Сервисные маршрутизаторы серии ESR

ESR-10, ESR-12V, ESR-12VF, ESR-15, ESR-15R, ESR-15VF, ESR-20, ESR-21, ESR-30, ESR-31, ESR-100, ESR-200, ESR-1000, ESR-1200, ESR-1500, ESR-1511, ESR-1511 rev.B, ESR-1700, ESR-3100, ESR-3150, ESR-3200, ESR-3200L, ESR-3250, ESR-3300, ESR-3350

Руководство по сообщениям Syslog

Версия ПО 1.46

Содержание

1 Аннотация 4
2 Описание сообщений Syslog 5
1. Описание сообщений AAA 5
1.1 Лог успешного входа в систему 5
1.2 Неудачная попытка входа в систему 5
1.3 Неверный пароль пользователя 5
1.4 Попытка войти с использованием неизвестного имени пользователя 6
1.5 Завершение сессии 6
1.6 Добавление нового пользователя 6
1.7 Удаление пользователя 7
1.8 Изменение привилегий для пользователя 7
1.9 Изменение пароля для пользователя 7
1.10 Изменение срока действия пароля пользователя 7
1.11 Особые логи при работе с пользователем по SSH 8
1.12 Особые логи при работе при повышении привилегий пользователя в CLI 9
2. Изменение состояния системы 10
2.1 Перезагрузка устройства 10
2.2 Выключение устройства (применимо только для vESR) 10
2.3 Перезагрузка устройства по иным причинам 10
2.4 Изменение даты на устройстве 11
2.5 Применение изменения конфигурации устройства (commit) 11
2.6 Конфигурация успешно применена (после ввода commit) 11
2.7 Подтверждение изменения конфигурации устройства (confirm) 11
2.8 Установка таймера подтверждения изменения конфигурации 12
2.9 Истечение таймера подтверждения изменения конфигурации 12
2.10 Ввод команды 12
2.11 Ошибки применения конфигурации на старте 13
3. Работа с файлами 15
3.1 Начало операции 15
3.2 Статус операции 16
4. События firewall 17
4.1 Защита от DoS / DDoS 17
4.2 Срабатывания zone-based firewall 17
4.3 Срабатывания HTTP(s) proxy 18
4.4 Срабатывания NAT-трансляции 19

4.5 Срабатывания ARP inspection 19
4.6 Срабатывания BGP FlowSpec 20
5. События системы обнаружения (предотвращения) вторжений 20
5.1 Срабатывание правила (сигнатуры) 20
5.2 Загрузка нового (или первого) списка правил в IPS 21
5.3 Начало применения нового списка правил 21
5.4 Успешное применение нового списка правил 22
5.5 Успешный запуск IPS 22
6. Описание событий системы защиты от атак перебором (auth-guard) 22
6.1 Блокировка источника 22
6.2 Автоматическая разблокировка по истечении срока бана 23
6.3 Ручная разблокировка пользователем 23

1 Аннотация

В данном руководстве приведены возможные сообщения, генерируемые модулем Syslog, для маршрутизаторов серии ESR с указанием возможных параметров сообщений и причин возникновения.

Логи на маршрутизаторах ESR оформлены по RFC 5424 с соблюдением всех обязательных полей.

В общем виде шаблон для логов на удалённый сервер выглядит следующим образом:

<$PRI>1 $ISODATE $HOSTNAME $APP_NAME - - - $SEQNUM: $MSG

В общем виде шаблон для логов для вывода в консоль (console, ssh, telnet) или локальный файл выглядит следующим образом:

$SEQNUM: $ISODATE $APP_NAME $MSG

Часть указанных полей не является обязательной и включается в режиме конфигурирования.

Имя приложения (APP-NAME) может быть указано при указании соответствующей настройки на устройстве (**syslog program-name**) (для логов на удалённый сервер имя приложения формируется безусловно, настройка влияет на отображение логов в консоли или сохранении в локальных файлах).

Порядковый номер сообщения (SEQNUM) подсистемы может быть указан при указании соответствующей настройки на устройстве (**syslog sequence-numbers**). Это строка вида «*%d: »*, в начале сообщения (при выводе в консоль или файл) либо перед полем MSG (при отправке сообщения на удаленный сервер).

Время может быть указано с точностью до миллисекунды (TIME-SECFRAC) при наличии соответствующей настройки на устройстве (**syslog timestamp msec**).

Ниже приведен пример полного вида лога, отправляемого на удаленный сервер, на примере логов аутентификации пользователя:

<86>1 2024-10-16T10:16:27+00:00 vesr login - - - 1: %AAA-LOCAL-I-SESSION: console: session opened for user admin

<86>1 2024-10-16T10:16:29+00:00 vesr login - - - 2: %AAA-LOCAL-I-SESSION: console: session closed for user admin

В документе используется формат представления лога без служебной информации – только MSG.

2 Описание сообщений Syslog

1. Описание сообщений AAA

1.1 Лог успешного входа в систему

Пример:

%AAA-LOCAL-I-SESSION: console: session opened for user testusername

Паттерн:

%AAA-LOCAL-I-SESSION: %s1: session opened for user %s2

Параметры:

%s1 — источник: sudo | console | ssh | telnet

%s2 — имя пользователя

1.2 Неудачная попытка входа в систему

Пример:

%AAA-W-CONSOLE: authenticate failed: Permission denied

Паттерн:

%AAA-W-CONSOLE: authenticate failed: Permission denied

Параметры:

Отсутствуют

1.3 Неверный пароль пользователя

Пример:

%AAA-F-FAILED: Incorrect password for user 'testusername' tty=console rhost=0.0.0.0

Паттерн:

%AAA-F-FAILED: Incorrect password for user '%s1' tty=%s2 rhost=%s3

Параметры:

%s1 — имя пользователя

%s2 — источник: sudo | console | ssh | telnet

%s3 — адрес удалённого хоста (0.0.0.0 для локальной аутентификации)

1.4 Попытка войти с использованием неизвестного имени пользователя

Пример:

%AAA-F-FAILED: Unknown user 'testusername' tty=console rhost=0.0.0.0

Паттерн:

%AAA-F-FAILED: Unknown user %s1' tty=%s2 rhost=%s3

Параметры:

%s1 — имя пользователя

%s2 — источник: sudo | console | ssh | telnet

%s3 — адрес удалённого хоста (0.0.0.0 для локальной аутентификации)

1.5 Завершение сессии

Пример:

%AAA-LOCAL-I-SESSION: console: session closed for user testusername

Паттерн:

%AAA-LOCAL-I-SESSION: %s1: session closed for user %s2

Параметры:

%s1 — источник: sudo | console | ssh | telnet

%s2 — имя пользователя

1.6 Добавление нового пользователя

Пример:

%USER-I-ADD: User testusername was created

Паттерн:

%USER-I-ADD: User %s was created

Параметры:

%s — имя пользователя

1.7 Удаление пользователя

Пример:

%USER-I-ADD: User testusername was removed

Паттерн:

%USER-I-ADD: User %s was removed

Параметры:

%s — имя пользователя

1.8 Изменение привилегий для пользователя

Пример:

%USER-I-INFO: Privilege level of user testusername was changed from 5 to 14

Паттерн:

%USER-I-INFO: Privilege level of user %s was changed from %d1 to %d2

Параметры:

%s — имя пользователя

%d1 — уровень привилегий до изменений

%d2 — уровень привилегий после изменений

1.9 Изменение пароля для пользователя

Пример:

%USER-I-INFO: Password of user testusername was changed

Паттерн:

%USER-I-INFO: Password of user %s was changed

Параметры:

%s — имя пользователя

1.10 Изменение срока действия пароля пользователя

Пример:

%USER-I-INFO: changed password expiry for testusername

Паттерн:

%USER-I-INFO: changed password expiry for %s

Параметры:

%s — имя пользователя

1.11 Особые логи при работе с пользователем по SSH

1.11.1 Успешная аутентификация по SSH

Пример:

%AAA-I-SSH: Accepted password for testusername from 10.0.0.1 port 54560 ssh2

Паттерн:

%AAA-I-SSH: Accepted password for %s1 from %s2 port %d %s3

Параметры:

%s1 — имя пользователя

%s2 — адрес, с которого происходит подключение

%d — порт, с которого происходит подключение

%s3 — протокол (ssh2)

1.11.2 Неуспешная аутентификация по SSH

Пример:

%AAA-I-SSH: Failed password for testusername from 10.0.0.1 port 54560 ssh2

Паттерн:

%AAA-I-SSH: Failed password for %s1 from %s2 port %d %s3

Параметры:

%s1 — имя пользователя

%s2 — адрес, с которого происходит подключение

%d — порт, с которого происходит подключение

%s3 — протокол (ssh2)

1.12 Особые логи при работе при повышении привилегий пользователя в CLI

1.12.1 Изменение пароля функционала повышения привилегий

Пример:

%USER-I-INFO: password for '$enab15$' changed by 'testusername'

Паттерн:

%USER-I-INFO: password for '$enab%d$' changed by '%s'

Параметры:

%d — изменённый уровень привилегий

%s — имя пользователя

2. Изменение состояния системы

2.1 Перезагрузка устройства

Пример:

%SYS-C-REBOOT: CLI: System reboot initiated by user testusername from console at 2037-08-23 09:47:49

Паттерн:

%SYS-C-REBOOT: CLI: System reboot initiated by user %s1 from %s2 at %Y-%B-%d %H:%M:%S

Параметры:

%s1 — имя пользователя

%s2 — источник: console | ssh | telnet

%Y-%B-%d %H:%M:%S — формат времени

2.2 Выключение устройства (применимо только для vESR)

Пример:

%SYS-C-REBOOT: CLI: System shutdown initiated by user testusername from console at 2037-08-23 09:47:49

Паттерн:

%SYS-C-REBOOT: CLI: System shutdown initiated by user %s1 from %s2 at %Y-%B-%d %H:%M:%S

Параметры:

%s1 — имя пользователя

%s2 — источник: console | ssh | telnet

%Y-%B-%d %H:%M:%S — формат времени

2.3 Перезагрузка устройства по иным причинам

Пример:

%SYS-C-REBOOT: Top-mgr: Service 'Cfgsync-mgr' stopped responding

Паттерн:

%SYS-C-REBOOT: %s

Параметры:

%s — причина перезагрузки устройства

2.4 Изменение даты на устройстве

Пример:

%TIME-I-INFO: System time was changed by user testusername

Паттерн:

%TIME-I-INFO: System time was changed by user %s

Параметры:

%s — имя пользователя

2.5 Применение изменения конфигурации устройства (commit)

Пример:

%CLI-I-CRIT: user testusername from console input: commit

Паттерн:

%CLI-I-CRIT: user %s from console input: commit

Параметры:

%s — имя пользователя

2.6 Конфигурация успешно применена (после ввода commit)

Пример:

%SYS-W-EVENT: Configuration is applied

Паттерн:

%SYS-W-EVENT: Configuration is applied

Параметры:

Отсутствуют

2.7 Подтверждение изменения конфигурации устройства (confirm)

Пример:

%CLI-I-CRIT: user testusername from console input: confirm

Паттерн:

%CLI-I-CRIT: user %s from console input: confirm

Параметры:

%s — имя пользователя

2.8 Установка таймера подтверждения изменения конфигурации

Пример:

%SYS-W-EVENT: board commit confirmation timer expires in 600 seconds

Паттерн:

%SYS-W-EVENT: board commit confirmation timer expires in %d seconds

Параметры:

%d — количество секунд

2.9 Истечение таймера подтверждения изменения конфигурации

Пример:

%SYS-W-EVENT: board commit confirmation timer expired, configuration has been reverted

Паттерн:

%SYS-W-EVENT: board commit confirmation timer expired, configuration has been reverted

Параметры:

Отсутствуют

2.10 Ввод команды

Пример:

%CLI-I-CMD: user testusername from console input: configure

Паттерн:

%CLI-I-CMD: user %s1 from console input: %s2

Параметры:

%s1 — имя пользователя

%s2 — вводимая команда

2.11 Ошибки применения конфигурации на старте

Для всех подобных ошибок нет специального паттерна, ошибки не имеют параметров.

2.11.1 Ошибка при загрузке по Zero Touch Provisioning — ошибка конфигурации

Пример:

*%SYS-W-EVENT: !!! ********** !!!*

%SYS-W-EVENT: !!! Configuration was loaded with errors, check error messages !!!

%SYS-W-EVENT: !!! Try preparing to restart ZTP !!!

*%SYS-W-EVENT: !!! ********** !!!*

2.11.2 Ошибка при загрузке на предыдущей конфигурации — ошибка конфигурации

Пример:

*%SYS-W-EVENT: !!! ********** !!!*

%SYS-W-EVENT: !!! Configuration was loaded with errors, check error messages !!!

%SYS-W-EVENT: !!! Start with default configuration !!!

*%SYS-W-EVENT: !!! ********** !!!*

2.11.3 Ошибка при загрузке на предыдущей конфигурации для Active-ноды кластера — ошибка конфигурации

Пример:

*%SYS-W-EVENT: !!! ********** !!!*

%SYS-W-EVENT: !!! Cluster master configuration was loaded with errors !!!

%SYS-W-EVENT: !!! Check error messages !!!

%SYS-W-EVENT: !!! Start with default configuration !!!

*%SYS-W-EVENT: !!! ********** !!!*

2.11.4 Ошибка при загрузке на предыдущей конфигурации для Standby-ноды кластера — ошибка конфигурации

Пример:

*%SYS-W-EVENT: !!! ********** !!!*

%SYS-W-EVENT: !!! Cluster workers configuration was loaded with errors !!!

%SYS-W-EVENT: !!! Check error messages !!!

%SYS-W-EVENT: !!! Start with default configuration !!!

*%SYS-W-EVENT: !!! ********** !!!*

2.11.5 Ошибка при загрузке на предыдущей конфигурации, попытка загрузиться по Zero Touch Provisioning — ошибка загрузки конфигурации

Пример:

*%SYS-W-EVENT: !!! ********** !!!*

%SYS-W-EVENT: !!! Failed to start with user configuration !!!

%SYS-W-EVENT: !!! Try preparing to restart ZTP !!!

*%SYS-W-EVENT: !!! ********** !!!*

2.11.6 Ошибка при загрузке на предыдущей конфигурации, попытка загрузиться с дефолтной конфигурацией — ошибка загрузки конфигурации

Пример:

*%SYS-W-EVENT: !!! ********** !!!*

%SYS-W-EVENT: !!! Failed to start with user configuration !!!

%SYS-W-EVENT: !!! Start with default configuration !!!

*%SYS-W-EVENT: !!! ********** !!!*

2.11.7 Перезагрузка вследствие ошибки подготовки загрузки по Zero Touch Provisioning

Пример:

*%SYS-W-EVENT: !!! ********** !!!*

%SYS-W-EVENT: !!! Failed preparing to restart ZTP, reboot system !!!

*%SYS-W-EVENT: !!! ********** !!!*

2.11.8 Перезагрузка вследствие успеха подготовки загрузки по Zero Touch Provisioning

Пример:

*%SYS-W-EVENT: !!! ********** !!!*

%SYS-W-EVENT: !!! Preparing to restart ZTP successful, reboot system !!!

*%SYS-W-EVENT: !!! ********** !!!*

2.11.9 Перезагрузка вследствие ошибки загрузки дефолтной конфигурации

Пример:

*%SYS-W-EVENT: !!! ********** !!!*

%SYS-W-EVENT: !!! Failed to start with default configuration, reboot system !!!

*%SYS-W-EVENT: !!! ********** !!!*

3. Работа с файлами

3.1 Начало операции

Пример:

%FILE_MGR-I-INFO: operation started: 'copy system:default-config system:candidate-config' (index: 1, origin: CLI)

Паттерн:

%FILE_MGR-I-INFO: operation started: '%s1' (index: %d, origin: %s2)

Параметры:

%s1 — операция:

- *copy %s1.1 %s1.2*
  - *%s1.1 — путь: откуда,*
  - *%s1.2 — путь: куда*
- *delete %s1.1*
  - *%s1.1 — путь до файла*
- *checksum %s1.1*
  - *%s1.1 — путь до файла*
- *tech-support archive prepare*
- *verify filesystem*
- *verify filesystem-detailed*
- *clear storage-device %s1.1 %s1.2*
  - *%s1.1 — путь до устройства*
  - *%s1.2 — имя устройства*
- *verify storage-device %s1.1*
  - *%s1.1 — путь до устройства, включая имя*
- *unmout storage-device %s1.1*
  - *%s1.1 — путь до устройства, включая имя*
- *boot system image-%d1.1*
  - *%d1.1 — номер образа*
- *create mtd partition '%s1.1'*
  - *%s1.1 — имя партиции*

%d — номер операции

%s2 — источник: CLI | SNMP

3.2 Статус операции

Пример:

%FILE_MGR-I-INFO: operation is finished: 'copy system:default-config system:candidate-config' (index: 1, origin:CLI)

Паттерн:

%FILE_MGR-I-INFO: operation %s1: '%s2' (index: %d, origin: %s1)

Параметры:

%s1 — статус

%s2 — операция:

copy %s2.1 %s2.2

%s2.1 — путь: откуда,

%s2.2 — путь: куда

delete %s2.1

%s2.1 — путь до файла

checksum %s2.1

%s2.1 — путь до файла

tech-support archive prepare

verify filesystem

verify filesystem-detailed

clear storage-device %s2.1 %s2.2

%s2.1 — путь до устройства

%s2.2 — имя устройства

verify storage-device %s2.1

%s2.1 — путь до устройства, включая имя

unmout storage-device %s2.1

%s2.1 — путь до устройства, включая имя

boot system image-%d2.1

%d2.1 — номер образа

create mtd partition '%s2.1'

%s2.1 — имя партиции

%d — номер операции

%s3 — источник: CLI | SNMP

4. События firewall

4.1 Защита от DoS / DDoS

Защиты могут быть включены в конфигурации в семействе команд firewall screen. Включение логирования осуществляется включением команд семейства logging firewall screen.

Пример:

%FIREWALL-W-WARN: screen 'ip-spoofing' (VRF_test) denied icmp 10.0.1.2 (US) (gi1/0/2 06:3a:61:66:72:7c) -> 10.0.1.3 (RU)

Паттерн:

%FIREWALL-W-WARN: screen '%s1' (%s2) %s3 %s4 %s5 (%s6) (%s7 %s8) -> %s9 (%s10)

Параметры:

'%s1' — тип защиты (win-nuke | zero-port | large-icmp | port-scan | syn-flood | destination-limit | source-limit | icmp-threshold | udp-threshold | ip-sweep | ip-spoofing | icmp-frag | udp-frag | syn-frag | unknown-proto | ip-frag | icmp-type-reserved | icmp-type-quench | icmp-type-echo-request | icmp-type-time-exceeded | icmp-type-unreachable | syn-fin-flags | fin-no-ack-flags | no-flags | land-attack | tcp-all-flags)

(%s2) — имя VRF (может отсутствовать, если не задано)

%s3 — действие (detected | denied)

%s4 — протокол

%s5 — IP-адрес (IPv6-адрес) источника

%s6 — код страны источника по GeoIP в виде (только при включённом geoip-логировании)

%s7 — имя интерфейса

%s8 — MAC-адрес отправителя пакета из Ethernet-заголовка (если MAC-адрес доступен)

%s9 — IP-адрес (IPv6-адрес) назначения

(%s10) — код страны назначения по GeoIP (только при включённом geoip-логировании)

4.2 Срабатывания zone-based firewall

Включается командой log в конфигурации zone-pair при задании action для правила.

Пример для IPv4-трафика:

%FIREWALL-I-LOG: zone-pair 'untrust trust' rule 1 (VRF_test) denied tcp 10.0.0.10:34618 (US) (gi1/0/2 50:3e:aa:02:98:87) -> 1.1.1.2:80 (RU) dscp 10

Паттерн для IPv4-трафика:

%FIREWALL-I-LOG: zone-pair '%s1 %s2' rule %d3 (%s4) %s5 %s6 %s7:%d7 (%s8) (%s9 %s10) -> %s11:%d11 (%s12) dscp %d13

Пример для IPv6-трафика:

%FIREWALL-I-LOG: zone-pair 'untrust trust' rule 1 (VRF_test) denied tcp [2001:db8::10]:34618 (US) (gi1/0/2 50:3e:aa:02:98:87) -> [2001:db8::1]:80 (RU)

Паттерн для IPv6-трафика:

%FIREWALL-I-LOG: zone-pair '%s1 %s2' rule %d3 (%s4) %s5 %s6 [%s7]:%d7 (%s8) (%s9 %s10) -> [%s11]:%d11 (%s12)

Параметры:

%s1 — зона источника

%s2 — зона назначения

%d3 — номер правила срабатывания

(%s4) — имя VRF (может отсутствовать, если не задано)

%s5 — действие (permitted | denied | rejected | redirected | detected | disabled)

%s6 — протокол

%s7:%d7 — IP-адрес источника : номер порта. (порт печатается при наличии и только для TCP/UDP)

[%s7]:%d7 — IPv6-адрес источника : номер порта. Если указан порт — IPv6-адрес в скобках, иначе без

(%s8) — код страны источника по GeoIP в виде (только при включённом geoip-логировании)

%s9 — имя интерфейса

%s10 — MAC-адрес отправителя пакета из Ethernet-заголовка (если MAC-адрес доступен)

%s11:%d11 — IP-адрес источника : номер порта. Порт печатается при наличии и только для TCP/UDP

[%s11]:%d11 — IPv6-адрес источника : номер порта. Если указан порт — IPv6-адрес в скобках, иначе без

(%s12) — код страны назначения по GeoIP в виде (только при включённом geoip-логировании)

%d13 — DSCP-метка

4.3 Срабатывания HTTP(s) proxy

Включается командой log enable в конфигурации http-профиля.

Пример:

%FIREWALL-I-LOG: http proxy 'Filter' (VRF_test) denied (JavaScript) 192.168.1.100:34618 (US) (gi1/0/2) -> 104.20.83.39:80 (RU)

Паттерн:

%FIREWALL-I-LOG: %s1 proxy '%s2' (%s3) %s4 (%s5) %s6:%d6 (%s7) %s8 -> %s9:%d9 (%s10)

Параметры:

%s1 — тип прокси (http | https)

'%s2' — имя профиля срабатывания

(%s3) — имя VRF (может отсутствовать, если не задано)

%s4 — действие (permitted | redirected | denied)

(%s5) — причина фильтрации (JavaScript | activex | cookie) (может отсутствовать)

%s6:%d6 — IP-адрес источника : номер порта (порт печатается при наличии)

%s7 — код страны источника по GeoIP (только при включённом geoip-логировании)

(%s8) — имя интерфейса

%s9:%d9 — IP-адрес источника : номер порта (порт печатается при наличии)

%s10 — код страны назначения по GeoIP (только при включённом geoip-логировании)

4.4 Срабатывания NAT-трансляции

Включение логирования осуществляется включением команд семейства logging nat. Здесь NAT proxy — это proxy-arp.

Пример:

%NAT-I-LOG: SNAT ruleset 'mine_awesome_set' rule 1 (VRF_test) permitted translation for tcp 192.168.1.254:65023 to 172.16.0.100:23

Паттерн:

%NAT-I-LOG: %s1 ruleset '%s2' rule %d2 (%s3) %s4 translation for %s5 %s6:%d6 %s7

Параметры:

%s1 — тип NAT (SNAT | DNAT | Proxy)

ruleset '%s2' rule %d2 — имя профиля и номер правила срабатывания (для source / destination NAT)

(%s3) — имя VRF (может отсутствовать, если не задано)

%s4 — действие (permitted | disabled)

%s5 — протокол

%s6:%d6 — IP-адрес : номер порта (при трансляции в порт)
Source NAT — адрес источника
Destination NAT и proxy-arp — адрес назначения.

%s7 — назначение трансляции (при наличии)
to port :%d7.1
%d7.1 — номер порта
to %s7.1:%d7.1
%s7.1:%d7.1 — IP-адрес : номер порта (при трансляции в порт)

4.5 Срабатывания ARP inspection

Включение логирования осуществляется включением команды logging firewall arp-inspection.

Пример:

%FIREWALL-W-WARN: arp-inspection (VRF_test) 50:3e:aa:02:98:87(192.168.56.11) -> 08:00:27:50:cf:2e(192.168.56.101) denied (gi1/0/1 50:3e:aa:02:98:87)

Паттерн:

%FIREWALL-W-WARN: arp-inspection (%s1) %s2(%s3) -> %s4(%s5) %s6 (%s7 %s8)

Параметры:

(%s1) — имя VRF (может отсутствовать, если не задано)

%s2 — MAC-адрес источника

%s3 — IP-адрес источника

%s4 — MAC-адрес назначения

%s5 — IP-адрес (IPv6-адрес) назначения

%s6 — действие (detected | denied)

%s7 — имя интерфейса срабатывания

%s8 — MAC-адрес отправителя пакета

4.6 Срабатывания BGP FlowSpec

Включение логирования осуществляется включением команд семейства logging bgp-flowspec.

Пример:

%FIREWALL-W-WARN: bgp-flowspec detected tcp 10.0.0.10 (US) (gi1/0/2 50:3e:aa:02:98:87) -> 1.1.1.2 (RU)

Паттерн:

%FIREWALL-W-WARN: bgp-flowspec %s1 %s2 %s3 %s4 (%s5 %s6) -> %s7 %s8

Параметры:

%s1 — действие (detected | denied)

%s2 — протокол

%s3 — IP-адрес (IPv6-адрес) источника

%s4 — код страны источника по GeoIP (только при включённом geoip-логировании)

%s5 — имя интерфейса

%s6 — MAC-адрес отправителя

%s7 — IP-адрес (IPv6-адрес) назначения

(%s8) — код страны назначения по GeoIP (только при включённом geoip-логировании)

5. События системы обнаружения (предотвращения) вторжений

5.1 Срабатывание правила (сигнатуры)

Правило срабатывания аналогично правилу срабатывания для open-source проекта Suricata, с мнемоникой *%IPS-I-INFO*

Примеры:

%IPS-I-INFO: [Drop] [1:30010:0] Rule 10 Drop [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.108:2048 -> 8.8.8.8:0

%IPS-I-INFO: [1:30020:0] Rule 20 Alert [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.108:2048 -> 8.8.4.4:0

%IPS-I-INFO: [2:10037:0] Traffic categorised as 'news'detected! [Classification: (null)] [Priority: 3] {TCP} 192.168.34.2:42194 -> 95.173.136.72:80

Паттерн:

%IPS-I-INFO: [%s1] [%d2:%d2:%d2] %s3 [Classification: %s4] [Priority: %d5] {%s6} %s7:%d7 -> %s8:%d8

Параметры:

[%s1] — действие над пакетом (может отсутствовать, если действие не производится)

%d2:%d2:%d2 - group id : rule id : revision id

%s3 — meta-сообщение

%s4 — классификатор

%d5 — приоритет

%s6 — протокол

%s7:%d7 — IP-адрес источника : номер порта

%s8:%d8 — IP-адрес назначения: номер порта

5.2 Загрузка нового (или первого) списка правил в IPS

Пример:

%IPS-I-INFO: 1 rule files processed. 252 rules successfully loaded, 0 rules failed

Паттерн:

%IPS-I-INFO: %d1 rule files processed. %d2 rules successfully loaded, %d3 rules failed

Параметры:

%d1 — количество файлов с правилами

%d2 — количество успешно загруженных правил

%d3 — количество неуспешно загруженных правил (ошибки в правилах, ошибки парсинга, etc)

5.3 Начало применения нового списка правил

Пример:

%IPS-N-NOTICE: rule reload starting

Паттерн:

%IPS-N-NOTICE: rule reload starting

5.4 Успешное применение нового списка правил

Пример:

%IPS-N-NOTICE: rule reload complete

Паттерн:

%IPS-N-NOTICE: rule reload complete

5.5 Успешный запуск IPS

Пример:

%IPS-I-INFO: Configuration provided was successfully loaded.

Паттерн:

%IPS-I-INFO: Configuration provided was successfully loaded.

6. Описание событий системы защиты от атак перебором (auth-guard)

6.1 Блокировка источника

Пример:

%AUTH_GUARD-I-INFO: Host "10.0.0.10" banned on service "ssh" in vrf "VRF_test" for "5" minutes

Паттерн:

%AUTH_GUARD-I-INFO: Host "%s1" banned on service "%s2" %s3 for "%d4" minutes

Параметры:

%s1 — IP-адрес (IPv4-адрес) источника

%s2 — имя сервиса, на котором зафиксирована атака: SSH | Telnet | SNMP

%s3 — блок ' in vrf "%s3"' — имя VRF (может отсутствовать, если не задано)

%d4 — длительность блокировки в минутах

6.2 Автоматическая разблокировка по истечении срока бана

Пример:

%AUTH_GUARD-I-INFO: Host "10.0.0.10" unbanned in vrf "VRF_test" after ban expiry

Паттерн:

%AUTH_GUARD-I-INFO: Host "%s1" unbanned %s2 after ban expiry

Параметры:

%s1 — IP-адрес (IPv4-адрес) источника

%s2 — блок ' in vrf "%s2"' — имя VRF (может отсутствовать, если не задано)

6.3 Ручная разблокировка пользователем

Пример:

%AUTH_GUARD-I-INFO: Host "10.0.0.10" unbanned manualy in vrf "VRF_test" by user "admin" on "console"

Паттерн:

%AUTH_GUARD-I-INFO: Host "%s1" unbanned manualy %s2 by user "%s3" on "%s4"

Параметры:

%s1 — IP-адрес (IPv4-адрес) источника

%s2 — блок ' in vrf "%s2"' — имя VRF (может отсутствовать, если не задано)

%s3 — имя пользователя, выполнившего разблокировку

%s4 — источник: sudo | console | ssh | telnet

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: https://eltex.ru/support

Servicedesk: https://servicedesk.eltex-co.ru

На официальном сайте компании вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку:

Официальный сайт компании: https://eltex.ru

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex.ru/download