КОД безопасности

Континент 4:

Автоматизация процессов

FW/UTM/IPS/RA/VPN/Antivirus/Proxy

КОД безопасности

О продукте

Континент 4

Универсальное устройство корпоративного уровня для всесторонней защиты сети (UTM) с поддержкой алгоритмов ГОСТ

Предназначен для решения следующих задач:

- Централизованная защита периметра корпоративной сети
- Сегментация внутренней сети
- Предотвращение сетевых вторжений
- Контроль приложений (L7-фильтрация трафика)
- URL-фильтрация
- Организация защищенного удаленного доступа

КОД безопасности

NGFW Континент 4

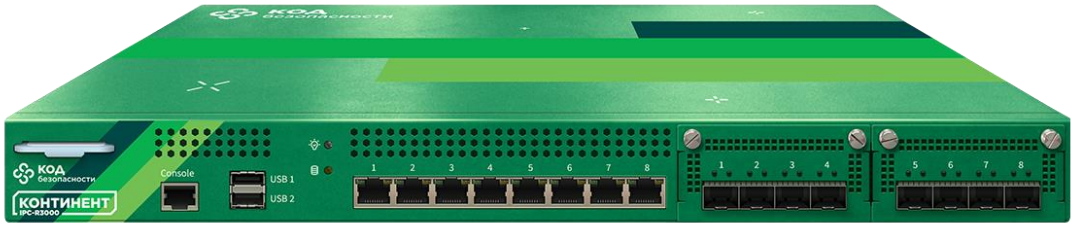
КШ — Криптошлюз (КШ)

КК — Криптокоммутатор (КК)

Детектор атак (ДА)

Центр управления сетью (ЦУС)

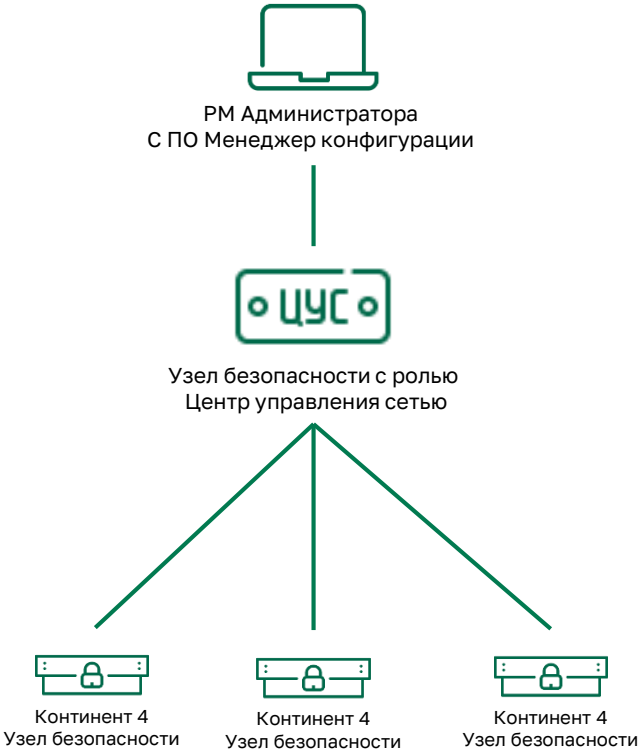
Узел безопасности (УБ)

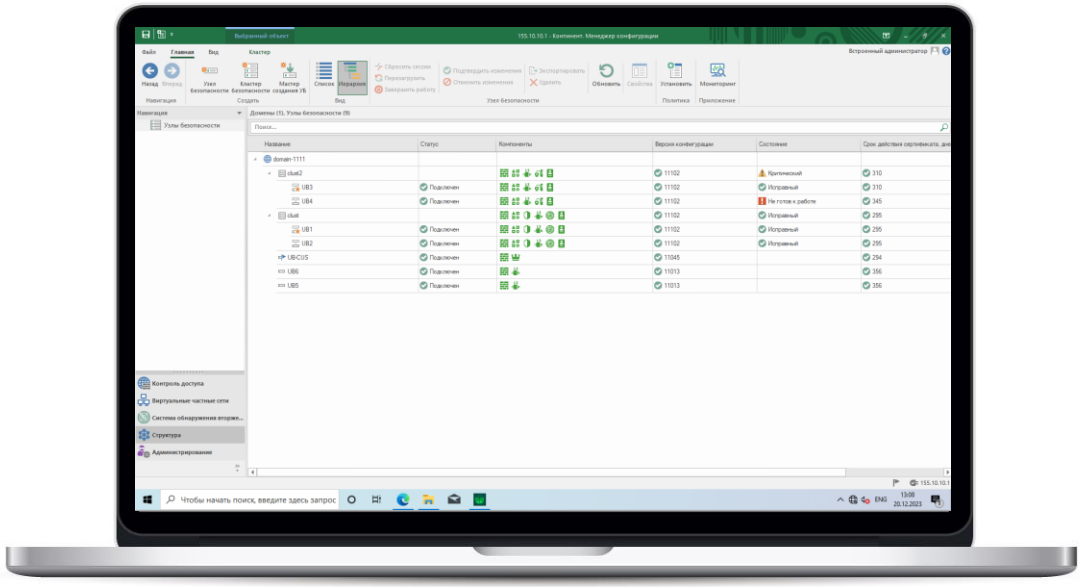


FW	IPS	App control	L2 VPN	L3 VPN	MGMT	Transparent Proxy
Threat Intelligence	Log	URL Filtering	User Identity	Antivirus	GeoIP	Explicit Proxy

КОД безопасности

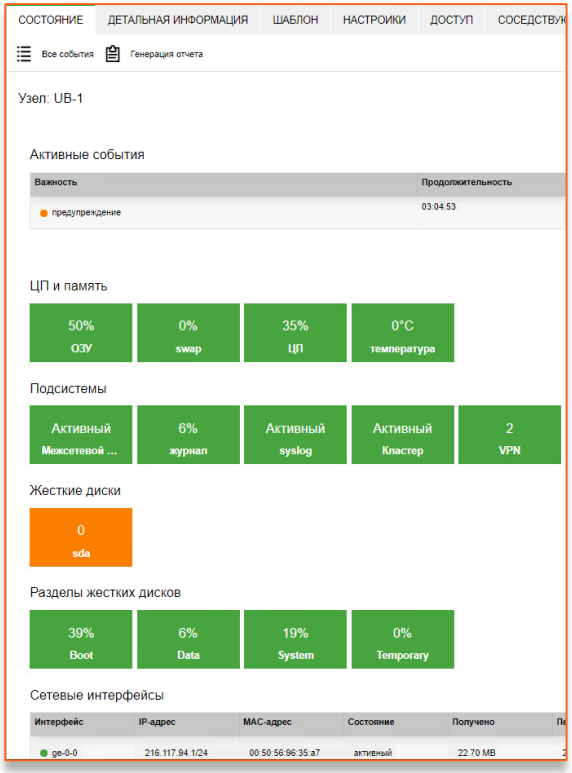
Управление

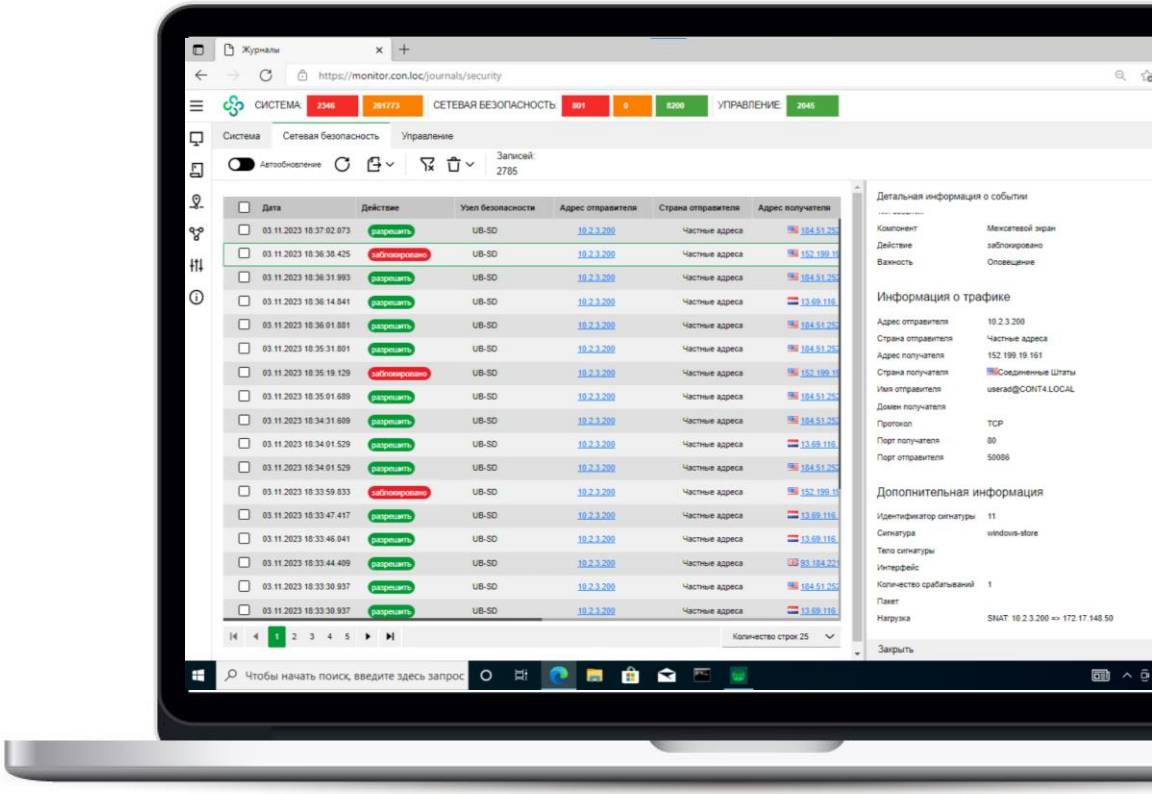




КОД безопасности

Веб-мониторинг





КОД безопасности

Система распространения обновлений

Сервер обновлений

Адрес: https://scupsrv.securitycode.ru

Имя пользователя: test_user

Пароль: ••••••••

Компоненты

Обновление ПО
Версия: 4.1.9.1844
Последний поиск обновления:
Запланированное обновление: Никогда
Расписание

Вендорские правила БРП
Версия: 4.1.9.148
Последний поиск обновления: 14.12.2023 11:00
Запланированное обновление: 15.12.2023 05:00
Расписание

Категории SkyDNS
Версия: Отсутствует
Последний поиск обновления:
Запланированное обновление: Никогда
Расписание

Фиды Threat Intelligence
Версия: Отсутствует
Последний поиск обновления:
Запланированное обновление: Никогда
Расписание

База хэшей Kaspersky
Версия: Отсутствует
Последний поиск обновления:
Запланированное обновление: Никогда
Расписание

Исключения Web/FTP-фильтрации
Версия: 4.1.7.1
Последний поиск обновления:
Запланированное обновление: Никогда
Расписание

База стран GEO/IP
Версия: Отсутствует
Последний поиск обновления:
Запланированное обновление: Никогда
Расписание

Название	Обновление ПО				Контрольная сумма	Дата установки...	Вендорски
	Версия	Предыдущая версия	Дата выпуска	Дата установки			Версия
dsf					0000000000000000		
node-1000	4.1.9-2585	4.1.7-1525	05.04.2024 08:00	12.07.2024 12:08	EE5396FAF8DD0E06	09.09.2024 11:43	
ub2	4.1.9-2585	4.1.7-1525			EE5396FAF8DD0E06	25.07.2024 03:57	
ub4	4.1.9-2585	4.1.7-1525			EE5396FAF8DD0E06	13.08.2024 17:28	
ub22	4.1.9-2585				EE5396FAF8DD0E06	13.08.2024 17:27	
UTM1	4.1.9-2585		05.04.2024 08:00	12.07.2024 15:24	EE5396FAF8DD0E06	30.09.2024 11:49	

Репозиторий обновлений

Версия	Тип	Дата выпуска	Размер, Кбайт	Резервное обновление	Описание
4.1.9.2585	Обновление ПО	05.04.2024 08:00	391 440		Обновление ПО
4.1.9.301	Вендорские правила БРП	18.07.2024 07:16	37 936		Обновление БРП
4.1.9.10848	База хэшей Kaspersky	29.09.2024 03:11	78 604		База хэшей Kaspersky
4.1.9.8338	Фиды Threat Intelligence	29.09.2024 08:22	182 090		Фиды Threat Intelligence
4.1.9.69	Категории SkyDNS	22.09.2024 21:19	1 487 955		Обновление Web/Ftp фильтров
4.1.9.2	Исключения Web/FTP-фильтрации	21.08.2024 01:10	2		Исключения Web/FTP фильтрации
4.1.9.72	База стран GEO/IP	25.09.2024 12:54	56 052		Список стран и IP адресов GeoIP

Расписание

Обновлять по расписанию Вкл.

- С периодом
- Единоразово
- Еженедельно по расписанию

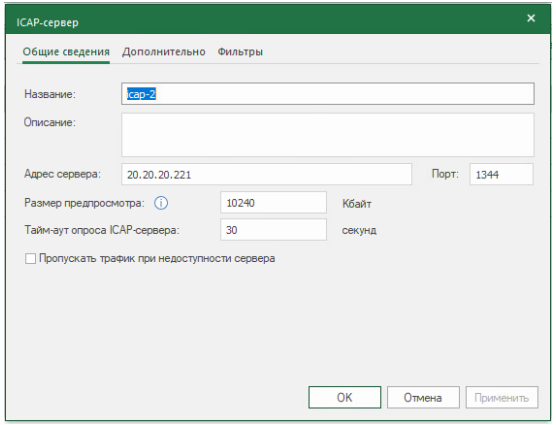
Даты обновления:

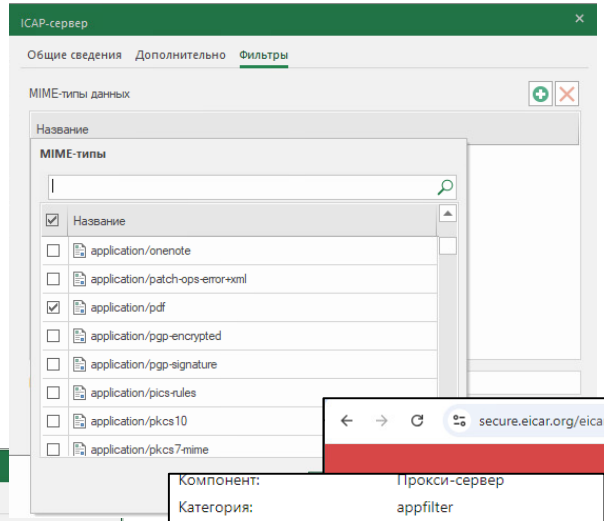
Старт	Пн	Вт	Ср	Чт	Пт	Сб	Вс
12:25	☑	☑	☑	☑	☑	☑	☑

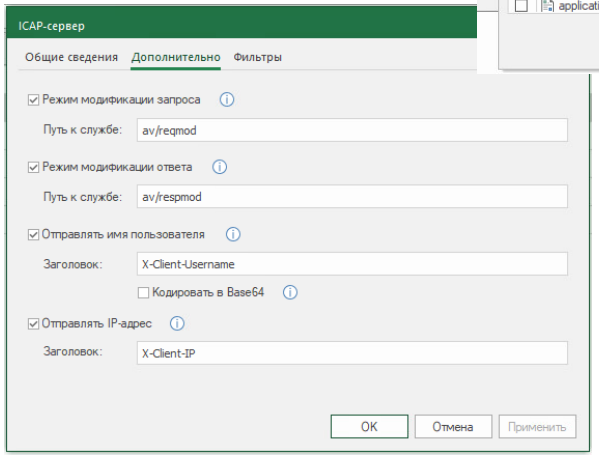
OK Отмена

КОД безопасности

Интеграция по ICAP

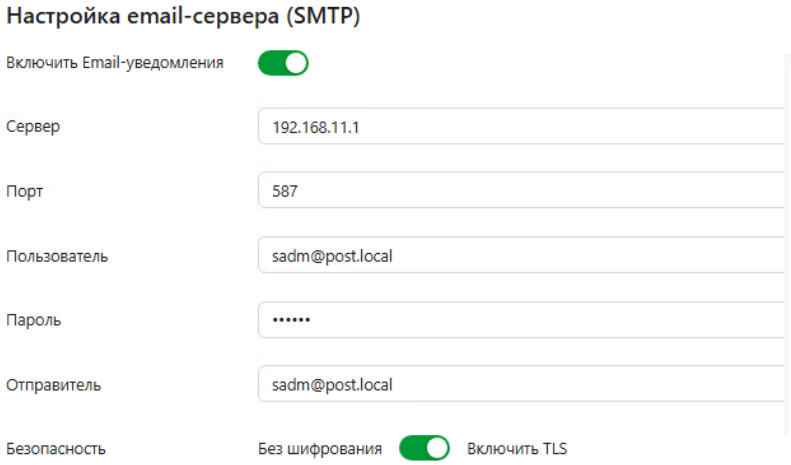


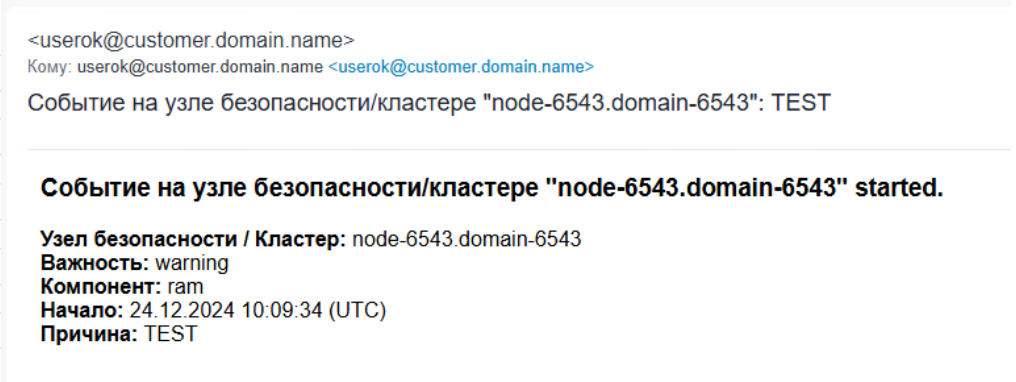




КОД безопасности

Уведомление\Мониторинг





SNMP

RFC1213-MIB

CONTINENT-SNMP-MIB

КОД безопасности

Инструменты автоматизированной работы администратора

Инструменты автоматизации работы администратора:

- Генерация правил МСЭ и NAT
- Генерация логических интерфейсов VLAN
- Экспорт конфигурации в сторонние системы
- Экспорт конфигурации в сторонние ЦУС
- Установка политики по расписанию
- Создание бэкапов по расписанию
- Импорт объектов IoC от вендора R-Vision
- Импорт объектов IoC от вендора Security-Vision
- Создание правил фильтрации и трансляции

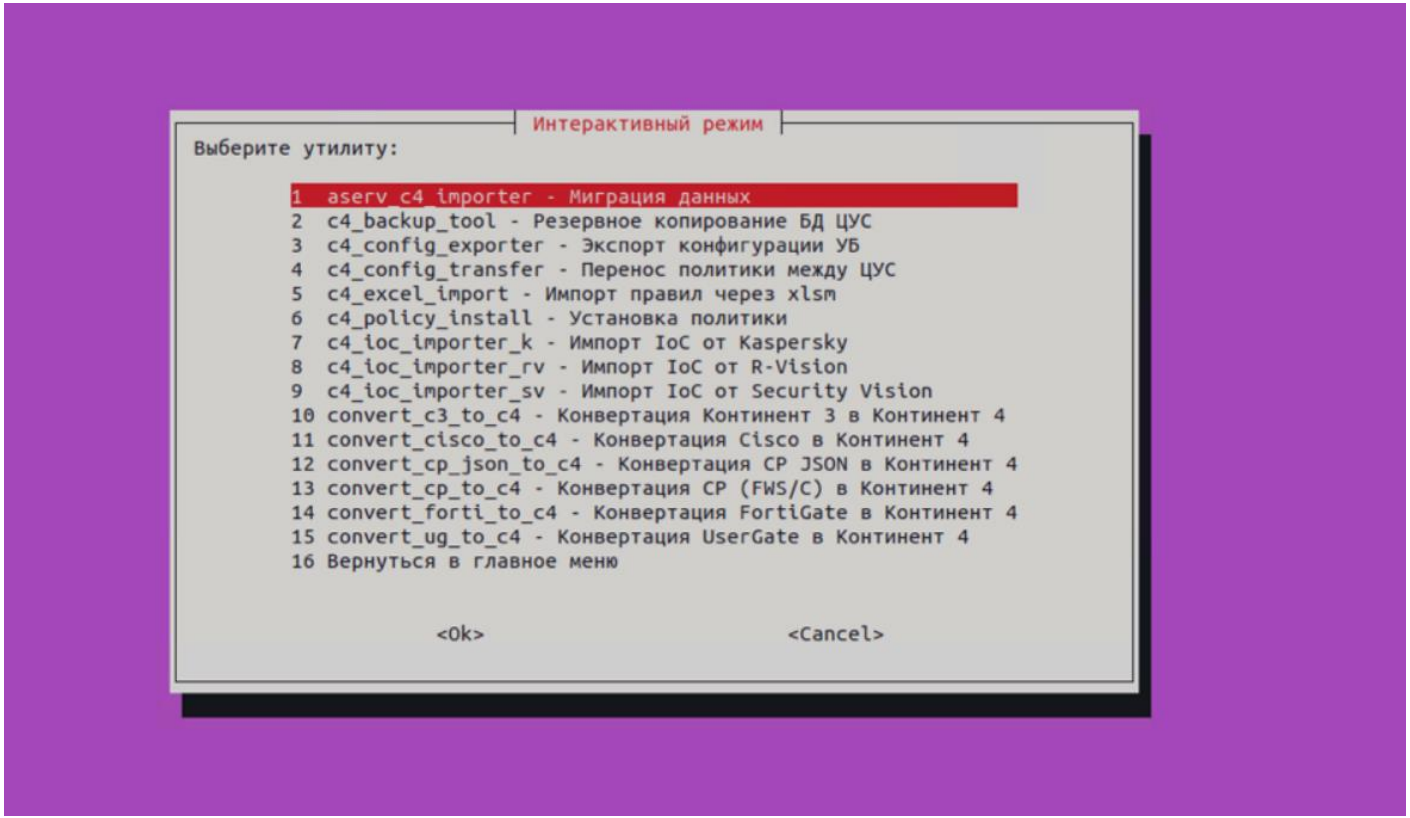
Инструменты автоматизированной миграции:

- Миграция с Check Point
- Миграция с FortiGate
- Миграция с Cisco ASA
- Миграция с Palo Alto
- Миграция с Континент 3
- Миграция данных с СД Континент 3 на СД Континент 4

Преимущество	Ценность
• API для работы с Континент 4 • Автоматизация процессов администрирования	Снижает нагрузку на команду администраторов

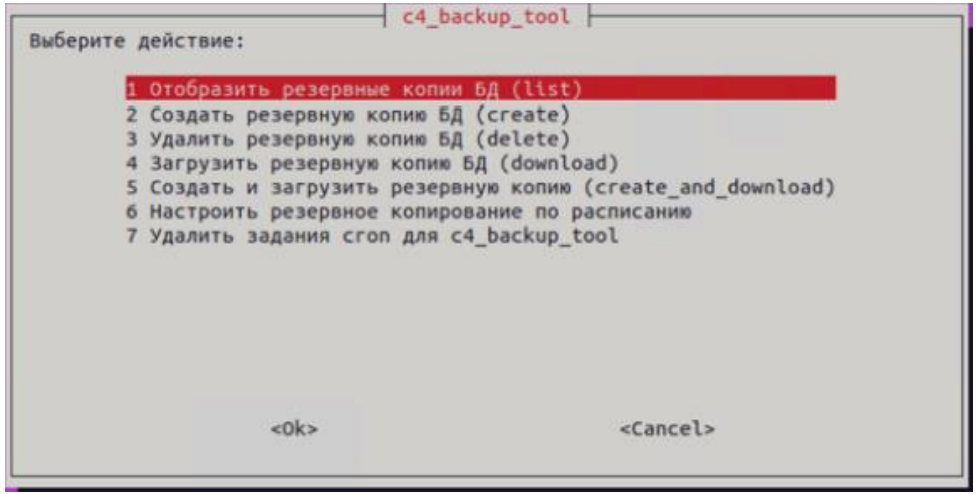
КОД безопасности

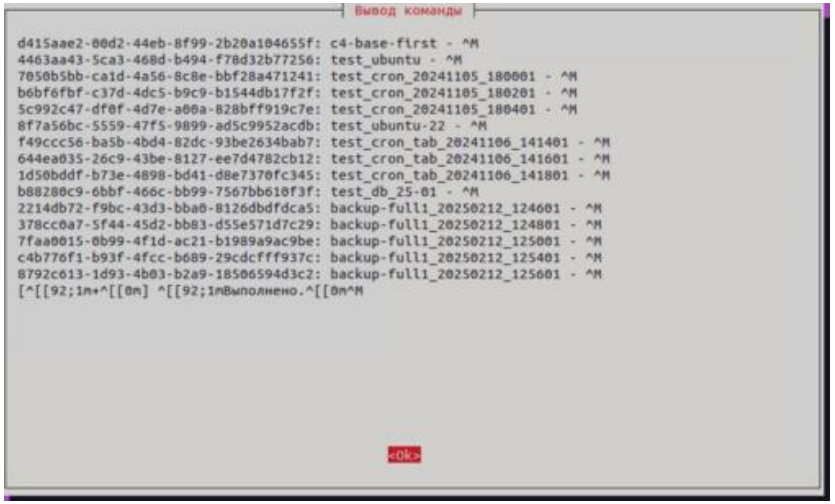
Сборка Утилит в docker



КОД безопасности

Резервное копирование (c4_backup_tool)



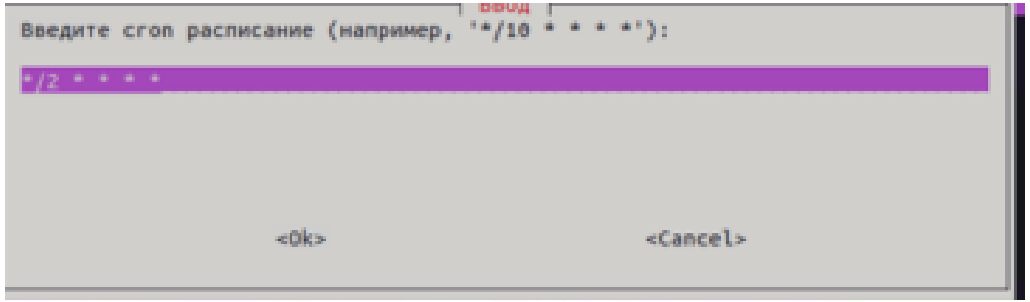


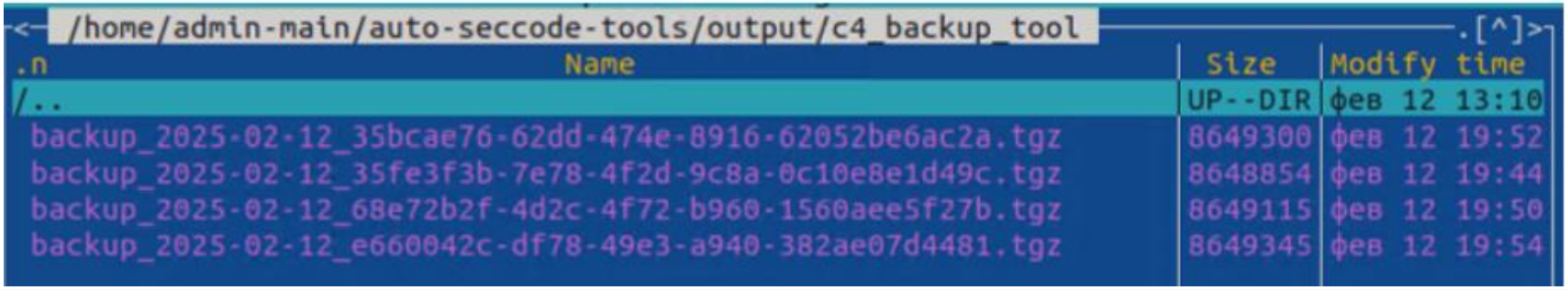
Поиск...

T...	Название	Время создания	Размер, Кбайт	Конфигурация	Настройки мониторинга	Данные мониторинга и аудита
	test_create	12.02.2025 16:39:19	8 446	●	●	
	backup-full1_20250212_125401	12.02.2025 12:48:30	8 444	●	●	

КОД безопасности

Резервное копирование (c4_backup_tool)





Резервные копии (18)

Поиск...

Т...	Название	Время создания	Размер, Кбайт	Конфигурация	Настройки мониторинга	Данные мониторинга и аудита
	test_cron_20250212_165401	12.02.2025 16:48:29	8 446	●	●	
	test_cron_20250212_165201	12.02.2025 16:46:30	8 446	●	●	
	test_cron_20250212_165001	12.02.2025 16:44:30	8 446	●	●	

КОД безопасности

Автоматизация миграции

- Прямой импорт политик Check Point, FortiGate, Cisco
- Импорт политик с Palo Alto и Juniper через промежуточный импорт в Check Point
- Миграция с Континент 3

Репозиторий – https://github.com/itseccode/c4_tools
Телеграм бот – https://t.me/STEPLOGIC_NetCalc_bot

КОД безопасности

Автоматизация миграции

itseccode Update patch_notes.txt

aserv_c4_importer	Add files via upload
c4_backup_tool	Update README.md
c4_config_exporter	Update README.md
c4_config_transfer	Update README.md
c4_ioc_importer_rv	Update README.md
c4_ioc_importer_sv	Update README.md
c4_lib	Add files via upload
c4_policy_install	Update README.md
c4_rules_maker	Update README.md
c4_vlan_maker	Update README.md
c4_xls_rules_maker	Add files via upload
convert_c3_to_c4	Update README.md
convert_cisco_to_c4	Add files via upload
convert_cp_json_to_c4	Update README.md
convert_cp_to_c4	Update README.md

4 months ago

Континент 4 - Инструменты

Важно! Последние изменения представлены в файле `patch_notes.txt`.

Репозиторий содержит инструменты для решения различных сервисных задач при использовании продукта Континент 4:

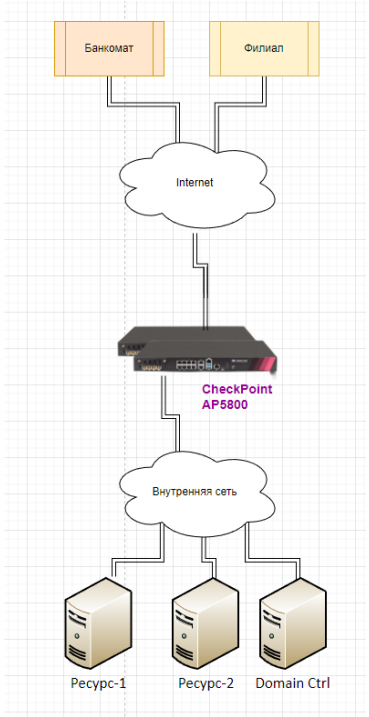
Инструмент	Назначение	Формат	Комментарий
`c4_lib`	Библиотека для работы с API Континент 4	Online	Нет
`c4_config_exporter`	Инструмент для экспорта конфигурации УБ для сторонних compliance-систем	Online	Только совместно с `c4_lib`
`c4_rules_maker`	Инструмент для генерации правил по заданным директивам	Online	Только совместно с `c4_lib`
`c4_vlan_maker`	Инструмент для генерации логических интерфейсов VLAN по заданному списку	Online	Только совместно с `c4_lib`
`c4_xls_rules_maker`	Инструмент для создания правил фильтрации (FW) и трансляции (NAT) по заданному шаблону	Online	Только совместно с `c4_lib`, в том числе для миграции данных из Palo Alto Networks
`c4_backup_tool`	Инструмент для создания и выгрузки резервной копии БД ЦУС	Online	Только совместно с `c4_lib`

КОД безопасности

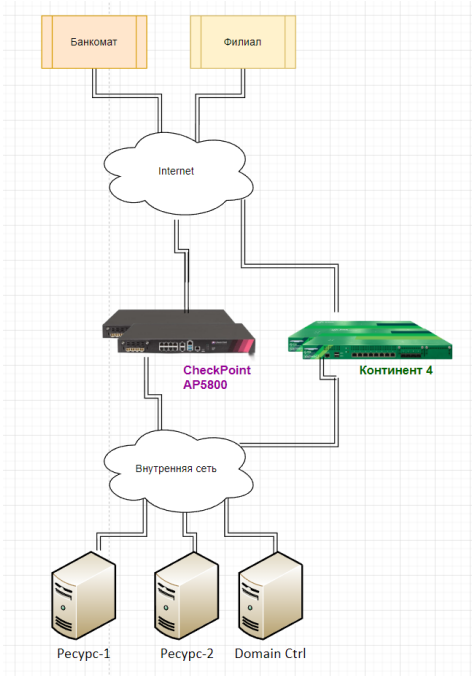
Переход с CheckPoint на Континент 4

КОД безопасности

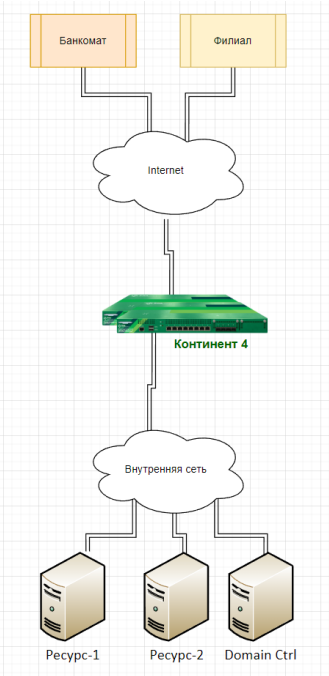
Переход с CheckPoint на Континент 4



1



2



3

КОД безопасности

Переход с CheckPoint на Континент 4

Этапы

Выгрузка файлов конфигурации с **Check Point**

Преобразование файлов конфигурации **Check Point** в формат **Континент 4**

Импорт политик и объектов в **Континент 4**

КОД безопасности

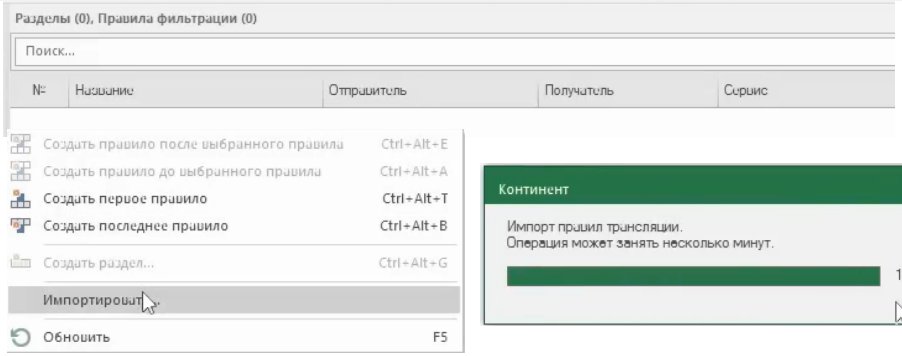
Переход с CheckPoint на Континент 4

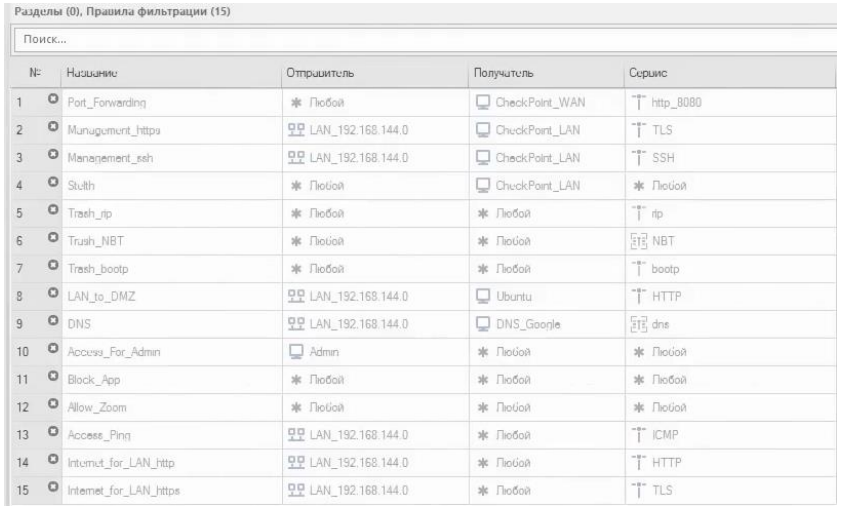
```
['00fa9e43-f5ae-0f65-e053-08241dc22da2'], 'domain': {'uid': '41e821a0-3720-11e3-aa6e-0800200c9fde', 'domain-type': 'domain', 'name': 'SMC User'}, 'content-negate': False,
 'name': 'Allow App', 'time': ['97aeb369-9aea-11d5-bd16-0090272ccb30'], 'install-on': ['6c488338-8eec-4103-ad21-cd461ac2c476'], 'action-settings': {'enable-identity-capti
ve-portal': False}, 'custom-fields': {'field-1': '', 'field-2': '', 'field-3': ''}}
2024-02-21 16:32:58 INFO     Сформирован отчёт: for_cont/report.txt
2024-02-21 16:32:58 INFO     Файл: for_cont/import-Standard_objects-fw.json
2024-02-21 16:32:58 INFO        В промежуточном файле:
2024-02-21 16:32:58 INFO                Сетевые объекты: 11
2024-02-21 16:32:58 INFO                Группы сетевых объектов: 1
2024-02-21 16:32:58 INFO                Сервисы: 7
2024-02-21 16:32:58 INFO                Группы сервисов: 2
2024-02-21 16:32:58 INFO                Временные интервалы: 0
2024-02-21 16:32:58 INFO                Правила фильтрации: 7
2024-02-21 16:32:58 INFO                Правила трансляции: 0
2024-02-21 16:32:58 INFO     Выходной файл найден, перезапись
2024-02-21 16:32:58 INFO     Записан файл: for_cont/import-Standard_objects-fw.json
2024-02-21 16:32:58 INFO        Успешно:
2024-02-21 16:32:58 INFO                Сетевые объекты: 7
2024-02-21 16:32:58 INFO                Группы сетевых объектов: 1
2024-02-21 16:32:58 INFO                Сервисы: 6
2024-02-21 16:32:58 INFO                Группы сервисов: 2
2024-02-21 16:32:58 INFO                Временные интервалы: 0
2024-02-21 16:32:58 INFO                Правила фильтрации: 7
2024-02-21 16:32:58 INFO                Правила трансляции: 0
2024-02-21 16:32:58 INFO        С предупреждениями:
2024-02-21 16:32:58 INFO                Сетевые объекты: 0
2024-02-21 16:32:58 INFO                Группы сетевых объектов: 0
2024-02-21 16:32:58 INFO                Сервисы: 0
2024-02-21 16:32:58 INFO                Группы сервисов: 0
2024-02-21 16:32:58 INFO                Временные интервалы: 0
2024-02-21 16:32:58 INFO                Правила фильтрации: 3
2024-02-21 16:32:58 INFO                Правила трансляции: 0
2024-02-21 16:32:58 INFO        С ошибками:
2024-02-21 16:32:58 INFO                Сетевые объекты: 0
2024-02-21 16:32:58 INFO                Группы сетевых объектов: 0
2024-02-21 16:32:58 INFO                Сервисы: 0
2024-02-21 16:32:58 INFO                Группы сервисов: 0
2024-02-21 16:32:58 INFO                Временные интервалы: 0
2024-02-21 16:32:58 INFO                Правила фильтрации: 0
2024-02-21 16:32:58 INFO                Правила трансляции: 0
2024-02-21 16:32:58 INFO        Итого:
2024-02-21 16:32:58 INFO                Сетевые объекты: 11
2024-02-21 16:32:58 INFO                Группы сетевых объектов: 1
2024-02-21 16:32:58 INFO                Сервисы: 7
2024-02-21 16:32:58 INFO                Группы сервисов: 2
2024-02-21 16:32:58 INFO                Временные интервалы: 0
2024-02-21 16:32:58 INFO                Правила фильтрации: 7
2024-02-21 16:32:58 INFO                Правила трансляции: 0
root@admin1-virtual-machine:/home/admin1/migration#
```

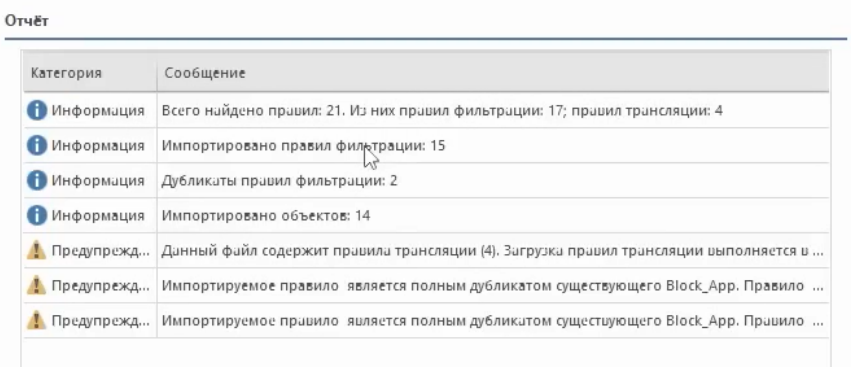
```
root@admin1-virtual-machine:/home/admin1/migration# python3 convert_cp_json_to_c4.py
usage:

python convert_cp_json_to_c4.py [-h] -i INPUT INPUT [-o OUTPUT_PATH]
                                [--log LOG] [--name NAME]
                                [--num_rule NUM_RULE]

Преобразование правил Check Point R80/ R80.X/ R81/ R81.X (Show Package Tool) в Континент 4.

options:
  -h, --help            Показать текущее сообщение помощи и выйти.
  -i INPUT INPUT, --input INPUT INPUT
                        Пути до файлов с объектами и правилами для преобразования
  -o OUTPUT_PATH, --output_path OUTPUT_PATH
                        Путь до папки для выходного файла
  --log LOG             Имя файла логирования
  --name NAME           Имя выходного файла
  --num_rule NUM_RULE   Ограничение по количеству правил в файле.

example: python convert_cp_json_to_c4.py -i input_objects_file_path.json input_rules_file_path.json -o output_folder_pat
h

root@admin1-virtual-machine:/home/admin1/migration# python3 convert_cp_json_to_c4.py -i Standard_objects.json Network-Ma
nagement_server.json -o for_cont
```

КОД безопасности

Добавление файла конфигурации







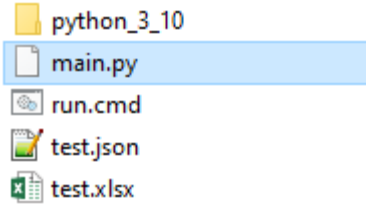
КОД безопасности

Дорогой дневник, пишу тебе правила Firewall

	A	B	C	D	E	F
1	name	rule_action	src	dst	Port	Protocol
2	Rule 1	block	16.34.0.0/16	48.177.0.1/32	59262	tcp
3						
4						
5						

Python:

```
import json
import openpyxl module
import openpyxl
```



КОД безопасности

Any-any-any-deny

```
[
      {
            "description": "Второе Правило для примера",
        "name": "any-any-deny",
        "is_enabled": false,    ##  отвечает за вкл\выкл правила
        "passips": false,
          "service": [],     ## «Любой» в Сервисе
        "is_inverse_src": "false",
        "is_inverse_dst": "false",
        "rule_action": "block",    ## Отвечает за Пропустить\Заблокировать
        "logging": false,    ## Отвечает за логирование
      "src":  [],     ## «Любой» в Отправителях
      "dst":  [],    ## «Любой» в Получателях
      "params": [] ## Временной интервал – Всегда
      }
]
```

32	any-any-deny	✱ Любой	✱ Любой	✱ Любой	✱ Любое
Отбросить	✱ Не задан	— Выкл	✱ Всегда	— Нет	— Нет	✱ Везде	Второе Правило для при...

КОД безопасности

КиберАльянс

Многофакторная

MULTIFACTOR
Avanpost
КОМПАНИЯ ИНДИД
Аладдин
КОМПАНИЯ АКТИВ

Балансировка нагрузки

ЦИФРОВЫЕ РЕШЕНИЯ

Анализ правил

EFROS DEFENCE OPERATIONS
Нетхаб
SPACE-BIT

Микросегментация

vGate

Планируются в ближайшее время

Песочницы

positive technologies
AV SOFT
kaspersky

Индикаторы компрометации

kaspersky
Security Vision
CyberThreatTech
R-Vision
BI.ZONE

Удаленный доступ

MacOS
iOS
АВРОРА

Комплаенс-контроль

Континент ZTN клиент
Сакура

КОД безопасности

Развитие Континент 4

Версия 4.2

- ✓ Поддержка программного L3 VPN **IPsec ГОСТ** (ТК26)
- ✓ Поддержка L3 VPN **IPsec RSA** для построения туннелей со сторонним оборудованием (Cisco, Eltex и пр.)
- ✓ Поддержка протокола **RADIUS** и двухфакторной аутентификации для СД (проверка на Avanpost FAM и Aladdin JAS)
- ✓ Передача на внешний syslog сервер только выбранных журналов
- ✓ МК **без ОС Windows** (Linux/Wine)
- ✓ **GeoIP для** ограничения подключений к **СД** только из определенных стран

КОД безопасности

Спасибо за внимание!

info@securitycode.ru
www.securitycode.ru