

**с•терра®**

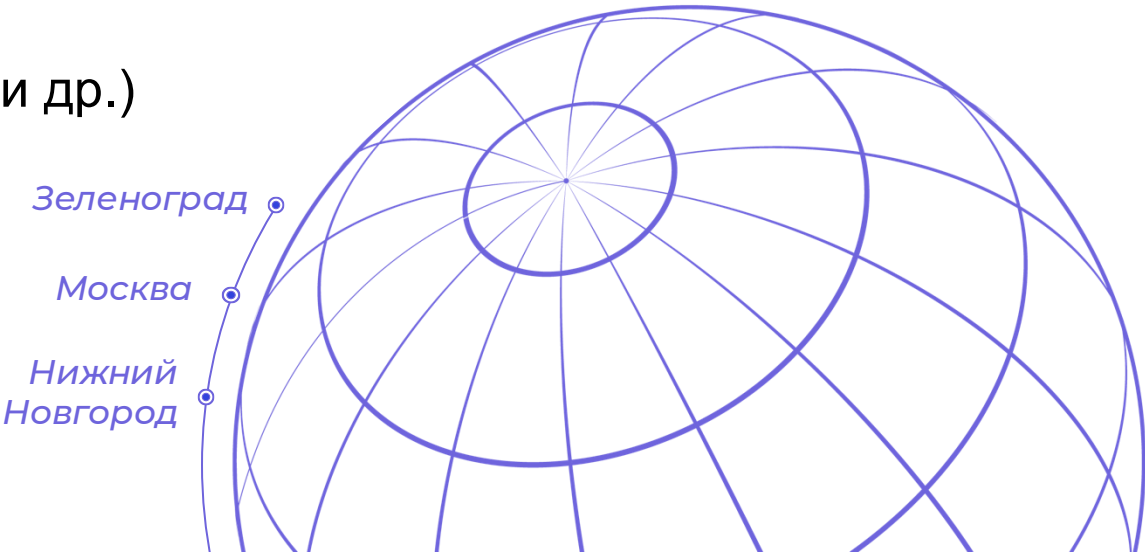
*Ваш ориентир в мире безопасности*

# С-ТЕРРА ЭКРАН-М

Москва, 2025

Разработка и производство **СЕРТИФИЦИРОВАННЫХ** средств защиты каналов связи (VPN, FW, TLS, NGFW и др.)

**КРИПТОГРАФИЧЕСКАЯ** защита информации.  
Лицензиаты **ФСБ** России и **ФСТЭК** России



## [ Органы власти ]

Безопасная цифровая среда для управления, устойчивости и доверия



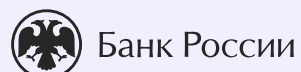
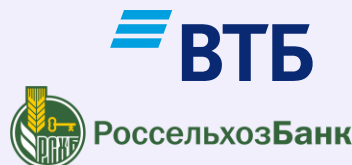
## [ Производство и ТЭК ]

ИБ-решения для непрерывной работы и защиты стратегической инфраструктуры



## [ Финансовые организации ]

Защита фин.сервисов, клиентских данных и критичных операций



## [ Операторы связи ]

Надёжность и контроль в сетях с миллионами подключений.



# ЧТО МЫ ПРЕДЛАГАЕМ РЫНКУ И ЧЕМ МЫ ЛУЧШЕ

*С-Терра Экран М - многофункциональный межсетевой экран уровня сети*

## [ Архитектура ]

- Разработана с нуля в 2023–2024 г.
- Создавалась под требования ФСТЭК

## [ Модульность ]

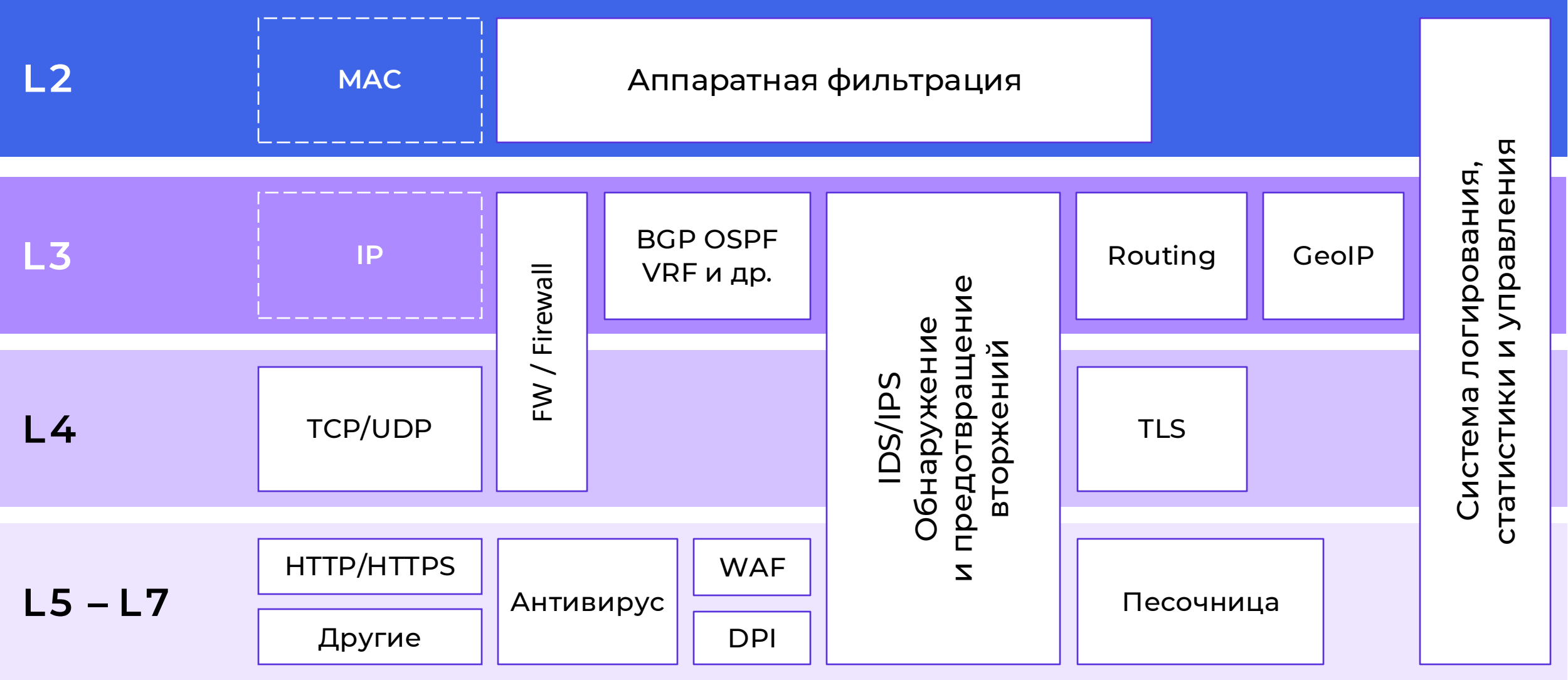
- Интеграция с внешними системами
- Гибкое изменение состава модулей

## [ Сертификация ]

- ФСТЭК по профилю защиты многофункциональных межсетевых экранов уровня сети четвертого класса защиты
- Российская разработка под ОС Astra Linux

## [ Опыт ]

- Существующие решения С-Терра
- Экспертиза и компетенции компании с более чем 21 летним опытом работы на рынке ИБ



Firewall, IPS, Контроль приложений, Антивирус, WAF, Песочница и другие

ЭКРАН-М

Информационная панель

Конфигурация

Модули

Система

Подчинённые ПАК

Резервные копии

Пользователи

Мониторинг

Сервисы

Правила трафика

Отчеты и журналы

Внешние системы

Песочница

Антивирус (ClamAV)

Тестирование

VPN

Модули

COB

Обнаружение и предотвращение атак

Интерфейс

Отключен

К разделу

Настроить

WAF

Firewall веб-приложений

Интерфейс

Отключен

К разделу

Настроить

Firewall

Firewall

Работает

К разделу

Контроль приложений

Глубокая проверка пакетов

Интерфейс

eth3

Работает

К разделу

Настроить

Маршрутизация

Маршрутизация

Работает

К разделу

Прокси

Настройка промежуточного сервера

Работает

К разделу

Логирование

Настройка внешнего логирования

Отключен

К разделу

Песочница

Изолированная среда запуска программ

Работает

К разделу

Настроить

Антивирус (ClamAV)

Антивирус. Последнее обновление баз совершено 7/16/2025, 5:35:28 PM. Количество сигнатур: 8723346. Версия баз: 28098

Работает

ДПИ успешно включен

## [ С-Терра Экран-М 8000 ]



## [ С-Терра Экран-М 7000 ]



В декабре 2024 года стартовала сертификация Экран-М на соответствие требованиям к ММЭ уровня сети во ФСТЭК РФ

2024  
Протестировано  
ЦБ РФ

2025  
Проверено  
ФСТЭК РФ

- Обработка трафика вынесена за пределы ядра в пользовательское пространство. Взаимодействие с сетевой картой напрямую
- Технологии DPDK и VPP



Пропускная способность в режиме FW + Stateful + NAT + IPS + Антивирус для **Экран М 8000 – до 24 Гбит/с**  
\*Согласно тестам Инфосистемы Джет

| Режим работы                                     | Пропускная способность на один порт |               | Количество правил       |
|--------------------------------------------------|-------------------------------------|---------------|-------------------------|
|                                                  | Экран-М 8000                        | Экран-М 7000  |                         |
| FW + Stateful                                    | До 96 Гбит/с                        | До 38 Гбит/с  | 100 тыс. ACL            |
| FW + IDS/IPS                                     | До 24 Гбит/с                        | До 12 Гбит/с  | 100 тыс. ACL + 40 тыс.  |
| FW + IDS/IPS + WAF                               | До 10 Гбит/с                        | До 6 Гбит/с   | 100 тыс. ACL + 60 тыс.  |
| FW + IDS/IPS + DPI + WAF + Антивирус + Песочница | До 5 Гбит/с                         | До 3.5 Гбит/с | 100 тыс. ACL + 150 тыс. |

# В ПЛАНАХ — РАСШИРЕНИЕ ЛИНЕЙКИ ДЛЯ ЭКРАН-М

*Модификации Экран-М на младших и средних аппаратных платформах*

## [ С-Терра Экран-М 100 ]



## [ С-Терра Экран-М 1000 ]



## [ С-Терра Экран-М 3000 ]



## [ С-Терра Экран-М 7000 ]



## [ Информационная безопасность ]

*IPS и IDS / URL-фильтрация / GeoIP / Прокси-сервер  
/ Расширенный DNS-анализ / Интеграция с MS AD*

- VPN  
*(IPsec IKEv2 без ГОСТ, WireGuard)*
- Межсетевой экран  
*(Firewall, в т.ч. stateful фильтрация)*
- Антивирус и Песочница  
*(изолированная среда анализа  
с контролем поведения объектов)*
- Определение категории  
сайта конкретного запроса  
*(категории фильтрации)*
- Интеграция с внешними  
системами по REST API  
*(включая автоматизацию реакции  
на инциденты, прямая интеграция  
с Гарда DLP)*
- Группировка событий различного типа,  
сгенерированных в рамках одной сессии  
*(межсетевое экранирование, защита от угроз,  
контроль передачи файлов, URL-фильтрация,  
времени сессий)*

В примере выполняется поиск и отключение совпадений по SID (signature ID)

<> Редактор регулярных выражений ?

Корректное

Регулярное выражение

\*sid:3400139;

Введите регулярное выражение (например: \*a-z0-9\_){3,16}\$)

Тестовая строка

\*sid:3400139;

Введите строку для проверки регулярного выражения

Результаты:

Найдено совпадений: 1

Справка по регулярным выражениям

☐ Включить

Применить

Закрыть

ЭКРАН.М

Правила

sterra\_adm

Администратор ММЭ

🔔

👤

Название

Поиск

eth0

IPS

Работает на интерфейсе eth0

Применить правила

Добавить

| Название ↑ | URI  | Последнее обновление | Логин | Категории | Правила |
|------------|------|----------------------|-------|-----------|---------|
| ^ Anomaly  | Файл | 25.07.2025 12:10:52  |       | 1         | 16      |

Название

Поиск

| Название  | Время создания      | Последнее обновление | Логин |
|-----------|---------------------|----------------------|-------|
| ^ Anomaly | 25.07.2025 12:10:54 | 25.07.2025 12:10:54  |       |

Поиск правил

Q

| SID     | Логин | Сообщение                               | Изменено            |
|---------|-------|-----------------------------------------|---------------------|
| 3400139 |       | Potential Idle TCP Connection Detected  | 25.07.2025 12:10:57 |
| 3400140 |       | SURICATA HTTP but not tcp port 80, 8080 | 25.07.2025 12:10:57 |
| 3400141 |       | SURICATA Port 80 but not HTTP           | 25.07.2025 12:10:57 |
| 3400143 |       | SURICATA Port 443 but not TLS           | 25.07.2025 12:10:57 |

Информационная панель

Конфигурация

Пользователи

Мониторинг

Сервисы

Правила трафика

URL фильтрация

COB

Правила

Данные

Репутационные списки

NAT

Firewall

Контроль приложений

WAF

Geo IP

Отчеты и журналы

Внешние системы

## [ Песочница ]

- Отчёт содержит подробную статистику по срабатываниям сигнатур
- Настройка работы песочницы по пользователям или хостам
- Поддерживается работа на всех аппаратных платформах линейки

## [ Антивирус ]

- Поддержка блокировки зашифрованных файлов
- Поддерживается работа на всех аппаратных платформах линейки
- Настройка антивируса для точечной проверки пользователей или хостов по IP / MAC адресам

← Вернуться

О задании

Решение о блокировке

Заблокировать

Вердикт

Опасное ПО

Уровень опасности

10 из 10

Статус проверки

✓ Завершено

Время создания

08.07.2025, 12:12:25

Время окончания

08.07.2025, 12:20:06

Источники для проверки

Ручная проверка

Роль

Администратор MM3

Пользователь

sterra\_admin

Файл

object10\_SANDBOX(1).docm

Тип файла

Microsoft Word 2007+

Размер

140537 bytes

SHA256

b5abc5e78a19aee590cee10f8fbbacdb43b8tc80a39a80c6add940186852774

SHA1

393cf04bafaecb9c5d9714c92b360423ab8ca810

MD5

febd8def8ce6c20651bc6a4d093b02b9

Общее количество обнаруженных сигнатур

3

Сумма угроз всех сигнатур

8

Конфигурация вредоносного ПО

Office DDE

Обнаруженные сигнатуры ^

Название

Поиск

Название ↑

Описание

Уровень опасности

allocates\_nox

Allocates read-write-execute memory (usually to unpack itself)

2

office\_dde

Malicious document featuring Office DDE has been identified

3

office\_vuln\_modules

Libraries known to be associated with a CVE were requested (may be False Positive)

3

Элементов на странице:

5

1 из 3

<

>

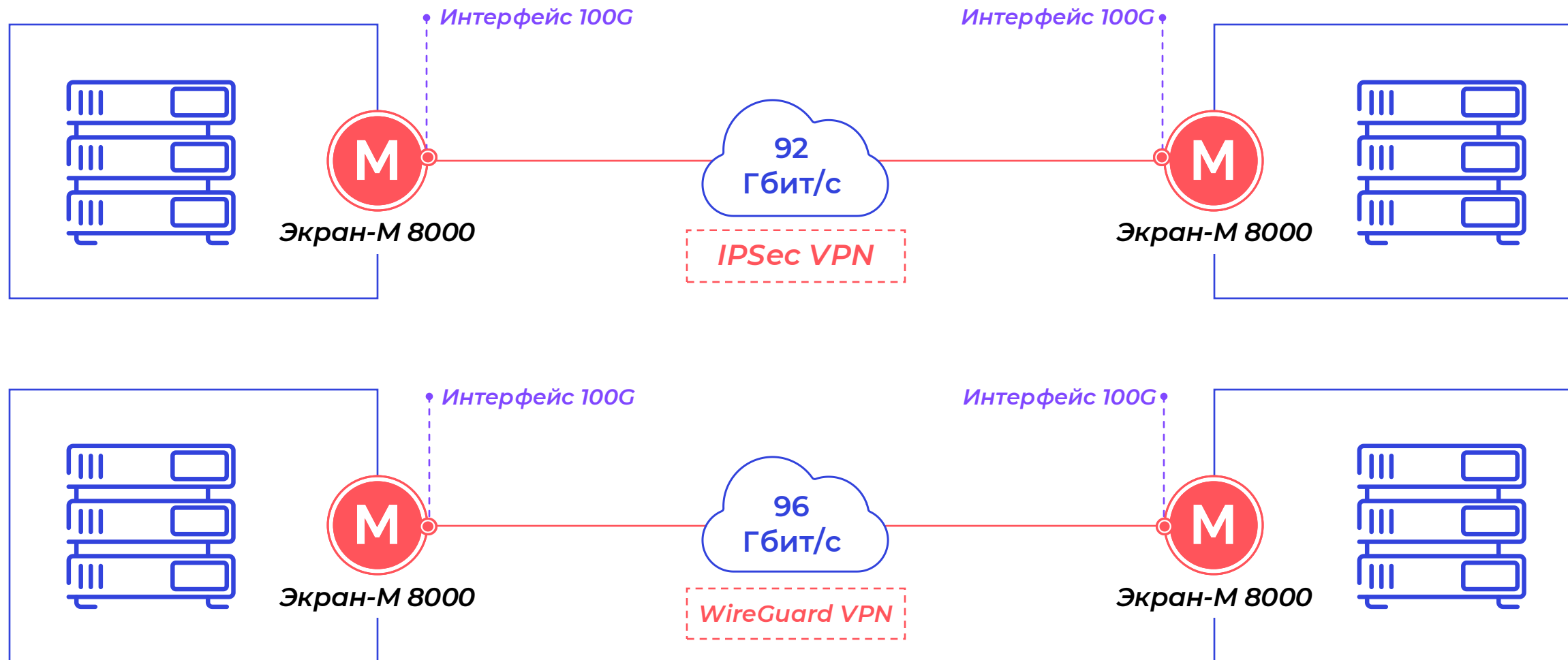
Поведенческий анализ

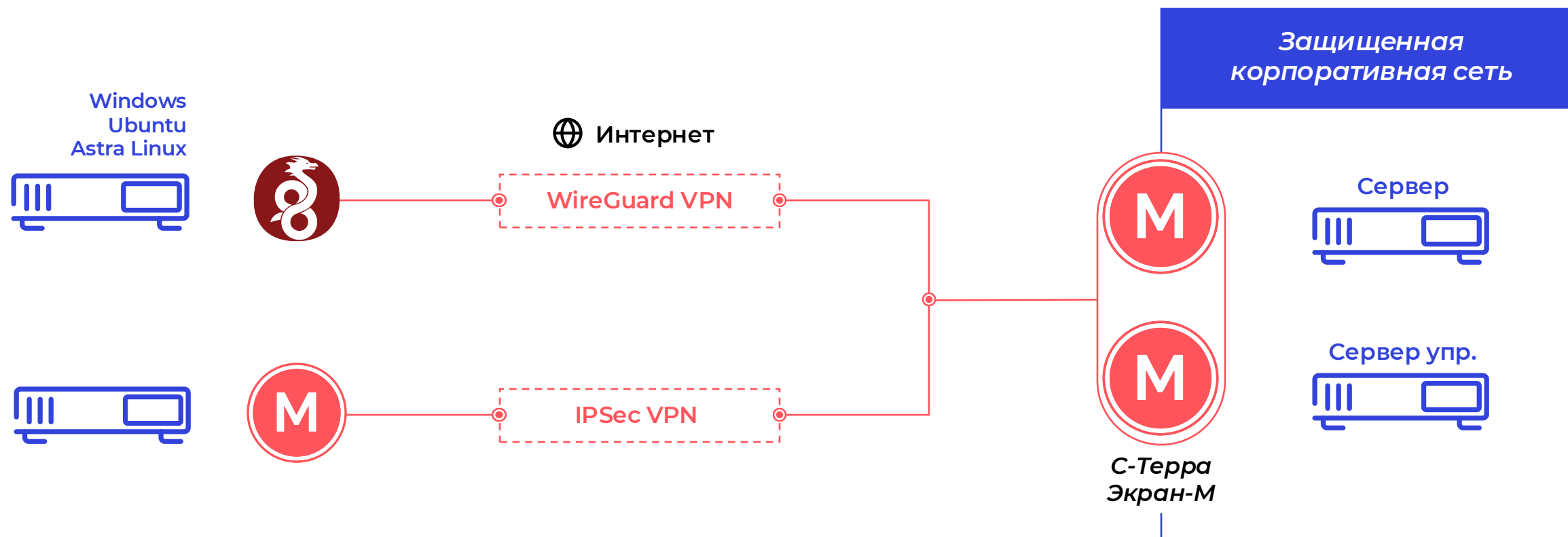
Развернуть ^

Опасное ПО

win7-sp1-x64 (Windows 7 Enterprise 6.1.7601 x4)

IPSec VPN и WireGuard VPN





События сбоев, события администрирования, обнаружения компьютерных атак, обнаружения вредоносного ПО

### Настройка отображения событий безопасности

Роль:  
sterra

#### События администрирования

Действия администраторов: ☒ Регистрировать события ☒ Уведомлять о событиях

Время изменения ▾ Модуль ▾ Событие ▾ Пользователь ▾ IP ▾  

#### События обнаружения компьютерных атак

События безопасности COB: ☐ Регистрировать события ☐ Уведомлять о событиях

Время ▾ ID ▾ Сообщение ▾ Тип атаки ▾ Вердикт ▾ Действие ▾ Протокол ▾ IP-клиента ▾ IP-хоста ▾  

#### События сбоев

События сбоев Экран-М: ☒ Регистрировать события ☒ Уведомлять о событиях

Дата и время ▾ Модуль ▾ Тип сбоя ▾ Описание ▾  

#### События обнаружения вредоносного ПО

События безопасности песочницы: ☒ Регистрировать события ☒ Уведомлять о событиях

Время ▾ Версия ▾ Категория ▾ Задача ▾ ОС песочницы ▾ Источник проверки ▾ Вердикт ▾ Уровень опасности ▾ Статус анализа ▾ Тип действия ▾ MD5 ▾ SHA1 ▾

События безопасности антивируса: ☐ Регистрировать события ☐ Уведомлять о событиях

## Применение политик безопасности на основе групп и пользователей

**Выбор пользователей**

☐ dc=example,dc=com ^

☐ cn=admin,dc=example,dc=com

☐ uid=newton,dc=example,dc=com

☐ uid=einstein,dc=example,dc=com

☐ uid=tesla,dc=example,dc=com

☐ uid=galileo,dc=example,dc=com

☐ uid=euler,dc=example,dc=com

☐ uid=gauss,dc=example,dc=com

☐ uid=riemann,dc=example,dc=com

☐ uid=euclid,dc=example,dc=com

☐ ou=mathematicians,dc=example,dc=com

☐ ou=scientists,dc=example,dc=com v

☐ cn=read-only-admin,dc=example,dc=com

☐ uid=test,dc=example,dc=com

☐ ou=chemists,dc=example,dc=com

☐ uid=curie,dc=example,dc=com

☐ uid=nobel,dc=example,dc=com

Пользователи сети

sterra\_admin

Администратор ММЭ

Правила сети

Коннектор

Пользователи сети

LDAP: соединение успешно

Настройка коннектора авторизации пользователя

Сохранение коннектора

Имя коннектора \*

Test\_AD

Имя хоста \*

ldap://10.21.3.102

Порт \*

389

Сохранить

Очистить

Настройка LDAP

DN \*

CN=test\_user,OU=NGFW\_Users,DC=ngfw,DC=stlab

Фильтр

(objectClass=\*)

Пароль \*

.....

Проверить соединение

Показать

© «С-Терра СиЭсПи», 2025

16

## [ Больше, чем вы ждёте ]

*SMTP / NTP-клиент / DHCP (сервер и relay) / PPPoE*

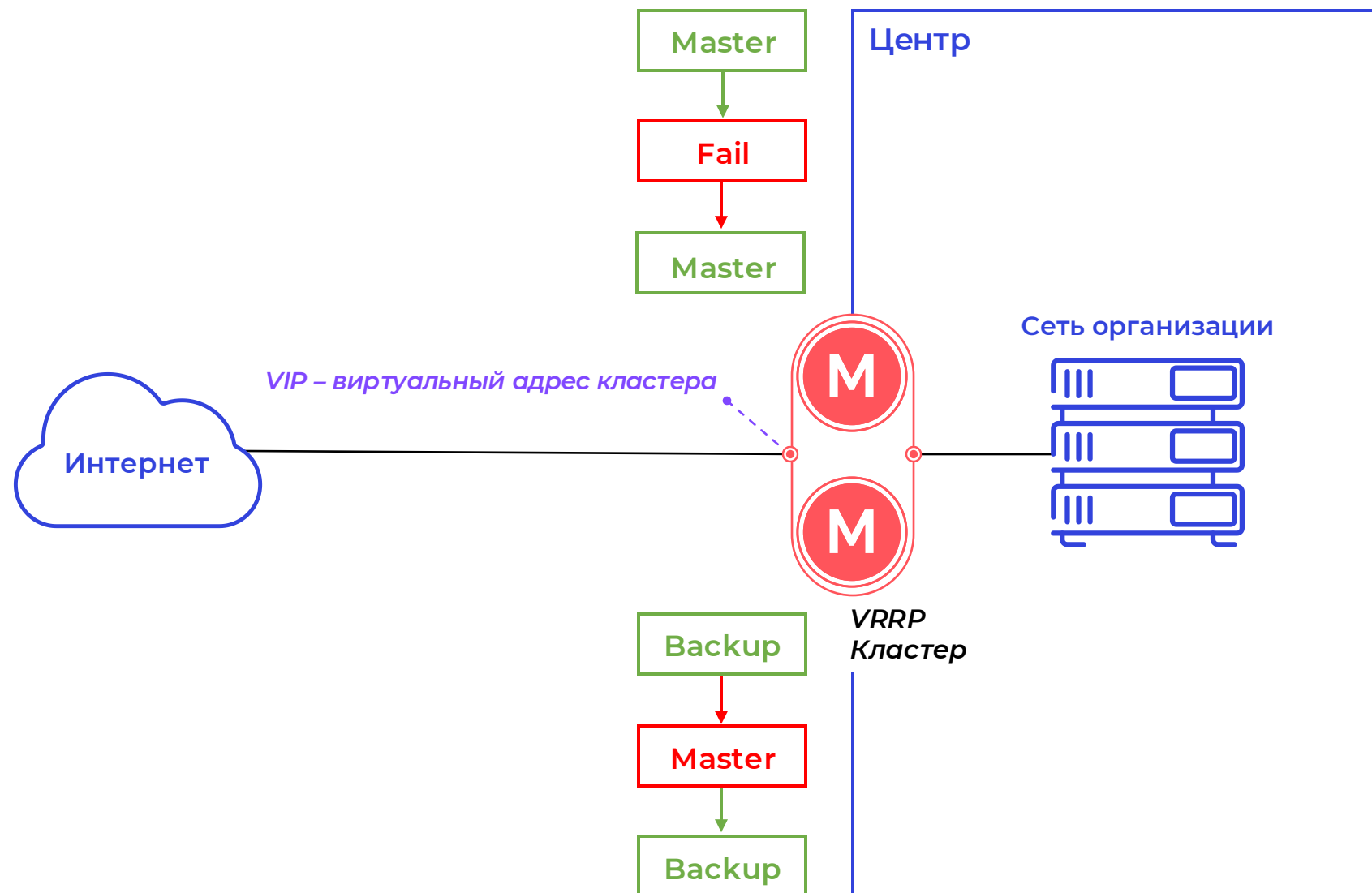
- NAT / PAT  
*(трансляция сетевых адресов и портов)*
- VLAN  
*(802.1Q)*
- VxLAN  
*(Virtual Extensible LAN – виртуализация сети)*
- IPv6  
*(NAT, маршрутизация, правила МЭ)*
- SPAN  
*(порт зеркалирования)*
- Статическая и динамическая маршрутизация  
*(OSPF, BGP)*
- LACP  
*(агрегация каналов)*
- Кластеризация  
*(отказоустойчивость на базе VRRPv3)*

# КЛАСТЕР ЭКРАН-М

Отказоустойчивость на базе протокола VRRPv3

## [ Типы отказов ]

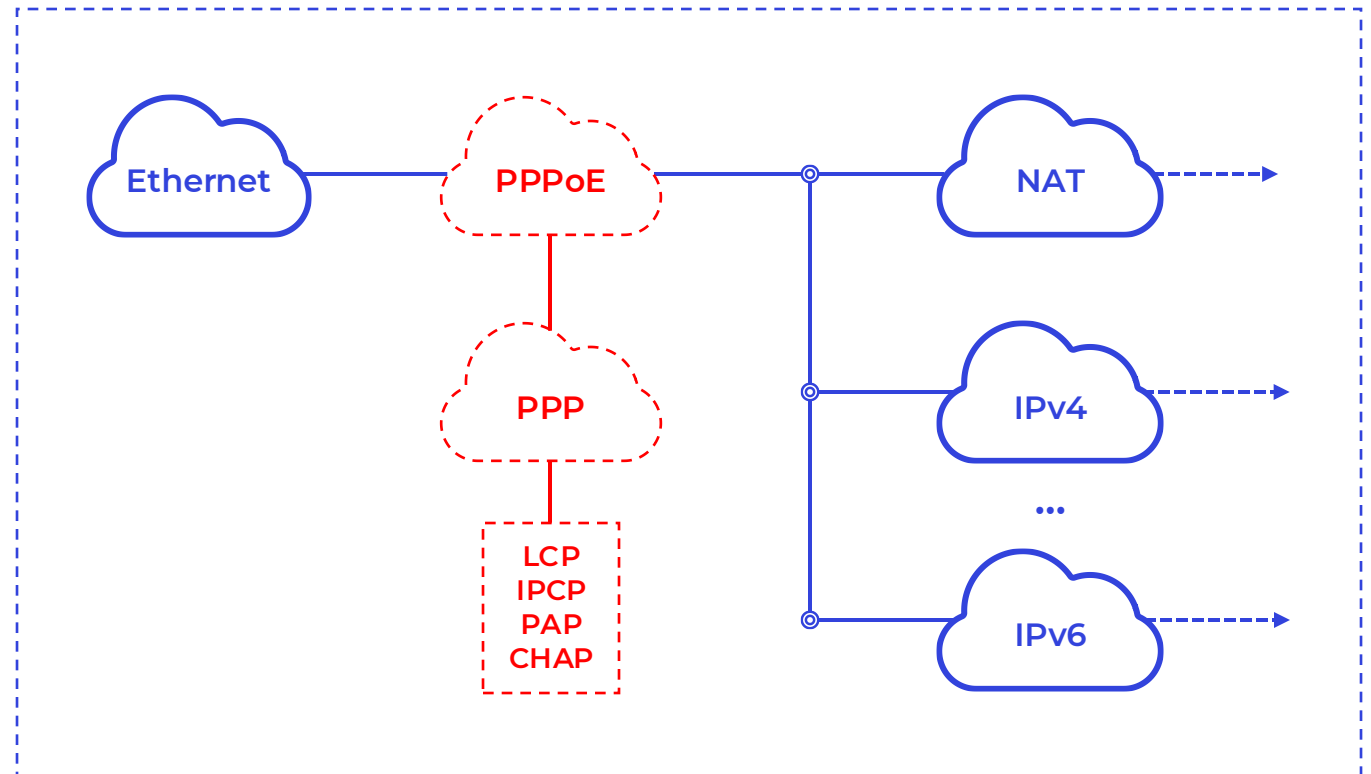
- Отключение питания
- Выход из строя аппаратной платформы
- Отказ сетевого интерфейса
- Отказ порта на коммутационном оборудовании



# ПОДДЕРЖКА СОЕДИНЕНИЙ PPPOE

*Point-to-Point Protocol over Ethernet - прямое подключение к провайдеру*

```
show pppoe client session
state:      11111
session_id: 19
sw_if_index: vpp0
LCP id:     7
AUTH id:    0
IPCP id:    3
MRU:        1492
Auth method: CHAP
Magic number: 0x327b23c6
our_ip:      47.1.1.118
peer_ip:     47.1.1.6
dns1:        8.8.8.8
dns2:        8.8.4.4
cookie_len:  20
cookie:      edc08bf80fcf949a660df456aab24d3cd1670000
username:    test
password:    test
provider:    pppoe
-- more -- (2-18/18)
```

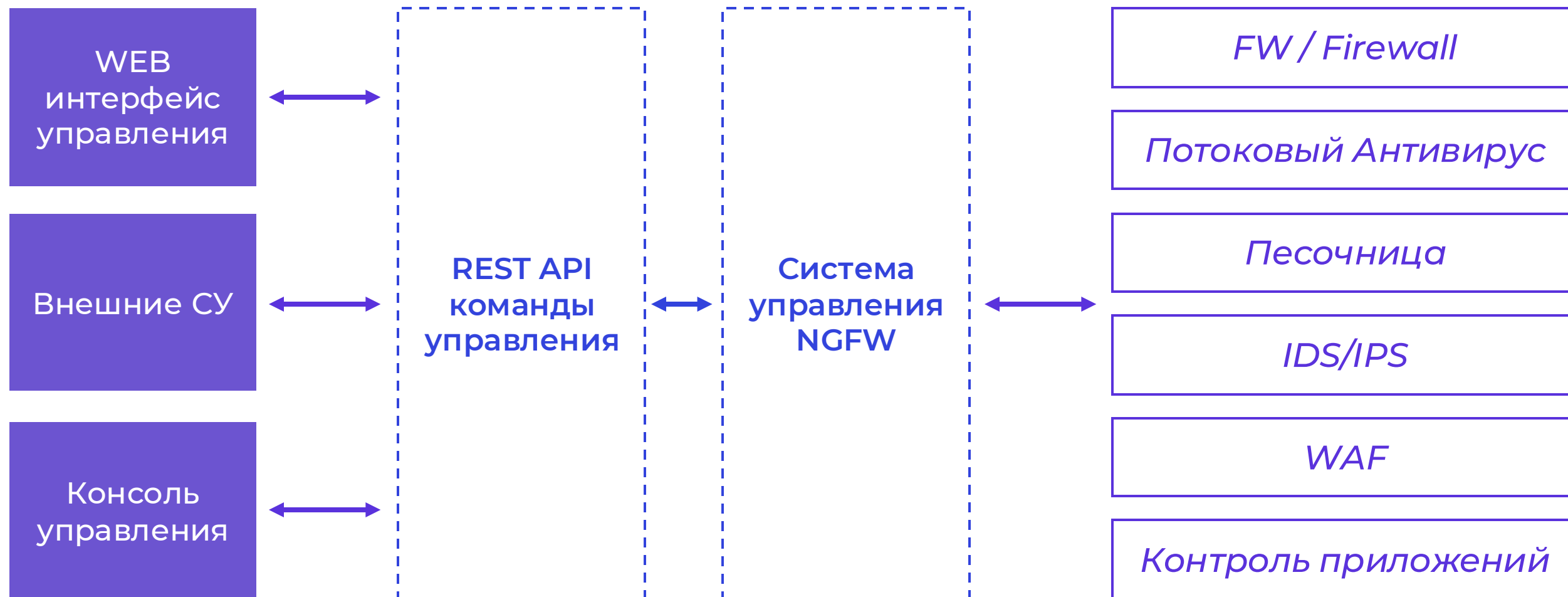


## [ Управление и эксплуатация ]

*Анализ и отслеживание изменений конфигурации / Создание пользователей и настройка ролей*

- Структура управления  
*(единая система с Web-интерфейсом, консолью и REST API для контроля всех функций Экран-М)*
- Автоматизация и контроль  
*(открытый REST API для интеграции с внешними системами и автоматизации управления)*
- Автоматические скрипты переноса настроек из других вендоров  
*(импорт настроек из решений других вендоров без ручной переработки)*
- Простая настройка ACL  
*(управление доступом через DRAG&DROP)*
- Визуализация зон и режимов работы интерфейсов  
*(наглядное отображение связей между зонами безопасности и сетевыми интерфейсами)*
- Групповое управление подчиненными межсетевыми экранами  
*(централизованное администрирование нескольких устройств из одного интерфейса)*

Единая система управления



# ОТКРЫТЫЙ REST API — АВТОМАТИЗАЦИЯ И КОНТРОЛЬ

Открытый интерфейс для подключения к вашей инфраструктуре

| OS     |                                  | ^ |
|--------|----------------------------------|---|
| GET    | /api/v1/os/disk                  | ▼ |
| GET    | /api/v1/version                  | ▼ |
| GET    | /api/v1/os/memory                | ▼ |
| GET    | /api/v1/os/cpu                   | ▼ |
| VPP    |                                  | ^ |
| GET    | /api/v1/vpp/interfaces           | ▼ |
| ACL    |                                  | ^ |
| POST   | /api/v1/vpp/acl/interfaces/rules | ▼ |
| DELETE | /api/v1/vpp/acl/interfaces/rules | ▼ |
| POST   | /api/v1/vpp/acl/rules            | ▼ |
| DELETE | /api/v1/vpp/acl/rules            | ▼ |

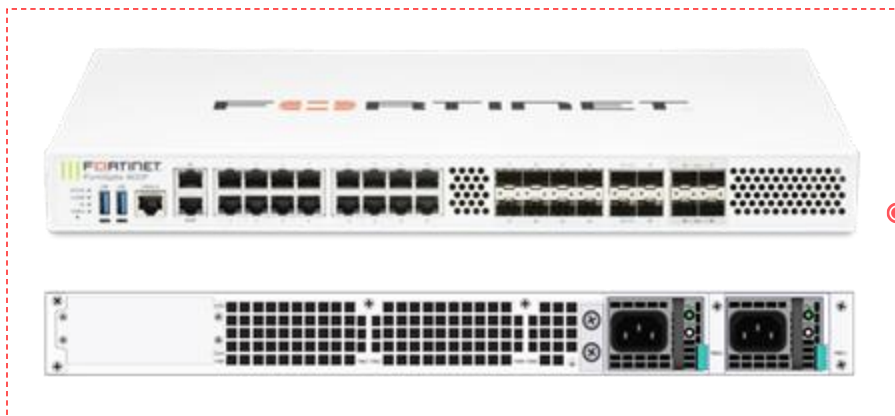
| FRR    |                            | ^ |
|--------|----------------------------|---|
| GET    | /api/v1/frr/ospf           | ▼ |
| POST   | /api/v1/frr/ospf           | ▼ |
| DELETE | /api/v1/frr/ospf           | ▼ |
| BGP    |                            | ^ |
| POST   | /api/v1/frr/bgp            | ▼ |
| POST   | /api/v1/frr/bgp/neighbors  | ▼ |
| DELETE | /api/v1/frr/bgp/neighbors  | ▼ |
| EIRGP  |                            | ^ |
| POST   | /api/v1/frr/eigrp          | ▼ |
| GET    | /api/v1/frr/eigrp          | ▼ |
| POST   | /api/v1/frr/eigrp/neighbor | ▼ |
| DELETE | /api/v1/frr/eigrp/neighbor | ▼ |

# АВТОМАТИЧЕСКИЕ СКРИПТЫ ПЕРЕНОСА КОНФИГУРАЦИИ

Возможность переноса настроек с оборудования других вендоров (FW + NAT).

Подбор конкретной аппаратной платформы С-Терра осуществляется с учётом требований проекта.

## [ FortiNet ]



Перенос

## [ Экран-М ]



## [ Check Point ]



Перенос

## [ Экран-М ]



# АНАЛИЗ И ОТСЛЕЖИВАНИЕ ИЗМЕНЕНИЙ В КОНФИГУРАЦИИ



## Сравнение правил (DIFF)

ЭКРАН-М

Правила

sterra\_admin

Изменения успешно получены.

Информационная Панель

Конфигурация

Просмотр изменений

Сбросить изменения

Обновленные правила

SID

Поиск

Переключить статус выбранного

|                          | SID     | Категория | Сообщение                           | Статус    | Действия           |
|--------------------------|---------|-----------|-------------------------------------|-----------|--------------------|
| <input type="checkbox"/> | 2008119 | tftp      | ET TFTP Outbound TFTP Error Message | Применено | Отменить Подробнее |

Правил на странице: 1 - 1 из 1

Принять изменения

Поиск сообщений

| SID     | Логин | Сообщение                           | Изменено            |
|---------|-------|-------------------------------------|---------------------|
| 2008117 |       | ET TFTP Outbound TFTP Data Transfer | 12.05.2025 16:19:00 |

Просмотр и редактирование правила

Категория: tftp

Старое правило

alert udp \$HOME\_NET any -> \$EXTERNAL\_NET 69 ( msg:"ET TFTP Outbound TFTP Error Message"; content:"|00 05|"; depth:2; byte\_test:1,&0x1F,0,relative; classtype:policy-violation; reference:url,en.wikipedia.org/wiki/Trivial\_File\_Transfer\_Protocol#TFTP\_messages; sid:2008119; rev:3; metadata: created\_at 2010\_07\_30, signature\_severity Informational, updated\_at 2019\_07\_26, service tftp;)

Новое правило

alert udp \$HOME\_NET any -> \$EXTERNAL\_NET 69 ( msg:"ET TFTP Outbound TFTP Error Message"; content:"|00 05|"; depth:2; classtype:policy-violation; sid:2008119; rev:3; metadata:created\_at 2010\_07\_30, signature\_severity Informational,updated\_at 2019\_07\_26;)

Редактирование

alert udp \$HOME\_NET any -> \$EXTERNAL\_NET 69 (msg:"ET content:"|00 05|"; depth:2; classtype:policy-violation; sid:2008119; rev:3; metadata:created\_at 2010\_07\_30, signature\_severity In )

Отмена Сохранить

# ГРУППОВОЕ УПРАВЛЕНИЕ ПОДЧИНЕННЫМИ МЕЖСЕТЕВЫМИ ЭКРАНАМИ



Контроль и управление из одного окна

ЭКРАН.М

< >

Информационная панель

Конфигурация

Модули

Система

**Подчинённые ПАК**

Резервные копии

Пользователи

Учетные записи

Пользователи сети

Обнаруженные устройства

Подчинённые ПАК

sterra\_adminsterra

Ваш лицензионный номер для подключения: 1234500890

Название

Поиск

Добавить группу

| Название        | Количество |  |
|-----------------|------------|--|
| Без группы      | 0          |  |
| Нижний Новгород | 1          |  |
| Зеленоград      | 1          |  |

Элементов на странице: 5 1 - 3 из 3

# РОЛЕВАЯ МОДЕЛЬ С-ТЕРРА ЭКРАН-М. СОЗДАНИЕ ПОЛЬЗОВАТЕЛЯ

*Экран-М обеспечивает возможность определения полномочий для пользователей ММЭ в пределах назначенных им ролей*

### Создание пользователя

Логин \*

Электронная почта \*

Пароль \*

Подтверждение пароля \*

Роль.

Администратор безопасности

Администратор безопасности

Администратор ММЭ

Администратор информационной (автоматизированной) системы

Sterra

# РОЛЕВАЯ МОДЕЛЬ С-ТЕРРА ЭКРАН-М. НАСТРОЙКА РОЛЕЙ

Экран-М обеспечивает возможность управления полномочиями для ролей в ММЭ

### Настройка ролей

☒ Редактировать ☐ Создать

Роль: 

Администратор ММЭ

#### Управление полномочиями

Доступные

Событийный выбор

Оповещение о вредоносном ПО

Оповещение о событиях безопасности

Оповещение о сетевой атаке

Настройка выгрузки данных

Выбранные

Создание учетных записей

Управление учетными записями

Назначение полномочий

Установка правил фильтрации

Изменение и удаление правил

< >  
« »

Сохранить Удалить Отмена

ПРОСТАЯ НАСТРОЙКА ACL — УПРАВЛЕНИЕ ДОСТУПОМ ЧЕРЕЗ DRAG&DROP



Настройка ACL без скриптов, консоли. Наглядно и удобно

Интерфейс eth3

Таблица всех ACL

Открыть фильтры

Выбранная цепочка правил: 7

Добавить ACL

|                                       | №  | ID | Описание                   | Количество правил | Действия |
|---------------------------------------|----|----|----------------------------|-------------------|----------|
|                                       | 1  | 0  | Service-Block-All          | 1                 |          |
|                                       | 2  | 1  | Service-Block-Not-Allowed  | 1                 |          |
|                                       | 3  | 2  | Service-Permit-Not-Blocked | 1                 |          |
| ▼ <input type="checkbox"/>            | 4  | 3  | Test_10000_ACL_5_objects   | 1                 | +        |
| ▼ <input type="checkbox"/>            | 5  | 4  | Test_10000_ACL_5_objects   | 1                 | +        |
| ▼ <input type="checkbox"/>            | 6  | 5  | Test_10000_ACL_5_objects   | 1                 | +        |
| ▼ <input type="checkbox"/>            | 7  | 6  | Test_10000_ACL_5_objects   | 1                 | +        |
| ▼ <input checked="" type="checkbox"/> | 8  | 7  | Test_10000_ACL_5_objects   | 1                 | +        |
| ▼ <input type="checkbox"/>            | 9  | 8  | Test_10000_ACL_5_objects   | 1                 | +        |
| ▼ <input type="checkbox"/>            | 10 | 9  | Test_10000_ACL_5_objects   | 1                 | +        |

Порядковый номер

Интерфейс eth3

ID: #2

Входящая

Исходящая

|                            | № | ID | Описание                 | Количество правил |
|----------------------------|---|----|--------------------------|-------------------|
| ▼ <input type="checkbox"/> | 1 | 3  | Test_10000_ACL_5_objects | 1                 |
| ▼ <input type="checkbox"/> | 2 | 6  | Test_10000_ACL_5_objects | 1                 |
| ^ <input type="checkbox"/> | 3 | 5  | Test_10000_ACL_5_objects | 1                 |

| № | Тип  | Источник пакета | Порт источника | Получатель пакета | Порт получателя | Протокол |  |
|---|------|-----------------|----------------|-------------------|-----------------|----------|--|
| 1 | Deny | 1.1.1.3/32      | 0-0            | 2.2.1.3/32        | 1002-1002       | TCP      |  |

Порядковый номер

|                            |   |   |                            |   |
|----------------------------|---|---|----------------------------|---|
| ▼ <input type="checkbox"/> | 4 | 7 | Test_10000_ACL_5_objects   | 1 |
| ▼ <input type="checkbox"/> | 5 | 4 | Test_10000_ACL_5_objects   | 1 |
|                            | 6 | 2 | Service-Permit-Not-Blocked | 1 |

Порядковый номер

ЭКРАН•М

< >

Информационная панель

Конфигурация

Модули

Система

Подчинённые ПАК

Резервные копии

Пользователи

Мониторинг

Сервисы

Правила трафика

Отчеты и журналы

Внешние системы

Песочница

Антивирус (ClamAV)

Система

sterra sterra

Зоны интерфейсов

eth1

N/A

Подключите модуль, перетащив его сюда

Удалить

eth2

40 Gbit/s

Подключите модуль, перетащив его сюда

Удалить

eth3

40 Gbit/s

UNC

Удалить

eth7

1 Gbit/s

Подключите модуль, перетащив его сюда

Удалить

eth6

10 Gbit/s

Подключите модуль, перетащив его сюда

Удалить

eth4

1 Gbit/s

Подключите модуль, перетащив его сюда

Удалить

Перетащите интерфейс сюда

Нераспределённые зоны

eth0

N/A

WAF COB DPI

Удалить

eth5

10 Gbit/s

Подключите модуль, перетащив его сюда

Удалить

Перетащите интерфейс сюда

Нераспределённые интерфейсы

LAN / WAN

Экран-М

WAN

eth0 eth5

LAN

eth1 eth2 eth3

eth7 eth6 eth4

© «С-Терра СиЭсПи», 2025

29

## [ События, отчёты и контроль ]

*Всё, что нужно для анализа инцидентов и отчётности по безопасности*

- Конструктор отчётов  
*(создание настраиваемых отчётов по событиям, трафику и инцидентам)*
- Подробное логирование событий безопасности  
*(все действия фиксируются на устройстве для анализа и формирования отчётов)*
- Совместимость с внешними системами  
*(передача событий REST API)*
- Гибкий экспорт событий безопасности  
*(CSV, JSON)*
- Поддержка стандартов экспортируемых форматов  
*(включая выгрузку в формате ГЦМ для взаимодействия с ГосСОПКА)*
- Поиск и фильтрация по событиям в интерфейсе  
*(быстрый доступ к нужной информации)*

Мониторинг

Сервисы

Правила трафика

Отчеты и журналы

Трафик

Настройка логирования

Журнал антивируса

Журнал песочницы

События безопасности

Действия администраторов

Журнал авторизации

ГЦМ ГосСОПКА

Конструктор отчетов

Syslog

Внешние системы

Маршруты

ID

Поиск

| ID ↑ | Выбран | Тип |
|------|--------|-----|
| 0    | ✓      | S   |
| 1    | ✓      | K   |
| 2    | ✗      | C   |
| 3    | ✓      | C   |
| 4    | ✓      | C   |

Настройка отображения

Выбрать все

Пользователи

☒ Действия с пользователями

☐ Пользователи сети

☒ Журнал авторизации

☐ Все пользователи сети

Сервисы

☐ Маршруты

☐ FRR config маршрутизации

☐ События статической маршрутизации

☐ Сетевые интерфейсы

Правила трафика

☐ События WAF

☐ События безопасности WAF

☐ История изменений COB

☐ События безопасности COB

☒ События безопасности песочницы

☐ События безопасности антивируса

Другие отчёты

☒ Действия администраторов

# ВЫГРУЗКА СОБЫТИЙ В ФОРМАТЕ ГЦМ ГОССОПКА



NAT

Firewall

Контроль приложений

WAF

Geo IP

Отчеты и журналы

Трафик

Настройка логирования

Журнал антивируса

Журнал песочницы

События безопасности

Действия администраторов

Журнал авторизации

ГЦМ ГосСОПКА

Конструктор отчетов

Syslog

Внешние системы

Песочница

ГЦМ ГосСОПКА

sterra sterra

Время начала  
07/07/2025, 05:51 PM

Время конца  
07/08/2025, 05:51 PM

Выборка  
1000

Отобразить

ID Модуля  
40

Тип сообщения

Поиск

Скачать

| Тип сообщения | ID-модуля | ID-сенсора   | Время               | ID-атаки | IP-клиента | IP-хоста  | Протокол | Порт атакующего узла | Порт атакуемого узла | Версия правила | Модуль |
|---------------|-----------|--------------|---------------------|----------|------------|-----------|----------|----------------------|----------------------|----------------|--------|
| 1             | 40        | 401234500890 | 08.07.2025 17:25:12 | 3400050  | 268477217  | 805348129 | 6        | 51213                | 80                   | 1              | 1      |
| 1             | 40        | 401234500890 | 08.07.2025 17:25:12 | 3400050  | 268499640  | 805370552 | 6        | 30953                | 80                   | 1              | 1      |
| 1             | 40        | 401234500890 | 08.07.2025 17:25:12 | 3400050  | 268449619  | 805320531 | 6        | 44916                | 80                   | 1              | 1      |
| 1             | 40        | 401234500890 | 08.07.2025 17:25:12 | 3400050  | 268456509  | 805327421 | 6        | 55589                | 80                   | 1              | 1      |
| 1             | 40        | 401234500890 | 08.07.2025 17:25:12 | 3400050  | 268440984  | 805311896 | 6        | 2802                 | 80                   | 1              | 1      |
| 1             | 40        | 401234500890 | 08.07.2025 17:25:12 | 3400050  | 268456500  | 805327412 | 6        | 30035                | 80                   | 1              | 1      |
| 1             | 40        | 401234500890 | 08.07.2025 17:25:12 | 3400050  | 268437536  | 805308448 | 6        | 8164                 | 80                   | 1              | 1      |
| 1             | 40        | 401234500890 | 08.07.2025 17:25:12 | 3400050  | 268458219  | 805329131 | 6        | 4762                 | 80                   | 1              | 1      |
| 1             | 40        | 401234500890 | 08.07.2025 17:25:12 | 3400050  | 268466838  | 805337750 | 6        | 28961                | 80                   | 1              | 1      |

Разработка нового релиза Экран-М с расширенным функционалом

## [ Экран-М новые релизы в разработке ]



## [ Защита ]



Многофункциональный  
межсетевой экран уровня сети  
вместе с ГОСТ-шифрованием



**Расширенная  
функциональность**

Сделаем на одном устройстве

NGFW

WAF

DPI

IDS / IPS

Sandbox

ГОСТ VPN

## [ Преимущества подхода ]

- 🌐 Многофункциональный межсетевой экран
- 📄 Поддержка ГОСТ-шифрования
- 💰 Экономия на закупках и обслуживании
- 🔧 Упрощение архитектуры сети

## Март

- Начало испытаний Экран-М 1.0 в Испытательной Лаборатории ФСТЭК

## Июль

- Расширение линейки аппаратных платформ
- Управление трафиком на уровне пользователей
- Автоматизация реакций на инциденты через API
- Скрипты переноса
- Расписание действия правил МЭ
- Расширенный DNS анализ
- Категория фильтрации

## Дальнейшее развитие продукта

### Разработка и выпуск новых релизов Экран-М

- Расшифровка и инспекция трафика SSL/TLS путем подмены сертификата
- Реализация управления скоростью трафика для конкретного пользователя или группы
- Расширение способов взаимодействия с системами управления инцидентами SOAR
- Персонализированные журналы для групп событий
- Отложенная установка политик межсетевого экранирования (расписание действия правил МЭ)
- Мобильный клиент

## Февраль

- SNMP мониторинг
- Увеличение производительности

## Май

- PPPOE
- Реализация полной инспекции трафика SSL / TLS

## Сентябрь

- Завершение сертификации Экран-М 1.0

- Поддержка передачи статистики по протоколу NetFlow во внешние системы
- Виртуальные контексты с отдельными ресурсами, таблицами маршрутизации и политиками фильтрации

## [ Отдел по работе с партнёрами ]



**partner@s-terra.ru**

Сотрудничество с С-Терра - развитие партнёрской сети и совместных инициатив

## [ Отдел по работе с клиентами ]



**sales@s-terra.ru**

Коммерческие условия и приобретение продукции

## [ Отдел технического консалтинга ]



**presale@s-terra.ru**

Технические консультации при выборе решения и в процессе пилотирования

## [ Отдел клиентского сервиса ]



**support@s-terra.ru**

Техническая поддержка по приобретённым решениям и платформам

# СПАСИБО ЗА ВНИМАНИЕ!

