– статическая (SNAT);

– динамическая (DAT);

– маскарадная – преобразование сетевых адресов и портов (NAPT), преобразование сетевых адресов (NAT) Overload, трансляция сетевого адреса в зависимости от TCP/UDP-порта получателя (PAT).

1.43. Zenator R Rt поддерживает настройку демилитаризованной зоны (DMZ) в сочетании с маршрутизацией и трансляцией адресов NAT или трансляцией портов PAT.

1.44. Zenator R Rt обеспечивает запрашивающие хосты IP-адресами и другими конфигурационными параметрами посредством DHCPv4.

1.45. Zenator R Rt обеспечивает распределение IP-адресов на определенный срок.

1.46. Zenator R Rt обеспечивает распределение IP-адресов с помощью DHCP тремя способами:

– ручное распределение;

– автоматическое распределение;

– динамическое распределение.

1.47. Zenator R Rt обеспечивает настройку интерфейса автоконфигурированием с помощью DHCP.

1.48. Zenator R Rt обеспечивает ретрансляцию сообщений DHCP между клиентами и серверами в разных подсетях.

1.49. Zenator R Rt предоставляет возможность конфигурирования себя с помощью интерфейса командной строки (CLI) следующими способами:

– локально (путем ввода с клавиатуры текстовых команд или через выделенный порт управления);

– удаленно (при подключении по сетевому протоколу прикладного уровня (SSH), простому протоколу сетевого управления (SNMP), с помощью прикладного программного интерфейса передачи состояния представления (REST API) или Telnet).

Примечания:

1. Zenator R Rt обеспечивает возможность отключения (блокирования) любого из способов управления.

2. Zenator R Rt обеспечивает возможность ограничения доступа к управлению только с доверенных IP-адресов, либо подсетей.

3. SNMP поддерживается в режиме мониторинга.

1.50. Zenator R Rt обеспечивает проверку корректности основных задаваемых параметров функционирования.

1.51. Zenator R Rt обеспечивает вывод текстового предупреждения в CLI при некорректно задаваемом параметре.

1.52. Zenator R Rt обеспечивает сохранение сконфигурированных профилей.

1.53. Zenator R Rt имеет возможность вывода информации о текущей загруженности центрального процессора и оперативного запоминающего устройства.

1.54. Zenator R Rt имеет возможность поддерживать работу сервиса сторожевого таймера («watchdog») для выполнения автоматической перезагрузки устройства в случае прекращения нормального функционирования демона (зависания).

1.55. Zenator R Rt имеет возможность вывода имеющихся в системе профилей, а также их копирования.

1.56. Zenator R Rt обеспечивает применение сохраненных профилей.

1.57. В Zenator R Rt разработан механизм управления очередями, предусматривающий поддержку методов CBQ, HFSC, FIFO, PQ, TBF, HTB.

1.58. Zenator R Rt обеспечивает возможность задать полосу пропускания в процентах для определенного администратором типа трафика.

1.59. Zenator R Rt обеспечивает задание статических IP-адресов своим интерфейсам и подынтерфейсам.

1.60. Zenator R Rt обеспечивает классификацию и приоритетную обработку пакетов по следующим критериям:

– порт (TCP/UDP) отправителя;
– порт (TCP/UDP) получателя;
– IP-адрес отправителя;
– IP-адрес получателя;
– MAC-адрес отправителя;
– значение поля «Протокол» заголовка IP;
– значение поля «ToS» (TOS/DSCP) заголовка IP;
– длина пакетов;
– значение трех битов в теге 802.1Q Ethernet-кадра;
– совокупность указанных критериев.

1.61. Zenator R Rt обеспечивает функционирование протокола обнаружения соседей (NDP).

1.62. В Zenator R Rt реализовано предупреждение перегрузок с поддержкой механизмов RED, ECN, GRED.

1.63. Zenator R Rt обеспечивает функционирование протокола передачи точного времени NTPv4 (Network Time Protocol) клиента/сервера с возможностью явно задать часовой пояс.

1.64. Zenator R Rt обеспечивает функционирование виртуальной локальной сети VLAN согласно стандарту Института Инженеров Электротехники и Электроники (IEEE) 802.1Q.

1.65. Zenator R Rt обеспечивает добавление и снятие тегов VLAN IEEE 802.1Q, VLAN QinQ IEEE 802.1ad на интерфейсах, работающих в режиме коммутатора.

1.66. Zenator R Rt обеспечивает возможность агрегации сетевых интерфейсов в группу IEEE 802.3ad.

1.67. Zenator R Rt обеспечивает функционирование протокола оповещения канального уровня (LLDP).

1.68. Zenator R Rt обеспечивает перенаправление (зеркалирование) трафика.

1.69. Zenator R Rt обеспечивает автоматическое создание логических подынтерфейсов сетевого уровня для каждого тега VLAN 802.1Q или совокупности верхнего и нижнего тегов VLAN QinQ, с возможностью привязки их к физическим портам.

1.70. Zenator R Rt обеспечивает возможность программного объединения портов Ethernet по технологии Bridge.

1.71. Zenator R Rt обеспечивает создание и функционирование через шифрованный IP-туннель IPSec.

1.72. Zenator R Rt обеспечивает преобразование сетевых адресов NAT.

1.73. В Zenator R Rt реализована система ролевого доступа со следующими пользователями:

– администратор сети (с функцией настройки сетевых интерфейсов и служб);

– администратор безопасности (с функцией настройки туннелей (VPN-соединений) и правил межсетевого экранирования);

– администратор аудита (с функцией доступа на чтение).

1.74. Zenator R Rt обеспечивает ведение следующих журналов регистрации:

– журнал «ids» (журнал системы обнаружения вторжений);

– журнал «auth» (журнал информации о фактах идентификации, аутентификации);

– журнал «ipfilter» (журнал событий срабатывания правил межсетевого экранирования);

– журнал «commands» (команды администратора Zenator R Rt, вводимые с консоли управления);

– журнал «daemon» (внутренний журнал агента управления Zenator R Rt);

– журнал «testing» (информация о самотестировании);

– журнал «syslog» (информация от ядра операционной системы и системных утилит);

– журнал «router» (информация о работе протоколов динамической маршрутизации).

1.75. В Zenator R Rt обеспечивается регистрация следующих событий:

– загрузка, инициализация системы и её остановка;

– вход/выход пользователей в систему/из системы, с фиксацией ошибок авторизации;

– результат фильтрации входящих/исходящих пакетов.

1.76. В Zenator R Rt при регистрации событий фиксируются:

– дата и время регистрируемого события;

– IP-адрес источника и IP-адрес получателя (при фильтрации), включая порты протоколов TCP, UDP.

1.77. В Zenator R Rt осуществляется автоматический контроль целостности ПО.

1.78. Zenator R Rt поддерживает протокол аутентификации, авторизации, сбора сведений об использованных ресурсах (RADIUS).

1.79. Zenator R Rt поддерживает протокол экспорта информации по IP-потоку (IPFIX).

1.80. Zenator R Rt поддерживает миграцию базовых настроек между версиями ПО.

1.81. Zenator R Rt поддерживает возможность программного отключения неиспользуемых портов и сервисов.

1.82. Zenator R Rt поддерживает передачу данных о событиях на удаленный сервер (syslog, SNMP trap).

1.83. Zenator R Rt обеспечивает программное определение позиций интерфейсов.

1.84. Zenator R Rt обеспечивает возможность обновления ПО.

1.85. Zenator R Rt обладает функциями самотестирования (проверки работоспособности).

1.86. Zenator R Rt обеспечивает проведение анализа трафика и применение необходимых сигнатур для корректного и точного обнаружения уязвимостей.

1.87. Zenator R Rt обеспечивает выявление признаков компьютерных атак, распределенных по нескольким сетевым пакетам.

1.88. Zenator R Rt обеспечивает поддержку статистического метода выявления аномалий сетевого трафика типа DoS-flooding.

1.89. Zenator R Rt обеспечивает возможность эвристического метода выявления сетевых атак, таких как «port scans», «host sweeps».

1.90. Zenator R Rt обеспечивает выявление в сетевом трафике нестандартных и фрагментированных пакетов формируемых протоколом межсетевых управляющих сообщений (ICMP).

1.91. Zenator R Rt обеспечивает функционирование механизмов «Flood protection» для обнаружения атак типа IP Flood (SYN, ICMP, UDP).

1.92. Zenator R Rt обеспечивает пассивный мониторинг протокола DNS в сетевом трафике с целью определения скомпрометированных доменов и блокирования запросов на URL-адреса.

1.93. Zenator R Rt обеспечивает обнаружение и блокировку атак типа дефрагментация IP, «пересборка» TCP, а также блокировку некорректных сетевых пакетов.

1.94. Zenator R Rt обеспечивает возможность добавления/редактирования сигнатур атак и эвристических правил выявления перспективных атак.

1.95. Zenator R Rt обеспечивает возможность удаленного обновления баз сигнатур атак и эвристических правил.

1.96. Zenator R Rt обеспечивает поддержку двойного стека протоколов IPv4 и IPv6.

1.97. В Zenator R Rt порты Ethernet, объединенные по технологии Bridge, должны иметь общий IP-адрес.

1.98. Zenator R Rt обеспечивает вывод в интерфейс управления информации об источниках маршрутов в таблице маршрутизации.

1.99. Zenator R Rt обеспечивает возможность просмотра через интерфейс управления таблицы принятых и анонсируемых маршрутов BGPv4.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Требования к техническим средствам

2.1.1. Zenator R Rt должен устанавливаться на аппаратную платформу (АП) «Сервер MS-3040» ЦРМП.466219.001 или на АП со следующими характеристиками:

1) процессор с архитектурой x86;

2) оперативная память – не менее 4 Гбайт;

3) постоянное запоминающее устройство – не менее 16 Гбайт;

4) интерфейс USB – не менее одного;

5) интерфейс стандарта RS-232 – не менее одного;

6) интерфейс Ethernet 10/100/1000BaseT, соответствующий требованиям IEEE 802.3u, 802.3ab – не менее двух;

7) интерфейс Ethernet 1000Base-X – не менее двух;

8) интерфейсный модуль SFP – не менее двух с характеристиками:

– стандарт Ethernet – 1000Base-LX;

– тип разъема – LC;

– тип волокна – одномодовое;

– длина волны – не менее 1310 нанометра;

– скорость передачи данных – до 1,25 Гбайт/с;

– рабочая дистанция – не менее 2000 м;

– количество волокон – не менее двух;

9) интерфейсный модуль SFP с характеристиками:

– стандарт Ethernet – 1000Base-T;

– тип разъема – RJ-45;

– тип кабеля – UTP-5;

– скорость передачи данных – до 1,25 Гбайт/с;

– рабочая дистанция – не менее 100 м.

Примечания:

1. Порт RS-232 необходим для технологического управления изделием в отсутствии подключаемых клавиатуры и монитора. На некоторых АП он может отсутствовать.

2. Количество интерфейсов Ethernet и SFP определяется договором поставки. Допускается применение интерфейсов SFP+.

2.1.2. В зависимости от версии ПО и комплектации оборудования функциональные возможности программы могут отличаться.

2.1.3. Для эксплуатации программы необходимо наличие не менее двух штатных единиц – администратора безопасности и администратора сети.

2.2. Требования к пользователю

2.2.1. Zenator R Rt используется в сетях связи, обрабатывающих информацию разной степени конфиденциальности.

При использовании Zenator R Rt применяются следующие требования:

– для обработки сведений, содержащих государственную тайну, люди, допущенные к работе с программой, должны действовать в соответствии с законом РФ «О государственной тайне» от 21.07.1993 № 5485-1, а также политикой безопасности и правилами обработки сведений, содержащих государственную тайну, утвержденными на предприятии;

– для обработки сведений, содержащих коммерческую тайну, люди, допущенные к работе с программой, должны действовать в соответствии с законом РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ, а также политикой безопасности и правилами обработки сведений, содержащих коммерческую тайну, утвержденными на предприятии.

2.2.2. Для работы с Zenator R Rt пользователю необходимо обладать следующими профессионально-техническими навыками:

– знать принципы функционирования и обладать опытом администрирования локальных вычислительных сетей;

– знать правила передачи информации, содержащей государственную или коммерческую тайну, по открытым каналам связи;

– знать средства и механизмы защиты информации, которые могут использоваться для передачи информации, содержащей государственную или коммерческую тайну, по открытым каналам связи и обладать опытом их использования;

– обладать навыками работы с ОС Linux на уровне опытного пользователя.

2.2.3. Для обслуживания программы необходимо не менее двух штатных единиц – администратор безопасности и администратор сети (пользователь программы).

Администратор безопасности должен иметь профильное образование в области информационной безопасности и обладать навыками в области администрирования средств защиты информации, а также иметь опыт администрирования локальных вычислительных сетей связи.

Администратор сети должен иметь опыт администрирования локальных вычислительных сетей связи.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Вход в программу

3.1.1. Для входа в программу необходимо к АП подсоединить технологическую персональную электронно-вычислительную машину (ПЭВМ) через USB-COM и COM-RJ 45.

3.1.2. Запустить технологическую ПЭВМ и авторизоваться в ОС.

Примечание. Установленная на технологическую ПЭВМ ОС должна быть сертифицированна.

3.1.3. Для установки сеанса связи между ПЭВМ и АП через последовательный COM-порт установить эмулятор терминала для ОС, установленной на ПЭВМ, аналогичный «minicom» для ОС на базе ядра Linux.

В данном руководстве в качестве примера описан вариант установки и настройки эмулятора терминала «minicom» на ПЭВМ с предустановленной ОС «Astra Linux Special Edition» версии 1.5. Перед началом работы необходимо:

1) открыть окно терминала, нажав сочетание клавиш «Alt + T»;

2) установить «minicom» с помощью команды

apt-get install minicom

Примечание. При установке «minicom» будет запрошен инсталляционный диск ОС;

3) запустить «minicom» с помощью команды

minicom -s

4) в открывшемся окне настройки конфигурации выполнить следующие действия:

– выбрать пункт «Настройка последовательного порта» и нажать «Enter»;

– убедиться (при необходимости выставить) в том, что для параметра «Скорость/Четность/Биты» выставлено значение «115200 8N1»;

– для параметров «Аппаратное управление потоком» и «Программное управление потоком» выставить значение «нет» и нажать «Enter»;

– выбрать пункт «Сохранить настройки как df1» и нажать «Enter»;

– выбрать пункт «Выход из Minicom» и нажать «Enter»;

5) в консоли включить «minicom» с помощью команды

minicom -D /dev/ttyUSB0

где ttyUSB0 – имя и номер последовательного порта, к которому подключена АП.

3.1.4. Запустить АП по питанию.

3.1.5. При включении АП автоматически запускается Zenator R Rt, и начинается процедура самотестирования, при этом осуществляются следующие проверки целостности:

– файловой системы;

– ПО;

– аппаратной конфигурации.

3.1.6. После запуска программы на АП в консоли технологической ПЭВМ необходимо авторизоваться.

В поле «zenator login: » ввести имя пользователя «admsec» и нажать клавишу «Enter».

В поле «Password: » ввести пароль «12345678i.» и нажать клавишу «Enter».

Примечания:

1. Пароль на экране не отображается. Данный пароль устанавливается «по умолчанию» в процессе инсталляции программы.

2. При первом запуске рекомендуется сменить пароль на более безопасный.

3. Длина задаваемого пароля не должна превышать 32 символа.

3.1.7. После входа в систему в консоли ПЭВМ появятся следующие сообщения:

1) «Welcome <name>!» – приглашение входа в систему с учетной записью «name» («name» – имя пользователя);

2) «zenator>» – строка приглашения к вводу команд.

3.2. Настройка программы

3.2.1. Общие сведения

3.2.1.1. Настройку программы следует производить с использованием созданной учетной записи из консоли ПЭВМ с помощью команд CLI.

3.2.1.2. Подробное описание команд CLI и их параметров для настройки программы приведено в приложении к данному руководству ИСКП.30334-01 34 01-1.

3.2.1.3. При описании формата вызова команды используются символы: квадратные скобки ([ ]), фигурные скобки ({ }), угловые скобки (< >) и вертикальная черта (|). При записи формата действуют следующие соглашения:

– параметры, указанные в квадратных скобках ([ ]), считаются необязательными;

– параметры, указанные в фигурных скобках ({ }), считаются обязательными;

– параметры, не заключенные ни в квадратные, ни в круглые скобки, считаются обязательными;

– параметры, указанные в угловых скобках (< >) являются значением параметра;

– вертикальная черта (|) указывает, что следует выбрать только один из перечисленных параметров. Например, запись вида «[a | b]» означает, что можно выбрать либо параметр «a», либо параметр «b», либо ни один из параметров. Аналогично, запись вида «{ a | b }» означает, что нужно выбрать либо параметр «a», либо параметр «b».

3.2.1.4. При описании команд используются одни и те же параметры. Назначение этих параметров приводится при первом упоминании в команде. Далее, в последующих командах, их описание может отсутствовать.

Примечание. Приведенные правила описания команд действуют в рамках каждого подраздела руководства.

3.2.1.5. Действия оператора должны осуществляться в соответствии с подсказками, выдаваемыми в процессе настройки программы. Для вызова подсказки к команде необходимо нажать сочетание клавиш «Shift+?».

3.2.1.6. Программа обеспечивает автодополнение команд по нажатию клавиши «Tab».

В случае, если команда состоит из одного слова, то при нажатии на клавишу «Enter» происходит автодополнение и последующее выполнение команды. В случае, если команда состоит из двух слов, то при вводе первого слова и нажатии на клавишу «Enter» происходит автодополнение первого слова, при вводе второго слова и нажатии на клавишу «Enter» происходит автодополнение второго слова и выполнение команды. В случае, если команда состоит из трех и более слов, автодополнение по клавише «Enter» не выполняется.

Автодополнение команд по клавише «Пробел» выполняется только при введении команд. При вводе значений параметров автодополнение не выполняется.

3.2.1.7. Получение справочной информации по конкретной команде выполняется командой

help <command_name>

где <command_name> – имя команды.

При нажатии клавиш «Tab» или «Пробел» на экран будет выведен список всех модулей системы, для которых выполняется данная команда.

3.2.1.8. Команды «commit», «rollback», «discard», «diff» и «! [<comments>]» выполняются в тех режимах конфигурации, в которых они доступны.

3.2.1.9. Применение последних изменений выполняется командой

commit [complete | confirmed] [delay][comment]

где complete – гарантированное завершение отложенного коммита;

confirmed – запуск процедуры отложенного коммита. В случае невыполнения завершения отложенного коммита за время задержки выполняется откат конфигурации (rollback);

delay – задержка в секундах перед выполнением команды «rollback»;

comment – описание для коммита, задается в двойных кавычках.

Примечания:

1. Если изменения конфигурации не применены, то в строке приглашения к вводу команд присутствует «!». После выполнения команд «discard» или «commit» знак «!» пропадает.

2. Команда «commit» не выполняется, если после выполнения любой команды в строке приглашения к вводу команд отсутствует «!».

3.2.1.10. Вывод статуса применения конфигурации выполняется с помощью команды

show commit status

3.2.1.11. Отмена последних изменений, примененных командой «commit», выполняется с помощью команды

rollback

3.2.1.12. Проверка конфигурации системы или отдельного модуля, выполняется с помощью команды

check commit [<module>]

где <module> – модуль, для которого необходимо проверить конфигурацию.

3.2.1.13. Вывод всех последних изменений, еще не примененных командой «commit», выполняется с помощью команды

diff

Примечание. Если после выполнения команды «commit» никаких изменений выполнено не было, то на экран ничего выведено не будет.

3.2.1.14. Отмена последних изменений, не примененных командой «commit», выполняется с помощью команды

discard [<mod-name>]

где <mod-name> – модуль, для которого необходимо отменить последние изменения.

При нажатии клавиш «Tab» или «Пробел» на экран будет выведен список всех модулей системы, для которых выполняется данная команда.

Примечание. Если параметр «mod-name» не указывать, то отмена последних изменений, не примененных командой «commit», будет выполнена для всех модулей.

3.2.1.15. Если после выполнения команды «commit» были выполнены изменения, то на экране будет отображен модуль, где будут указаны предыдущая конфигурация системы и текущая конфигурация системы. Знаком «-» и красным цветом обозначена предыдущая конфигурация системы, знаком «+» и зеленым цветом обозначена текущая конфигурация системы (команда «commit» еще не выполнялась). Для отмены выполнения команды, а также для удаления заданных параметров к команде добавляется префикс «no».

Примечание. Префикс «no» используется только для тех команд, в которых он доступен.

3.2.1.16. Программа обеспечивает возможность настройки системы с помощью команд основной конфигурации, а также выполнением команд доступных в режиме конфигурации.

После входа в режим конфигурации обеспечивается возможность выполнения команд конфигурации с помощью префикса «do» добавленного к команде

do <command>

где <command> – команда из режима основной конфигурации.

Примечание. С префиксом «do» могут выполняться все команды основной конфигурации, кроме «discard», «load» и «commit».

3.2.1.17. Для активации/деактивации системного почтовика используется команда

system mailer {integrity | login | ids | alert | failure} {on | off}

где on – включение системного менеджера;

off – выключение системного менеджера.

3.2.1.18. Добавление комментария в историю пользовательского ввода выполняется при помощи специального символа «!» следующим образом

! [<comments>]

где <comments> – комментарий.

3.2.1.19. При работе с системой рекомендуется использование USB-накопителей с архитектурой файловой системы Ext2, Ext3, Ext4 и VFAT. Для обмена данными с ОС Windows необходимо использовать файловую систему VFAT.

3.2.2. Настройка аутентификации

3.2.2.1. Для задания режима аутентификации используется команда

system authentication mode {session | command}

где session – сессионный режим;

command – покомандный режим.

3.2.2.2. Для задания минимальной длины пароля используется команда

system authentication password min-length <min_len>

где <min_len> – значение минимальной длины пароля в символах. Может принимать значения от «1» до «256». Значение «по умолчанию» равно «1».

3.2.2.3. Для установки требуемого уровня сложности пароля используется команда

system authentication password complexity <complexity>

где <complexity> – уровень сложности пароля, может принимать значения от «0» до «3». Значение «по умолчанию» равно «0».

Для уровня сложности равного:

– «0» – требования к паролю не предъявляются;

– «1» – пароль должен содержать прописные и строчные буквенные символы;

– «2» – пароль должен содержать прописные и строчные буквенные символы, цифры;

– «3» – пароль должен содержать прописные и строчные буквенные символы, цифры и специальные символы.

3.2.2.4. Сброс настроек аутентификации для пользователя выполняется командой

system authentication reset <user>

где <user> – имя пользователя.

3.2.2.5. Для установки количества попыток авторизации и времени блокировки/разблокировки пользователя используется команда

system authentication password attempts {<attempts>} [lock-time <lock_val>] [unlock-time <unlock_val>]

где <attempts> – максимальное количество попыток авторизации. Значение «по умолчанию» равно «3»;

<lock_val> – интервал между неудачными попытками ввода пароля, задается в секундах. Может принимать значения от «0» до «365», «по умолчанию» равно «0»;

<unlock_val> – продолжительность блокировки пользователя при превышении попыток авторизации, задается в секундах. Может принимать значения от «0» до «365», «по умолчанию» равно «60».

3.2.2.6. Включение/выключение аутентификации пользователей через radius-сервер выполняется командой

system authentication radius {on | off}

3.2.2.7. Включение/выключение аутентификации пользователей через ldap-сервер выполняется командой

system authentication ldap {on | off}

3.2.2.8. Отображение конфигурации аутентификации пользователя для пользователя или для всех пользователей выполняется командой

show system authentication local [<user>]

3.2.3. Система разграничения доступа

3.2.3.1. Система дискреционного доступа, входящая в состав агента управления, вводит дополнительный функционал по обеспечению разграничения доступа на основе дискреционной модели.

3.2.3.2. Для реализации данного функционала вводится понятие объекта (ресурса) доступа. В Zenator R Rt определен следующий перечень защищаемых информационных ресурсов:

– команды;

– журналы;

– внешние носители информации (USB-накопители);

– профили (текущая конфигурация устройства или сохранённая в файле).

Для каждой команды CLI вводится запись, сопоставляющая имя команды и список ресурсов, к которым команде необходим доступ для успешного выполнения.

3.2.3.3. Для взаимодействия с Zenator R Rt предусмотрено три группы пользователей:

– администраторы сети (АС) (группа «admin»);

– администраторы безопасности (АБ) (группа «admsec»);

– администраторы аудита (АА) (группа «admaud»).

Матрица доступа определяет и разграничивает права АС, АБ и АА, которые представлены в таблице 1.

Таблица 1

Пользователь/функция	АБ	АС	АА	Примечание
Создание, сохранение, применение профиля конфигурации изделия	+	-	-	Согласно ролевой модели в части профилей конфигурации (таблица 2)
Импорт профиля конфигурации с внешнего носителя	+	-	-	
Экспорт профиля конфигурации на внешний носитель	+	-	-	Строго владелец профиля конфигурации
Управление учетными записями пользователей	+	-	-	
Изменение качества паролей, настройка пароля временного действия	+	-	-	
Настройка политики блокировки пользователей при неуспешном использовании механизма аутентификации/идентификации: – время блокировки; – количество неуспешных попыток, после которых пользователь блокируется	+	-	-	
Модификация прав на функционал согласно ролевой модели	+	-	-	Включение/выключение прав «по разрешению»
Настройка физических интерфейсов	+	-	-	
Настройка loopback-интерфейсов	+	-	-	
Настройка работы в режиме сетевого моста	+	-	-	
Настройка конфигурации VLAN в рамках сетевого моста	+	-	-	
Настройка маршрутизации, основанной на политиках маршрутизации	+	-	-	
Настройка трансляции портов и адресов средствами NAT	+	-	-	
Настройка агрегации физических интерфейсов	+	-	-	
Настройка статической, динамической маршрутизации (RIPv2, RIPing, OSPFv2, BGPv4)	+	-	-	
Настройка протоколов VRRP, BFD, LLDP, IGMPv3	+	-	-	

Пользователь/функция	АБ	АС	АА	Примечание
Настройка режима работы изделия в кластере вида «Активный» / «Пассивный»	+	-	-	
Настройка DHCP-сервера	+	-	-	
Настройка DNS-клиента, DNS-proxy	+	-	-	
Настройка конфигурации туннелей IPSec, L2TP, IPIP/GRE, OpenVPN	+	-	-	
Настройка доступа по протоколам SSHv2, Telnet и SNMP	+	-	-	
Конфигурация туннелей PPTP/PPPoE-сервера и PPTP/PPPoE-клиента	+	-	-	
Конфигурация VXLAN-интерфейсов	+	-	-	
Настройка зеркалирования трафика на физические интерфейсы	+	-	-	
Настройка конфигурации доступа с помощью REST API- сервера	+	-	-	
Добавление/удаление доверенных узлов и сетей в части управления изделием	+	-	-	
Настройка скорости физического интерфейса, режима работы (half duplex, full duplex)	+	-	-	
Настройка времени по сетевому протоколу NTP	+	-	-	
Настройка ARP-proxy	+	-	-	
Разделение трафика в соответствии с классом трафика между физическими каналами	+	-	-	
Применение правил фильтрации на основе ACL	+	-	-	
Включение/выключение учета событий, подвергающихся аудиту в: – журнал «auth» (журнал информации о фактах идентификации, аутентификации); – журнал «ipfilter» (журнал событий срабатывания правил межсетевого экранирования); – журнал «commands» (журнал команд администратора, вводимых с консоли управления); – журнал «daemon» (внутренний журнал агента управления); – журнал «testing» (информация о самотестировании системы); – журнал «syslog» (информация от ядра ОС и системных утилит); – журнал «ids» (информация о работе системы обнаружения вторжений);	+	-	-	

Пользователь/функция	АБ	АС	АА	Примечание
– журнал «router» (информация о работе протоколов динамической маршрутизации)				
Включение/выключение выдачи предупреждающих сообщений на консоль управления изделия	+	-	-	
Настройка параметров архивации журналов	+	-	-	
Включение/выключение записи событий, подвергающихся аудиту, на внешний узел по протоколу Syslog, SNMP trap	+	-	-	
Тестирование целостности по запросу, конфигурация расписания самотестирования целостности	+	-	-	
Проведение ручного тестирования: – правил фильтрации; – прохождения сетевых пакетов	+	-	-	
Настройка внутреннего представления времени	+	-	-	
Предоставление технологического доступа к изделию	+	-	-	
Задание политики фильтрации «по умолчанию»	+	-	-	
Выключение/перезагрузка изделия	+	-	-	
Возврат до заводских настроек	+	-	-	
Задание серверов, с которых будет осуществляться загрузка обновлений изделия с последующей их установкой	+	-	-	
Создание шаблонов (списков) правил фильтрации трафика	+	-	-	
Управление Zenator R Rt с помощью: – локального управления; – протоколов Telnet, SSHv2, SNMP и REST API	+	-	-	
Перемаркировка трафика в части: – установки значения поля MSS TCP-пакета; – установки класса обслуживания внутреннего поля «DSCP» и в полях «TOS»	+	-	-	
Мониторинг состояния каналов средствами ICMP	+	-	-	
Настройка числа одновременных подключений с одного IP-адреса	+	-	-	
Выгрузка журналов событий, подвергаемых аудиту, на внешний носитель	+	-	-	
Программное отключение внешнего носителя	+	-	-	
Просмотр информации о текущей загруженности центрального процессора и ОЗУ	+	-	-	

Пользователь/функция	АБ	АС	АА	Примечание
Ведение журнала трафика, проходящего через изделие, на внешнем узле по протоколу IPFIX	+	+	+	
Просмотр настроек в части: – интерфейсов; – статической маршрутизации; – динамической маршрутизации (RIPv2, RIPing, OSPFv2, BGPv4); – приоритизации трафика; – протоколов BFD, LLDP, IKE, IGMPv3	+	-	-	
Просмотр журналов событий: – журнала «auth»; – журнала «ipfilter»; – журнала «commands»; – журнала «daemon»; – журнала «testing»; – журнала «syslog»; – журнала «router»; – журнала «ids»	+	-	-	Просмотр позволяет осуществлять выборку и сортировку данных из журнала
Просмотр настроек изделия в части: – маршрутизации, основанной на политиках; – трансляции адресов; – списков классификации трафика; – перемаркировки трафика	+	-	-	
Просмотр настроек изделия в части: – туннелирования; – фильтрации трафика; – управления изделием; – журналирования; – самотестирования (контроля целостности); – протокола NTP	+	-	-	

3.2.3.4. В таблице 2 представлена ролевая модель доступа к профилям конфигурации.

Таблица 2

Право	Пояснение	Примечание
r	Применение/чтение профиля конфигурации	
w	Модификация сохраненного профиля конфигурации	

Право	Пояснение	Примечание
c	Разрешение смены активного профиля на другой и/или создание нового профиля на основе активного	
o	Владелец профиля может модифицировать права доступа на данный профиль. Право владения профилем конфигурации подразумевает возможность его удаления, а также его сохранения на внешний носитель	Единовременно может существовать только один владелец профиля конфигурации

3.2.3.5. В части конфигурации заводских настроек для АБ разрешен полный доступ ко всем функциям изделия.

3.2.4. Управление пользователями и группами

3.2.4.1. Для взаимодействия с программой предусмотрено три группы пользователей:

– «admin» – администраторы сети;

– «admsec» – администраторы безопасности;

– «admaud» – администраторы аудита.

3.2.4.2. После первоначальной установки существуют следующие учётные записи:

– «admin» – в группе admin;

– «admsec» – в группе admsec;

– «admaud» – в группе admaud.

Для учетных записей «admsec», «admin» и «admaud» изначально установлен пароль «12345678i.» без кавычек.

Указанные выше учетные записи не могут быть удалены.

3.2.4.3. Создание нового пользователя выполняется командой

system user add {admin | admsec | admaud} <name> password <pass> [aging <age_val>]

где <name> – имя нового пользователя. Может принимать значения от «2» до «32»;

<pass> – пароль для нового пользователя. Длина пароля должна быть не меньше минимальной длины пароля, заданной с помощью команды приведенной в 3.2.2.2;

<age_val> – количество дней жизни пароля.

3.2.4.4. Блокировка/разблокировка пользователя выполняется командой

system user {lock | unlock} <name>

где <name> – имя пользователя;

lock – блокировать пользователя;

unlock – разблокировать пользователя.

Примечание. Возможности блокировки пользователя «admsec» не существует.

3.2.4.5. Изменение пароля существующего пользователя выполняется командой

system user edit <name> password <pass> [aging <age_val>]

где <pass> – новый пароль для пользователя. Длина пароля должна быть не меньше минимальной длины пароля, заданной с помощью команды, приведенной в 3.2.2.2.

3.2.4.6. Добавление/удаление почты пользователя выполняется командой

[no] system user mail <name> <email>

где <email> – почта пользователя. Почтовое имя пользователя задается в формате «abc@def.mail».

3.2.4.7. Удаление пользователя выполняется командой

system user del <name>

3.2.4.8. Установка/удаление лимита подключений к системе для пользователя выполняется командой

[no] system user limit <name> <limit>

где <limit> – ограничение одновременного входа пользователей в систему.

3.2.4.9. Просмотр списка пользователей системы, их группы и статус выполняется командой

show system users

3.2.4.10. Примечание. При выводе списка пользователей системы около имени заблокированного пользователя отображается восклицательный знак (например, «(!) user»).

3.2.5. Управление профилями конфигурации

3.2.5.1. Установка доступа/запрета на выполнение команды выполняется командой

grant command access {admin | admsec | admaud} {p | d} <module_name> “<command_name>”

где <module_name> – имя модуля;

<command_name> – имя команды. Необходимо указывать в двойных кавычках.

p – разрешить выполнение команды (permit);

d – запретить выполнение команды (deny).

Примечание. Команда выполняется для групп «admin» и «admaud» при наличии прав на выполнение для конкретной группы пользователей.

3.2.5.2. Регистрация нового пустого профиля выполняется командой

register profile <profile_name>

где <profile_name> – имя профиля.

Примечание. Для регистрации профиля команда «commit» не требуется.

3.2.5.3. Назначение права доступа к профилю для группы пользователей выполняется командой

grant profile access {admin | admsec | admaud} [rwco] <profile_name>

где параметры <r>, <w>, <c>, <o>:

– <r> – применение/чтение профиля конфигурации;

– <w> – модификация сохраненного профиля конфигурации;

– <c> – смена активного профиля и/или создание нового профиля на основе активного;

– <o> – владелец профиля может модифицировать права доступа на данный профиль;

<profile-name> – имя профиля.

Право владения профилем конфигурации подразумевает возможность его удаления, а также его сохранения на внешний носитель. Возможно присвоение прав владельца нескольким группам пользователей.

3.2.5.4. Назначение прав доступа на произведение действий над журналами для группы пользователей выполняется командой

grant log access {admin | admsec | admaud} [rw] {syslog | auth | commands | daemon | ipfilter | testing | router | ids}

где параметры <r>, <w>:

– <r> – чтение;

– <w> – запись на внешний носитель.

3.2.5.5. Удаление из списка ранее зарегистрированного профиля выполняется командой

unregister profile <profile_name>

3.2.5.6. Регистрация внешнего носителя системы выполняется командой

register flash

3.2.5.7. Удаление внешнего носителя из списка зарегистрированных в системе устройств выполняется командой

unregister flash <num>

где <num> – номер внешнего носителя.

3.2.5.8. Монтирование USB-накопителя в систему выполняется командой

system mount flash

3.2.5.9. Отмонтирование USB-накопителя от устройства выполняется командой

system umount flash

Примечание: Последовательность работы с flash-накопителем выглядит следующим образом:

register flash

system mount flash

system umount flash

unregister flash <number>

3.2.5.10. Сохранение профиля с конфигурацией в системе выполняется командой

save profile <profile_name>

Примечания:

1. Для сохранения профиля его следует сначала зарегистрировать.

2. При сохранении профиля команда «commit» не требуется.

3.2.5.11. Сохранение профиля конфигурации на первый примонтированный USB-накопитель выполняется командой

save profile <profile_name> flash

3.2.5.12. Загрузка профиля с базовой конфигурацией выполняется командой

load profile <profile_name>

Примечания:

1. Перед загрузкой нового профиля удаляются все настройки текущего профиля.

2. Загрузка профиля группы пользователей с разрешением доступа только на чтение и модификацию (параметры «rw» заданные в соответствии с 3.2.5.3) делает недоступным загрузку других профилей.

3.2.5.13. Загрузка профиля конфигурации в систему с первого примонтированного USB-накопителя выполняется командой

load profile <profile_name> flash

Примечание. Для применения профиля необходимо его зарегистрировать в системе в соответствии с 3.2.5.2 и загрузить в соответствии с 3.2.5.12.

3.2.5.14. Сброс настроек конфигурации программного обеспечения к заводской базовой конфигурации выполняется командой

load profile null

Примечания:

1. При выполнении этой команды будут удалены все несохраненные настройки.
2. После выполнения команды, сохраненные ранее профили остаются в системе.
3. После выполнения команды происходит автоматичиский вход под пользователем, выполнившим команду.

3.2.5.15. Установка профиля как загружаемого при старте системы выполняется командой

set running-profile <config_name>

где <config_name> – имя профиля.

3.2.5.16. Вывод текущих настроек прав доступа к команде выполняется командой

show command access <module_name> “<command_name>”

где <module_name> – имя модуля;

<command_name> – имя команды. Необходимо указывать в двойных кавычках.

3.2.5.17. Вывод текущих настроек прав доступа к журналам выполняется командой

show log access {syslog | auth | commands | daemon | ipfilter | testing | router | ids}

3.2.5.18. Вывод списка команд, которые доступны данной группе пользователей, выполняется командой

show group access {admin | admsec | admaud}

Примечания:

1. Для перехода в конец списка команд необходимо нажать сочетание клавиш «Shift+G».
2. Для выхода из списка команд необходимо нажать сочетание клавиш «Shift+Q».

3.2.5.19. Вывод текущих настроек прав доступа для профиля выполняется командой

show profile access <profile_name>

3.2.5.20. Вывод списка всех зарегистрированных профилей конфигурации, а также информации, какой профиль активный, а какой загружается при старте системы, выполняется командой

show profiles

3.2.5.21. Вывод конфигурации профиля выполняется командой

show profiles [<profiles_name>]

3.2.5.22. Вывод списка зарегистрированных в системе внешних носителей выполняется командой

show flash

3.2.5.23. Вывод текущей конфигурации системы или конкретного модуля выполняется командой

show running-profile [<module_name>]

1. Для выхода из файла текущей кофигурации необходимо нажать комбинации клавиш «Shift+Q».

2. При нажатии комбинации клавиш «Shift+?», после ввода команды «show running-profile», на экран будет выведен список всех модулей системы, для которых выполняется данная команда.

3.2.6. Управление интерфейсами

3.2.6.1. Вход в режим конфигурации интерфейса выполняется командой

interface <iface_name>

где <iface_name> – имя интерфейса.

3.2.6.2. Вывод конфигурации всех интерфейсов или определенного интерфейса выполняется командой

show interfaces [detail] [serial | <iface_name>] [statistics]

где serial – отображение информации о последовательных интерфейсах;

detail – отображение расширенных настроек конкретного интерфейса или всех интерфейсов;

statistics – отображение статистики.

3.2.6.3. Установка/удаление IP-адреса интерфейса выполняется командой

[no] ip-address <ip_addr/mask>

где <ip_addr/mask> – IP-адрес/маска подсети интерфейса.

Примечание. Одному интерфейсу можно назначить больше одного IP-адреса.

3.2.6.4. Выключение/включение интерфейса выполняется командой

[no] shutdown

3.2.6.5. Выход из режима конфигурации физического интерфейса выполняется командой

exit

3.2.7. Команды просмотра и управления журналами

3.2.7.1. Вывод журнала выполняется командой

show log {syslog | auth | commands | daemon | ipfilter | testing | router | ids}

[search [after <start_date> <start_time>] | [before <end_date> <end_time>]] | [sender <name_sender>] | [success {OK | FAIL}] | [action <action>] | [level <level>] | [module <name_module>] | [text <text>] [limit <limit>] [tail <count_tail>]

где <start_date> – начальная дата интервала поиска в формате «yyyy-mm-dd»;

<end_date> –конечная дата интервала поиска в формате «yyyy-mm-dd»;

<start_time> – начальное время интервала поиска в формате «hh:mm:ss» или «hh:mm»;

<end_time> – конечное время интервала поиска в формате «hh:mm:ss» или «hh:mm»;

<name_sender> – имя отпровителя;

success – сортировка по успешности действия. Параметр может принимать значения «OK» или «FAIL»;

<action> – действие. Поиск вхождения указанной подстроки;

<level> – уровень записи в журнал;

<name_module> – имя модуля поиска, на основании действий которого была создана запись в журнале;

<text> – текстовая строка;

<limit> – максимальное число записей, которое необходимо вывести;

<count_tail> – количество строк с конца файла.

Примечания:

1. Доступны следующие журналы для регистрации событий:

– «syslog» – журнал системных команд;

– «auth» – журнал событий аутентификации;

– «commands» – журнал команд пользователя;

– «daemon» – журнал выполненных функций;

– «ipfilter» – журнал событий срабатывания правил межсетевого экранирования;

– «testing» – журнал тестирования и самотестирования системы;

– «router» – журнал, содержащий информацию о работе протоколов динамической маршрутизации;

– «ids» – журнал системы обнаружения вторжений.

2. Параметр «start_date» должен быть меньше или равен «end_date». Параметр «start_time» должен быть меньше или равен «end_time».

3. Параметр «level» может принимать следующие значения:

– debug – отладочная информация;

– info – информационные сообщения;

– warning – предупреждения;

– error – сообщения об ошибках;

– critical – критические ошибки в программе.

4. Для перехода в конец файла (при выводе журналов или другой информации) необходимо нажать сочетание клавиш «Shift + G».

5. Для выхода из файла, необходимо нажать сочетание клавиш «Shift + Q».

3.2.7.2. Просмотр журнала системных сообщений при загрузке изделия и в процессе его работы выполняется командой

show log syslog

3.2.7.3. Выгрузка журнала на внешний носитель выполняется командой

save log {syslog | auth | commands | daemon | ipfilter | testing | router | ids} flash [clear]

где clear – очистить журнал после копирования на внешний носитель.

3.2.8. Настройка возможностей удаленного конфигурирования

3.2.8.1. Включение/выключение возможности удаленного конфигурирования Zenator R Rt с помощью протокола SSH выполняется командой

system ssh {on | off}

«По умолчанию» протокол SSH включен.

3.2.8.2. Задание порта подключения для протокола SSH выполняется командой

ssh port <number>

где <number> – номер порта для подключения. Может принимать значения от «0» до «65535». Значение «по умолчанию» равно «22».

3.2.8.3. Установка/удаление режима разрешения доступа по SSH-протоколу определенным хостам или пользователям выполняется командой

[no] ssh {allow | deny} [user <user_name>] [host <ip_pattern>]

где <user_name> – имя пользователя;

<ip_pattern> – IP-адрес хоста;

allow – установка режима разрешения указанным пользователям доступ по SSH;

deny – установка режима запрета указанным пользователям доступ по SSH.

3.2.8.4. Вывод состояния протокола SSH выполняется командой

show ssh

3.2.8.5. Включение/выключение возможности удаленного конфигурирования Zenator R Rt с помощью протокола Telnet выполняется командой

system telnet {on | off}

«По умолчанию» протокол Telnet включен.

3.2.8.6. Задание порта подключения для протокола Telnet выполняется командой

telnet port <number>

где <number> – номер порта для подключения. Может принимать значения от «0» до «65535». Значение «по умолчанию» равно «23».

3.2.8.7. Вывод состояния протокола Telnet выполняется командой

show telnet

3.2.9. Система обнаружения вторжений

3.2.9.1. Включение/отключение интерфейса IDS выполняется командой

system ids {on | off}

3.2.9.2. Установка/удаление интерфейса проброса пакетов выполняется командой

[no] ids mode {transparent | bridge | router} [interface <iface_value> <copy_slot>] [queue-num <queue_num_val>]

где <copy_slot> –интерфейс проброса пакетов;

<iface_value> – имя интерфейса;

transparent – прозрачный режим;

bridge – режим сетевого моста (IDS);

router – режим роутера (IPS);

<queue_num_val> – номер очереди.

Примечание. Параметр «queue-num» задается при включенном режиме роутера, при этом значение номера очереди <queue_num_val> должно соответствовать номеру очереди, задаваемому при добавлении правила фильтрации.

3.2.9.3. Установка/удаление внутренней сети для режима IDS выполняется командой

[no] ids home-net {any | <network>}

где <network> – IP-адрес сети.

3.2.9.4. Включение/отключение правила выполняется командой

ids rule <rule_num> {enable | disable}

где <rule_num> – номер правила.

3.2.9.5. Сохранение IDS-правил на USB-накопитель выполняется командой

save ids-rules flash

Примечание. IDS-правила сохраняются на USB-накопитель в архивированном виде в файл формата «ids_rules_backup.tar».

3.2.9.6. Загрузка правил с USB-накопителя для режима IDS выполняется командой

load ids-rules flash <file_name>

где <file_name> – имя файла. Доступные следующие расширения для имен файлов «.tar», «.tar.gz», «.tgz», «.tar.gzip», «.tar.bz2», «.tbz2», «.tbz,» «.tar.xz», «.txz», «.tar.zst», «.tzst».

ВНИМАНИЕ! Данный механизм полностью перезапишет каталог с правилами.

3.2.9.7. Восстановление правил IDS выполняется командой

ids restore-rules

3.2.9.8. Задание уровня эврестического анализа выполняется командой

ids sense-level <low | medium | high>

3.2.9.9. Вывод конфигурации IDS выполняется командой

show ids

3.2.9.10. Вывод списка правил IDS выполняется командой

show ids rules

3.2.10. Обновление программного обеспечения

3.2.10.1. Задание/добавление адреса доверенного сервера обновлений выполняется командой

system update-server <address> [cert <cert_file> <key_file>]

где <address> – адрес сервера обновлений.

Требования к формату задаваемого адреса:

– протокол передачи данных – «http», «ftp» (например, «http://example.spb.ru», «ftp://10.10.10.1»);

– может записываться с префиксом или без него (например, «http://www.example.spb.ru» или «http://example.spb.ru»);

– разрешен ввод адреса доменного имени сервера до третьего уровня (например, «http://www.example.spb.ru»);

– разрешено задание сервера в виде IP-адреса для протокола «http» (например, «http://10.10.10.1»);

– при обновлении с USB-накопителя – «file:///<path>», где <path> – адрес до директории, в которой примонтирован USB-накопитель (например, «mnt/usb»).

Перед указанием адреса, USB-накопитель должен быть примонтирован и зарегистрирован в системе;

<cert_file> – имя файла, содержащего сертификат клиента;

<key_file> – имя файла, содержащего ключ сертификата.

3.2.10.2. Вывод адреса сервера обновлений выполняется командой

show system update-server

3.2.10.3. Получение списка обновлений Zenator R Rt выполняется командой

system update

3.2.10.4. Обновление общесистемного ПО выполняется командой

system upgrade

3.2.10.5. Откат ПО до предыдущей версии выполняется командой

system rollback

3.2.11. Системные команды

3.2.11.1. Системные команды управления пользователями и группами приведены в 3.2.4.

3.2.11.2. Администрирование системных модулей выполняется командой

system modules <name> {on | off | reload}

где <name> – название модуля;

on – включение модуля;

off – выключение модуля;

reload – перезагрузка модуля.

3.2.11.3. Просмотр списка модулей, находящихся в системе, выполняется командой

show system modules

3.2.11.4. Задание имени текущего устройства ввода-вывода выполняется командой

system console <tty_port>

где <tty_port> – имя текущего устройства ввода-вывода.

3.2.11.5. Создание/удаление учетной записи пользователя службы поддержки выполняется командой

[no] system maintenance-access

3.2.11.6. Редактирование имени хоста системы выполняется командой

set system hostname <system_name>

где <system_name> – имя хоста системы.

3.2.11.7. Задание/удаление почтового имени «по умолчанию» выполняется командой

[no] set system mailname <mailname>

где <mailname> – почтовое имя. Почтовое имя задается в формате «abc@def.mail».

3.2.11.8. Перезагрузка системы без сохранения конфигурации (загружается профиль «null») выполняется командой

system reboot

3.2.11.9. Выключение системы выполняется командой

system shutdown

3.2.11.10. Включение/отключение программного интерфейса приложения (API) выполняется командой

system api {on | off | certificate <file_name>}

где <file_name> – имя файла сертификата.

3.2.11.11. Включение/выключение IDS выполняется командой

system ids {on | off}

3.2.11.12. Включение/выключение LLDP выполняется командой

system lldp {on | off}

3.2.11.13. Проверка доступности удаленного узла с помощью ICMP-запросов выполняется командой

ping <addr> [source {iface <iface_name> | addr <ip_addr>}] [size <size>] [interval <interval>] [count <count>] [timeout <timeout>] [tos <tos>],

где <addr> – IP-адрес удаленного узла;

<iface_name> – имя интерфейса;

<size> – размер пакета. Значение задается в байтах;

<interval> – временной интервал работы команды, задается в секундах. Значение «по умолчанию» равно «1»;

<count> – количество генерируемых ICMP-запросов;

<timeout> – значение интервала в секундах;

<tos> – значение ToS.

Примечание. Прервать выполнение команды можно с помощью клавиши «Enter».

3.2.11.14. Захват и проверка сетевого трафика на интерфейсе выполняется командой

tcpdump <iface_name>

где <iface_name> – имя интерфейса.

3.2.11.15. Сканирование сети выполняется командой

nmap <host_port>

где <host_port> – адрес хоста и порт.

3.2.11.16. Загрузка/сохранение сертификата SSL выполняется командой

{load | save} certificate flash <file_name>

где <file_name> – имя файла сертификата.

3.2.11.17. Удаление сертификата SSL выполняется командой

delete certificate {all | <file_name>}

3.2.11.18. Сохранение системных неизменяемых файлов на флеш-носитель выполняется командой

save backup flash

3.2.11.19. Разрешение доменного имени выполняется командой

domain lookup <name>

где <name> – имя сервера.

3.2.11.20. Вывод информации сертификатов SSL выполняется командой

show certificate <file_name>

где <file_name> – имя файла CA-сертификата.

3.2.11.21. Вывод информации о загруженности центрального процессора выполняется командой

show system cpu-load interval <interv>

где <interv> – время, задается в секундах.

3.2.11.22. Вывод почтового имени, заданного «по умолчанию», выполняется командой

show system mailname

3.2.11.23. Вывод имени системы выполняется командой

show system hostname

3.2.11.24. Вывод информации о загруженности оперативного запоминающего устройства выполняется командой

show system memory-load

3.2.11.25. Вывод названия программного обеспечения Zenator R Rt и его версии выполняется командой

show version

3.2.11.26. Вывод номера сборки программного обеспечения Zenator R Rt выполняется командой

show version build zenator

3.2.11.27. Вывод версии пакета программного обеспечения Zenator R Rt выполняется командой

show version build <имя пакета>

3.2.11.28. Вывод номера сборки пакета системы обнаружения вторжений выполняется командой

show version build snort-rules-default

3.2.11.29. Вывод имени текущего устройства ввода-вывода выполняется командой

show system console

3.2.11.30. Вывод состояния сервиса API выполняется командой

show system api

3.2.12. Контроль целостности

3.2.12.1. Программа имеет систему контроля целостности, обеспечивающую обслуживание двух типов объектов:

– постоянно неизменяемые;

– транзакционно-изменяемые.

К первому типу относятся системные файлы, исполняемые файлы сервисов, предоставляемых изделию.

Транзакционно-изменяемыми являются журналы и файлы конфигурации изделия.

3.2.12.2. При установке программы создаются таблицы контрольных сумм для каждого из типов объектов. Сами таблицы также подлежат контролю целостности.

Программа производит автоматическую проверку целостности транзакционно-изменяемых объектов.

Программа производит проверку целостности неизменяемых объектов при старте системы.

3.2.12.3. Принудительная проверка целостности всех журналов выполняется командой

check integrity logs

3.2.12.4. Принудительная проверка целостности журнала выполняется командой

check integrity log {syslog | auth | commands | daemon | ipfilter | testing | router | ids}

3.2.12.5. Задание принудительной проверки всех изменяемых конфигурационных файлов изделия выполняется командой

check integrity configs

3.2.12.6. Задание принудительной проверки всех неизменяемых конфигурационных файлов изделия выполняется командой

check integrity system

3.2.12.7. Задание интервала проверки контроля целостности выполняется командой

check integrity interval <interval_val>

где <interval_val> – значение интервала проверки контроля целостности, задается в секундах. Может принимать значения от «180» до «7200». «По умолчанию» проверка целостности выполняется каждые 30 мин.

3.2.12.8. Отображение параметров контроля целостности выполняется командой

show system check-integrity interval

3.2.13. Тестирование

3.2.13.1. Тестирование выполняется с помощью команды

test [<test_name>]

где <test_name> – имя теста.

Параметр может принимать следующие значения:

– «acl» – тест функций фильтрации и логирования;

– «static_routes» – тест функций создания статистических маршрутов;

– «bridge» – тест функций создания сетевых мостов;

– «loopback» – тест функций loopback.

3.2.13.2. Вывод списка тестов или содержание теста выполняется командой *show tests [<test_name>]*

3.2.14. Доступ с помощью REST API

3.2.14.1. В Zenator R Rt реализован REST API - прикладной программный интерфейс, который использует HTTP-запросы для получения, извлечения, размещения и удаления данных.

Аббревиатура REST в контексте API расшифровывается как «передача состояния представления».

3.2.14.2. Подробное описание применения и настройки доступа к интерфейсу REST API приведено в приложении к данному руководству ИСКП.30334-01 34 01-1.

3.2.15. Технологический доступ

3.2.15.1. Технологический доступ предназначен для прямого доступа к средствам ПО и используется службой технической поддержки для решения задач, недоступных штатными средствами.

3.2.15.2. Технологический доступ осуществляется локально или через сетевое подключение по протоколам SSH или Telnet при помощи двойной авторизации. На первом этапе сотрудником технической поддержки осуществляется ввод имени пользователя и пароля одноразовой учетной записи. На втором этапе производится авторизованное технологическое подключение.

Примечание. Для протоколов SSH и Telnet требуется предварительное включение с помощью команд «system ssh on» или «system telnet on».

3.2.15.3. Для создания одноразовой учетной записи служит команда «maintenance_access», выполняемая АБ изделия. В результате ее выполнения будет получено имя пользователя и пароль, которые необходимо сообщить при обращении в службу технической поддержки.

4. СООБЩЕНИЯ ОПЕРАТОРУ

4.1. Действия оператора должны осуществляться в соответствии с подсказками, выдаваемыми на экран монитора в процессе функционирования Zenator R Rt.

4.2. Сообщения, выдаваемые программой оператору, могут быть двух типов:

– сообщения, отображаемые после применения изменений командой «commit»;

– сообщения, отображаемые после выполнения команды.

4.3. Все сообщения приведены в приложении к данному руководству ИСКП.30334-01 34 01-1.

Перечень принятых сокращений

АА	– администратор аудита
АБ	– администратор безопасности
АП	– аппаратная платформа
АС	– администратор сети
ОС	– операционная система
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина
API	– Application Programming Interface (программный интерфейс приложения)
ARP	– Address Resolution Protocol (протокол разрешения адресов)
BGP	– Border Gateway Protocol (пограничный межсетевой протокол)
CLI	– Command Line Interface (интерфейс командной строки)
DAT	– Dynamic Address Translation (динамическое преобразование адресов)
DHCP	– Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)
DMZ	– демилитаризованная зона
DNS	– Domain Name System (система доменных имен)
GRE	– Generic Routing Encapsulation («общая инкапсуляция маршрутов» – протокол туннелирования сетевых пакетов)
IEEE	– Institute of Electrical and Electronics Engineers (Институт Инженеров Электротехники и Электроники)
ICMP	– Internet Control Message Protocol (протокол межсетевых управляющих сообщений)
IGMP	– Internet Group Management Protocol (протокол управления групповой передачей данных)
IGP	– Interior Gateway Protocol (протокол внутренних маршрутизаторов)
IPFIX	– Internet Protocol Flow Information Export (протокол экспорта информации по IP-потоку)
IPIP	– IP over IP («IP поверх IP» – протокол туннелирования)
LLDP	– Link Layer Discovery Protocol (протокол оповещения канального уровня)

MSS – Maximum Segment Size (максимальный размер полезного блока данных)

MTU – Maximum Transmission Unit (максимальный размер полезного блока данных)

NAPT – Network Address Port Translation (преобразование сетевых адресов и портов)

NAT – Network Address Translation (преобразование сетевых адресов)

NDP – Neighbor Discovery Protocol (протокол обнаружения соседей)

NTP – Network Time Protocol (протокол передачи точного времени)

OSPF – Open Shortest Path First (протокол динамической маршрутизации)

PAT – Port Address Translation (технология трансляции сетевого адреса в зависимости от TCP/UDP-порта получателя)

PPP – Point-to-Point Protocol (туннельный протокол типа «точка-точка»)

PPPoE – Point-to-Point Protocol Over Ethernet (сетевой протокол канального уровня передачи кадров PPP через Ethernet)

PPTP – Point-to-Point Tunneling Protocol (туннельный протокол типа «точка-точка» в стандартной, незащищенной сети)

RADIUS – Remote Authentication in Dial-In User Service (протокол аутентификации, авторизации, сбора сведений об использованных ресурсах)

REST API – прикладной программный интерфейс передачи состояния представления

RIP – Routing Information Protocol (протокол маршрутизации)

RIPng – Routing Information Protocol Next Generation (протокол маршрутизации для IPv6)

SNAT – Static Network Address Translation (статический NAT)

SNMP – Simple Network Management Protocol (простой протокол сетевого управления)

SSH – Secure Shell (сетевой протокол прикладного уровня)

VLAN – Virtual Local Area Network (виртуальная локальная сеть)

VPN – Virtual Private Network (виртуальная частная сеть)

VRRP – Virtual Router Redundancy Protocol (сетевой протокол, объединяющий группу маршрутизаторов в один виртуальный маршрутизатор)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	Номер документа	Входящий номер сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					