

Континент 4:

Автоматизация процессов

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



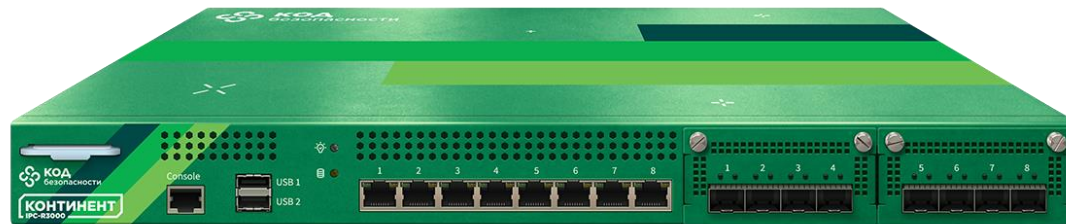
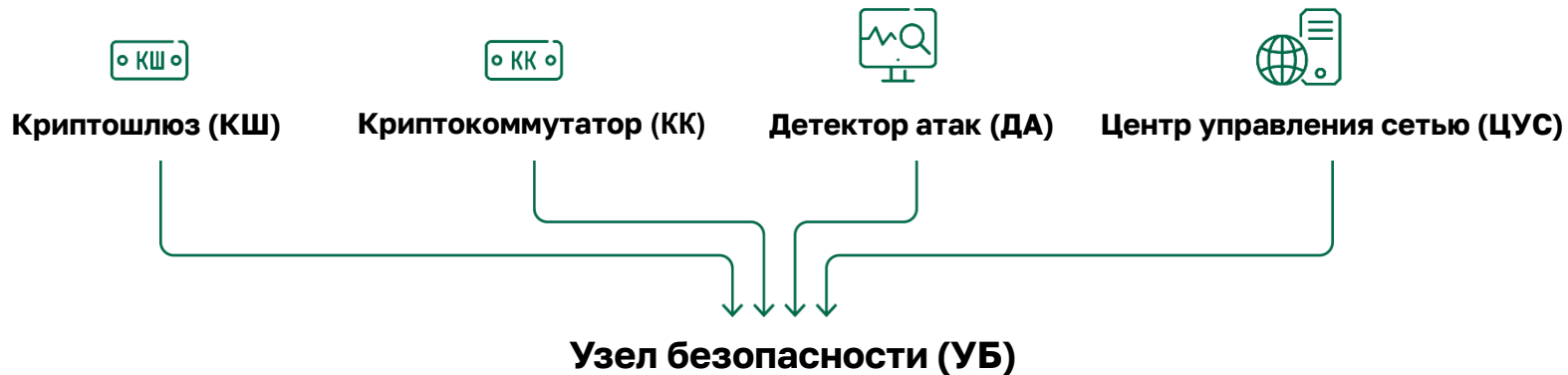
Континент 4

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

Предназначен для решения следующих задач:

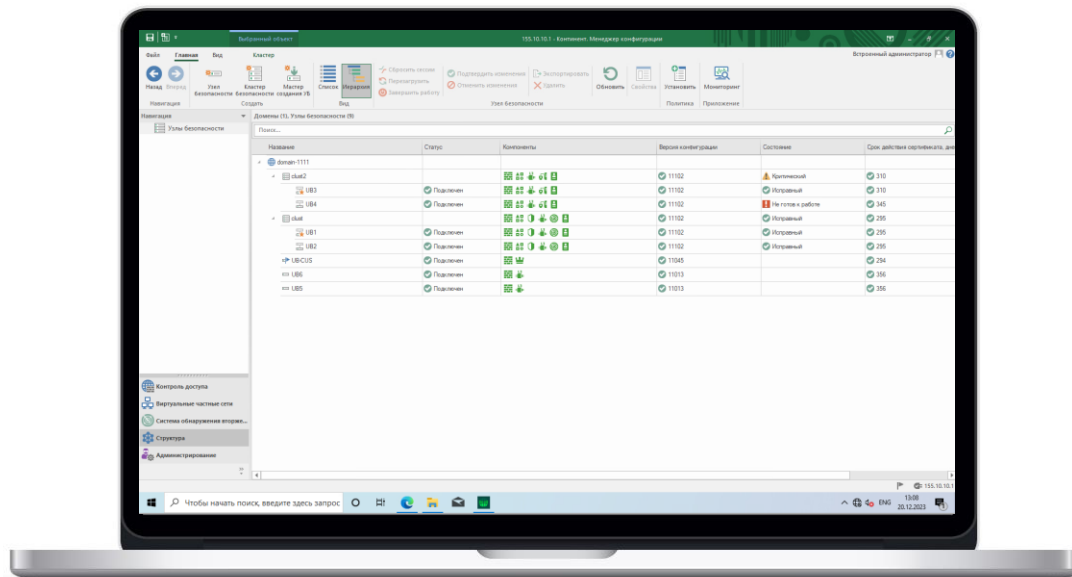
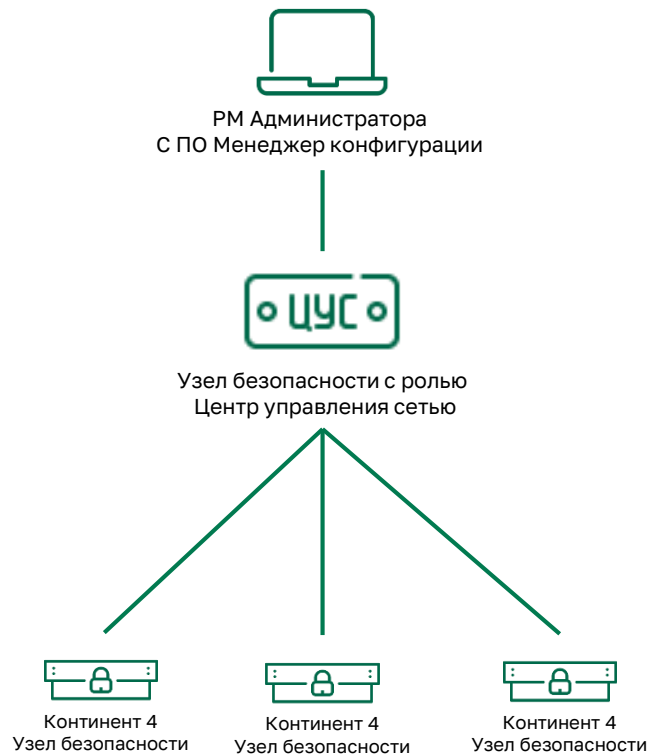
- ✓ Централизованная защита периметра корпоративной сети
- ✓ Сегментация внутренней сети
- ✓ Предотвращение сетевых вторжений
- ✓ Контроль приложений (L7-фильтрация трафика)
- ✓ URL-фильтрация
- ✓ Организация защищенного удаленного доступа

NGFW Континент 4



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





СОСТОЯНИЕ | ДЕТАЛЬНАЯ ИНФОРМАЦИЯ | ШАБЛОН | НАСТРОЙКИ | ДОСТУП | СОСЕДСТВУ

Все события | Генерация отчета

Узел: UB-1

Активные события

Важность	Продолжительность
предупреждение	03.04.53

ЦП и память

50% ОЗУ	0% swp	35% ЦП	0°C температура
---------	--------	--------	-----------------

Подсистемы

Активный Межсетевой ...	6% журнал	Активный suxlog	Активный Кластер	2 VPN
-------------------------	-----------	-----------------	------------------	-------

Жесткие диски

0 sda

Разделы жестких дисков

39% Boot	6% Data	19% System	0% Temporary
----------	---------	------------	--------------

Сетевые интерфейсы

Интерфейс	IP-адрес	MAC-адрес	Состояние	Получено
ge-0-0	216.117.94.1/24	00:50:56:96:35:a7	активный	22.70 MB

Журналы | <https://monitor.con.tcc/journals/security>

СИСТЕМА 2546 | 261773 | СЕТЕВАЯ БЕЗОПАСНОСТЬ 801 | 0 | 8200 | УПРАВЛЕНИЕ 2045

Система | Сетевая безопасность | Управление

Автообновление | Залить: 2785

Дата	Действие	Узел безопасности	Адрес отправителя	Страна отправителя	Адрес получателя
03.11.2023 18:37:02.073	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:36:38.425	заблокировать	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:36:31.993	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:36:14.041	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:36:01.881	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:35:31.801	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:35:19.129	заблокировать	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:35:01.609	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:34:31.609	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:34:01.529	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:34:01.529	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:33:59.833	заблокировать	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:33:47.417	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:33:46.041	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:33:44.409	разрешить	UB-SD	10.2.3.200	Частные адреса	93.104.272
03.11.2023 18:33:38.937	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161
03.11.2023 18:33:38.937	разрешить	UB-SD	10.2.3.200	Частные адреса	152.199.19.161

Количество строк 25

Детальная информация о событии

Компонент: Межсетевой экран
 Действие: заблокировано
 Важность: Оповещение

Информация о трафике

Адрес отправителя: 10.2.3.200
 Страна отправителя: Частные адреса
 Адрес получателя: 152.199.19.161
 Страна получателя: Соединенные Штаты
 Имя отправителя: usenat@CONT4.LOCAL
 Домен получателя: usenat@CONT4.LOCAL
 Протокол: TCP
 Порт получателя: 80
 Порт отправителя: 50086

Дополнительная информация

Идентификатор сигнатуры: 11
 Сигнатура: windows-store
 Тело сигнатуры:
 Интерфейс:
 Количество срабатываний: 1
 Плав:
 Настройка: SNAT: 10.2.3.200 => 172.17.148.50

Залить

Чтобы начать поиск, введите здесь запрос

Система распространения обновлений








Сервер обновлений

Адрес:

Имя пользователя:

Пароль:

Компоненты

- 
Обновление ПО
 Версия: 4.1.9.1844
 Последний поиск обновления:
 Запланированное обновление: Никогда
- 
Вендорские правила БРП
 Версия: 4.1.9.148
 Последний поиск обновления: 14.12.2023 11:00
 Запланированное обновление: 15.12.2023 05:00
- 
Категории SkyDNS
 Версия: Отсутствует
 Последний поиск обновления:
 Запланированное обновление: Никогда
- 
Фиды Threat Intelligence
 Версия: Отсутствует
 Последний поиск обновления:
 Запланированное обновление: Никогда
- 
База хэшей Kaspersky
 Версия: Отсутствует
 Последний поиск обновления:
 Запланированное обновление: Никогда
- 
Исключения Web/FTP-фильтрации
 Версия: 4.1.7.1
 Последний поиск обновления:
 Запланированное обновление: Никогда
- 
База стран GEO/IP
 Версия: Отсутствует
 Последний поиск обновления:
 Запланированное обновление: Никогда

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
 Ежедневно по расписанию

Даты обновления: + ✕

Старт	Пн	Вт	Ср	Чт	Пт	Сб	Вс
12:25	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Интеграция по ICAP

ICAP-сервер

Общие сведения Дополнительно Фильтры

Название:

Описание:

Адрес сервера: Порт:

Размер предпросмотра: Кбайт

Тайм-аут опроса ICAP-сервера: секунд

Пропускать трафик при недоступности сервера

OK Отмена Применить

ICAP-сервер

Общие сведения Дополнительно Фильтры

MIME-типы данных

Название:

MIME-типы

- application/onenote
- application/patch-ops-error+xml
- application/pdf
- application/pgp-encrypted
- application/pgp-signature
- application/pics-rules
- application/pkcs10
- application/pkcs7-mime

ICAP-сервер

Общие сведения Дополнительно Фильтры

Режим модификации запроса

Путь к службе:

Режим модификации ответа

Путь к службе:

Отправлять имя пользователя

Заголовок:

Кодировать в Base64

Отправлять IP-адрес

Заголовок:

OK Отмена Применить

secure.eicar.org/eicar.com

Access denied

Компонент: Прокси-сервер

Категория: appfilter

Действие: заблокировано

Важность: Тревога

Информация о трафике

Адрес отправителя: 20.20.20.20

Страна отправителя: Соединенные Штаты

Адрес получателя: 89.238.73.97

Страна получателя: Германия

Имя отправителя:

Домен получателя:

Протокол: HTTP(S)

Порт отправителя: 56817

Порт получателя: 443

Дополнительная информация

Идентификатор сигнатуры: 0

Сигнатура: 1

Тело сигнатуры:

Интерфейс:

Пакет:

Нагрузка: GET https://secure.eicar.org/eicar.com (text/html)

Количество срабатываний: 1

berky Web Traffic Security

requested page cannot be provided

s: https://secure.eicar.org/eicar.com

Настройка email-сервера (SMTP)

Включить Email-уведомления

Сервер

Порт

Пользователь

Пароль

Отправитель

Безопасность Без шифрования Включить TLS

<userok@customer.domain.name>

Кому: userok@customer.domain.name <userok@customer.domain.name>

Событие на узле безопасности/кластере "node-6543.domain-6543": TEST

Событие на узле безопасности/кластере "node-6543.domain-6543" started.

Узел безопасности / Кластер: node-6543.domain-6543

Важность: warning

Компонент: ram

Начало: 24.12.2024 10:09:34 (UTC)

Причина: TEST

SNMP

RFC1213-MIB

CONTINENT-SNMP-MIB

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

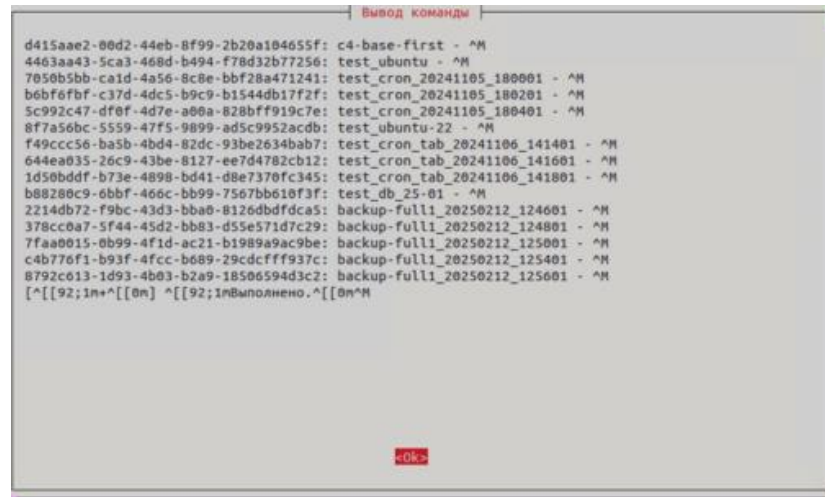
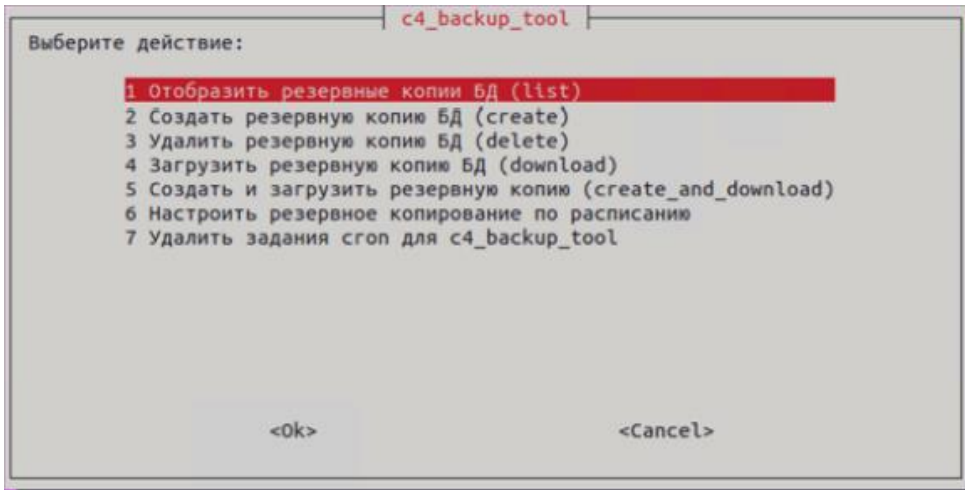
Преимущество	Ценность
<ul style="list-style-type: none">• API для работы с Континент 4• Автоматизация процессов администрирования	Снижает нагрузку на команду администраторов







Сборка Утилит в docker

```
Интерактивный режим
Выберите утилиту:
1 aserv c4 importer - Миграция данных
2 c4_backup_tool - Резервное копирование БД ЦУС
3 c4_config_exporter - Экспорт конфигурации УБ
4 c4_config_transfer - Перенос политики между ЦУС
5 c4_excel_import - Импорт правил через xlsm
6 c4_policy_install - Установка политики
7 c4_ioc_importer_k - Импорт IoC от Kaspersky
8 c4_ioc_importer_rv - Импорт IoC от R-Vision
9 c4_ioc_importer_sv - Импорт IoC от Security Vision
10 convert_c3_to_c4 - Конвертация Континент 3 в Континент 4
11 convert_cisco_to_c4 - Конвертация Cisco в Континент 4
12 convert_cp_json_to_c4 - Конвертация CP JSON в Континент 4
13 convert_cp_to_c4 - Конвертация CP (FWS/C) в Континент 4
14 convert_forti_to_c4 - Конвертация FortiGate в Континент 4
15 convert_ug_to_c4 - Конвертация UserGate в Континент 4
16 Вернуться в главное меню

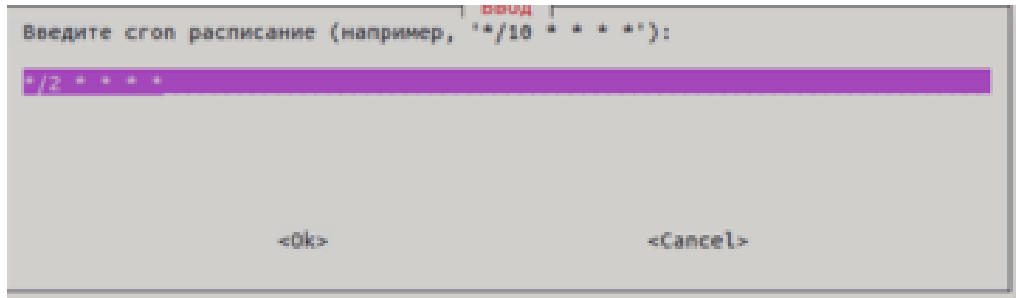
<Ok> <Cancel>
```

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			

Резервное копирование (c4_backup_tool)












```

<- /home/admin-main/auto-seccode-tools/output/c4_backup_tool .[^]>
.n
Name Size Modify time
/.. UP--DIR фев 12 13:10
backup_2025-02-12_35bcae76-62dd-474e-8916-62052be6ac2a.tgz 8649300 фев 12 19:52
backup_2025-02-12_35fe3f3b-7e78-4f2d-9c8a-0c10e8e1d49c.tgz 8648854 фев 12 19:44
backup_2025-02-12_68e72b2f-4d2c-4f72-b960-1560aee5f27b.tgz 8649115 фев 12 19:50
backup_2025-02-12_e660042c-df78-49e3-a940-382ae07d4481.tgz 8649345 фев 12 19:54
    
```

Резервные копии (18)

Поиск...

T...	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			



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



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

Континент 4 - Инструменты

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

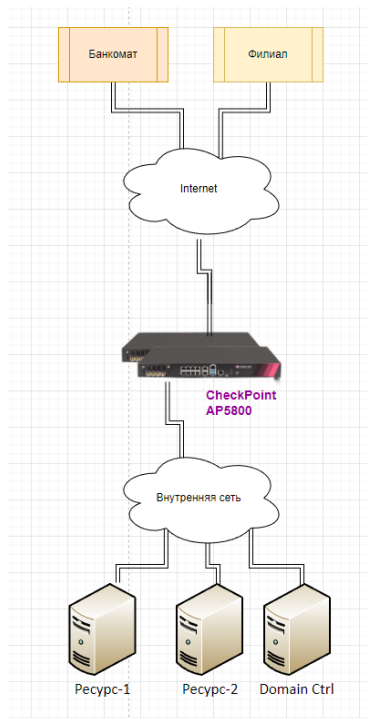
Репозиторий содержит инструменты для решения различных сервисных задач при использовании продукта Континент 4:

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

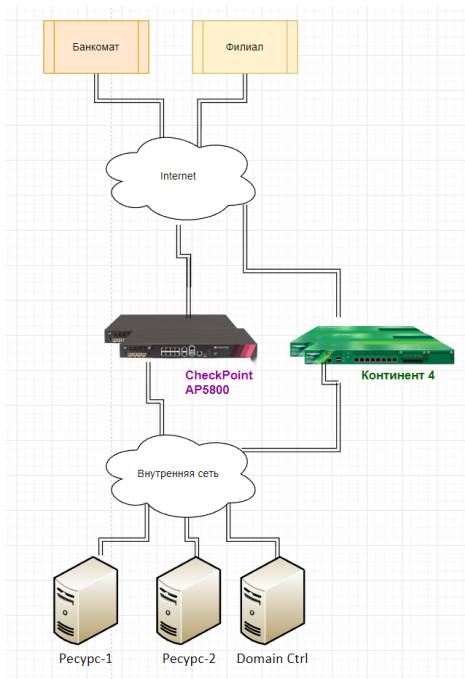
4 months ago

Переход с CheckPoint на Континент 4

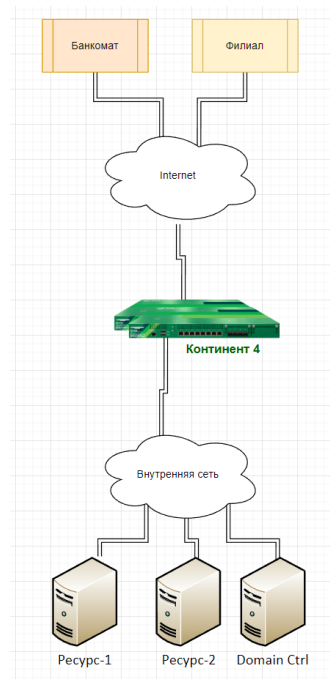




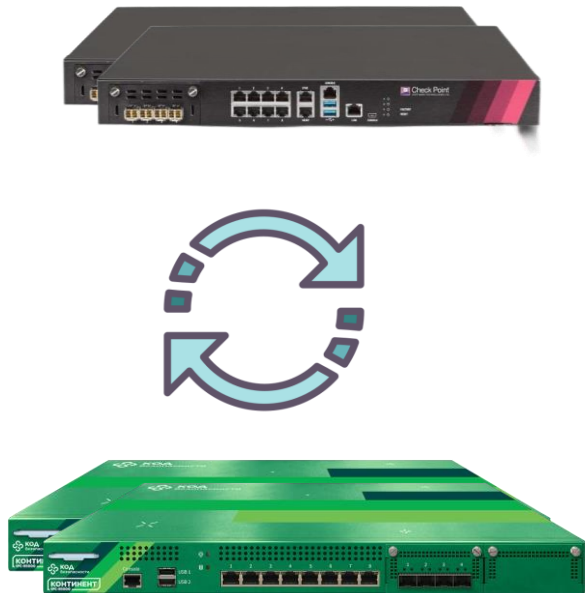
1



2



3



Этапы



Выгрузка файлов конфигурации с **Check Point**

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

Импорт политик и объектов в **Континент 4**

```
['00fa9e43-f5ae-0f65-e053-00241dc22da2'], 'domain': {'uid': '41e021a0-3720-11e3-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-captive-portal': False}, 'custom-fields': {'field-1': '', 'field-2': '', 'field-3': ''}}
```

```
2024-02-21 16:32:58 INFO Сформирован отчет: 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_path

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

Добавление файла конфигурации

Разделы (0), Правила фильтрации (0)

Поиск...

N:	Название	Отправитель	Получатель	Скрипт
	Создать правило после выбранного правила			Ctrl+Alt+E
	Создать правило до выбранного правила			Ctrl+Alt+A
	Создать первое правило			Ctrl+Alt+T
	Создать последнее правило			Ctrl+Alt+B
	Создать раздел...			Ctrl+Alt+G
	Импортировать			
	Обновить			F5

Континент

Импорт правил трансляции.
Операция может занять несколько минут.

100 %



Разделы (0), Правила фильтрации (15)

Поиск...

N:	Название	Отправитель	Получатель	Скрипт
1	Port_Forwarding	* Любая	CheckPoint_WAN	http_8080
2	Management_https	LAN_192.168.144.0	CheckPoint_LAN	TLS
3	Management_ssh	LAN_192.168.144.0	CheckPoint_LAN	SSH
4	Slueth	* Любая	CheckPoint_LAN	* Любая
5	Trash_ip	* Любая	* Любая	ip
6	Trash_NBT	* Любая	* Любая	NBT
7	Trash_bootp	* Любая	* Любая	bootp
8	LAN_to_DMZ	LAN_192.168.144.0	Ubuntu	HTTP
9	DNS	LAN_192.168.144.0	DNS_Google	dns
10	Access_For_Admin	Admin	* Любая	* Любая
11	Block_App	* Любая	* Любая	* Любая
12	Allow_Zoom	* Любая	* Любая	* Любая
13	Access_Ping	LAN_192.168.144.0	* Любая	ICMP
14	Internet_for_LAN_http	LAN_192.168.144.0	* Любая	HTTP
15	Internet_for_LAN_https	LAN_192.168.144.0	* Любая	TLS

Отчёт

Категория	Сообщение
Информация	Всего найдено правил: 21. Из них правил фильтрации: 17; правил трансляции: 4
Информация	Импортировано правил фильтрации: 15
Информация	Дубликаты правил фильтрации: 2
Информация	Импортировано объектов: 14
Предупрежд...	Данный файл содержит правила трансляции (4). Загрузка правил трансляции выполняется и ...
Предупрежд...	Импортируемое правило является полным дубликатом существующего Block_App. Правило ...
Предупрежд...	Импортируемое правило является полным дубликатом существующего Block_App. Правило ...

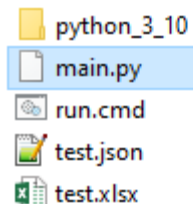
Дорогой дневник, пишу тебе правила Firewall

	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
```



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...

КиберАльянс

Многофакторная

MULTIFACTOR Avanpost
КОМПАНИЯ ИНДИД Алладдин
АКТИВ

Балансировка нагрузки

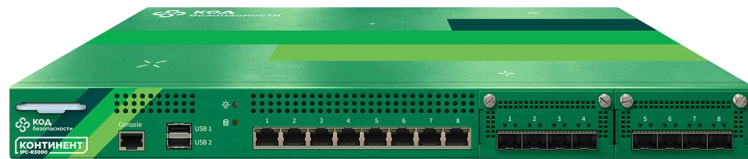
ЦИФРОВЫЕ РЕШЕНИЯ

Анализ правил

EFROS DEFENCE OPERATIONS Нетхаб
SPACE-BIT

Микросегментация

vGate



Песочницы

positive technologies AVSOFT
kaspersky

Индикаторы компрометации

kaspersky Security Vision
CyberThreatTech R-Vision
BI.ZONE

Удаленный доступ

Windows Linux MacOS
iOS Android ABPOPA

Комплаенс-контроль

Континент ZTN клиент
Сакура

Планируются
в ближайшее
время

Версия 4.2

- ✓ Поддержка программного L3 VPN **IPsec ГОСТ** (TK26)
- ✓ 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



Спасибо за внимание!

info@securitycode.ru
www.securitycode.ru

