# ОПТИМИЗИРУЕМ ПОЛИТИКИ, СОГЛАСУЕМ ДОСТУП, ИЩЕМ ДЫРЫ И ЗАСТАВЛЯЕМ, НАКОНЕЦ, РАБОТАТЬ NGFW (А НЕ ВАС)

REM,

# ОСНОВНЫЕ ЗАДАЧИ РЕШЕНИЙ КЛАССА NSPM

# **1**∃

Оптимизация политик Как эффективно анализировать и оптимизировать политики <u>безопасности?</u>

# Ê

#### Управление политиками

Как централизованно управлять правилами на МЭ разных вендоров?

# $\odot$

#### Мониторинг

Как контролировать состояние подключенных устройств?

# G

#### Контроль

Как контролировать изменения конфигураций устройств?

#### 

#### Мультивендорная реализация

Как интегрировать решения разных вендоров МЭ в систему управления?

# ?

#### Безопасность Как обеспечить необходимые уровень доступов и сетевой безопасности компании?

# <u>Ç</u>

#### Совместимость

Как интегрировать продукт в существующую инфраструктуру?



#### Ограничение прав

Как ограничить права доступа пользователей к устройствам?

# НОТА КУПОЛ.УПРАВЛЕНИЕ

Единый мультивендорный центр контроля, управления и оптимизации работы межсетевых экранов, UTM, NGFW

#### Ценность для клиента

- Ускорение и унификация настройки из единого интерфейса политик МЭ всех вендоров устройств, установленных в инфраструктуре компании
- + Видимость всех устройств МЭ в сети компании и своевременное нахождение неисправных
- Быстрый ввод в эксплуатацию новых сегментов сети с помощью клонирования конфигураций на одно или несколько устройств
- Полная видимость изменений политик на устройствах и возможность быстро найти устройство, политики которого нарушили какие-либо бизнес-процессы компании
- Оптимально настроенные политики безопасности во всей инфраструктуре компании и отсутствие политик, снижающих пропускную способность сети компании и ее защищенность

#### Функции

#### 

#### Мониторинг состояния всех установленных МЭ

Подключение и мониторинг состояния доступности подключенных устройств МЭ: UserGate, CheckPoint, Cisco ASA, Fortigate и др.

#### ଞ

#### Управление конфигурациями

Автобэкапирование конфигураций подключенных устройств, их клонирование на другие устройства, сравнение версий между собой и анализ

#### **厶**»

#### Интеграция с SIEM/SOAR

 $\exists \bigcirc \bot \bigcirc \bot \bigcirc | \mathsf{KAUOV}$ 

Отправка журналов событий продукта «НОТА | КУПОЛ. Управление» в сторонние системы по протоколу Syslog

#### 낹

## Управление политиками безопасности

Централизованный контроль и управление политиками / правилами МЭ вендоров: UserGate, CheckPoint, Cisco ASA и др.

#### Ŧ

## Оптимизация правил на всех устройствах

Выявление аномалий в правилах МЭ: избыточных, дублирующихся, теневых и других. Рекомендации по их оптимизации

#### Q

#### Администрирование

Предоставление прав доступа в систему локальным пользователям и из Active Directory / Astra Linux Directory. Управление парольной политикой. Журнал событий

# ЗАДАЧИ

## $\exists \Box \Box \Box | \mathsf{KAUOV}$

#### Когда актуально?

Анализ доступов

Оптимизация правил доступа

Оценка рисков несанкционированного доступа в действующей структуре

Согласованное изменение политик ИБ, контроль исполнения

Защита доступов ключевых бизнес-приложений

Выявление и устранение ошибок в инфраструктуре

Снижение нагрузки устройства до 30-50%

Устранение (изменение) опасных и потенциально опасных правил

Анализ изменений в доступе до внесения

Контроль доступности: платежных, биллинговых, финансовых приложений

# РОЛИ

# $\exists \Box \Box \Box | \mathsf{KAUOV}$

#### Сетевой инженер

(управляет устройствами автоматизация управления и настройки конфигурации сетевых устройств)

- Автоматизация управления (бэкапы, централизованная настройка, раскатка политик, оптимизация работы устройств)
- Приведение настроек в соответствие с политиками безопасности, предиктивная проверка внедрения планируемых изменений



#### **CISO** (контролер)

- Контроль инфраструктуры установленным политикам, отсутствию уязвимостей и/или возможности их эксплуатации, контроль сетевой инфраструктуры на соответствие политикам безопасности, автоматизация проверки
- Определение политик безопасности



#### Инженер ИБ

- Контроль и управление политиками на каждом отдельно взятом устройстве
- Контроль отсутствия уязвимостей и/или возможности их эксплуатации
- Определение зон безопасности и межсетевого взаимодействия

# АНАЛИЗ ПОЛИТИК



изменениям, происходящим на устройстве. Мы хотим, чтобы политики были настроены безопасно и оптимизированы



H C T C H C T C

#### АНАЛИЗ ПОЛИТИК

Н ∣ КА⊔ОV	Главная 🗲 Анализ политик 🗲 Сводка	3						义 Администратор
Управление	🗟 Анализ политик							0
🔓 Рабочий стол	Сводка Оптимизация Очис	стка Переупорядочивание	Глобальный поиск					
Список устройств	Выбор устройства	Всего правил	Политики Анализ политик от 19.06.2024 (	02:37:53 Обновить				
🌔 Конфигурации	UG test111111111 172.31.142.165	** 31	№ Название	Действие	Зона источника	Включено	Адрес источника	Зона назначения
а Анализ политик	Получите наглядное представление об прописанных в брандмауэре	о всех правилах,			Untrusted			
Отслеживание измен	Запрещающие правила	26			Trusted Cluster		BAD SEARCH BLA	
	Разрешающие правила	Как эффективно ана	ализировать и оптимизиров	ать политики	Linspection z		ENTENSYS_BLACK	Cluster
🧟 Администратор	Входящие правила брандмауэра	безопасности?	· · ·		-to-Site			
	Исходящие правила брандмауэра	В продукте НОТА КУ политик», который п	/ПОЛ.Управление предусмо позволяет посмотреть прав	трен раздел «Анали ила в различных	I <b>3</b> )MZ			DMZ
	Отключенные правила	категориях, выявить рекомендации по оп	ь существующие аномалии, ттимизации объектов и прае	а также получать зил.				Untrusted
	Правила с отключённым логированием	Для просмотра сфо в раздел «Анализ по	ормированных отчетов анал опитик» из меню спева.	иза необходимо пе	рейти <sup>it</sup>			Untrusted
	Разрешенные ANY-ANY правила		5 <u>VPN for Site-to-Site to Trusted and Untr</u>	usted Pазрешить	VPN for Site-to-Site			Untrusted Trusted
	Правила, разрешающие трафик любого сервиса без ограничений	5	6 <u>Allow trusted to untrusted</u>	И Разрешить	Trusted			Untrusted
	Двунаправленные правила	0	7 <u>Allow from DMZ to Untrusted</u>	И Разрешить	DMZ			Untrusted
			8 <u>trst</u>	🛛 Запретить				
			9 <u>test</u>	🛛 Запретить				
~			Найдено записей: <b>31</b>			~	< 1 из 1 р	> > 50 \

Н ∣ КА⊔ОИ	Главная 🗲 Анализ политик 🗲 Сводка								义 Администратор
Управление	🗟 Анализ политик								۲
Рабочий стол	Сводка Оптимизация Очист	гка Переупорядочивание	Глобальнь	ій поиск					
🔡 Список устройств	Выбор устройства	Всего правил	Политин	ки Анализ политик от 19.06.2024 02:37:53	Обновить				
🌔 Конфигурации	UG test1111111111172.31.142.165	** 31	Nº ⊦	азвание	Действие	Зона источника	Включено	Адрес источника	Зона назначения
FQ Анализ политик	Чтобы посмотреть о правил, необходимо устройство из списка	гчет по сводке выбрать а	1 1	23	🛛 Запретить	Untrusted VPN for remote acc Trusted Cluster Tunnel inspection z		BAD_SEARCH_BLA	Cluster
<u>С</u> Администратор	Разрешающие правила Входящие правила брандмауэра	2				Management DMZ VPN for Site-to-Site		ENTENSYS_BLACK	
	Исходящие правила брандмауэра	8	2 <u>v</u>	<u>vvvc</u>	🗴 Запретить	Cluster DMZ			DMZ
	Отилюченные правила	11	3 <u>E</u>	Block to botnets	🗴 Запретить	Trusted			Untrusted
	Правила с отключённым логированием	17	4 <u>E</u>	xample block RU RKN by IP list	🗴 Запретить	Trusted Management DMZ			Untrusted
	Разрешенные ANY-ANY правила	4	5 \	/PN for Site-to-Site to Trusted and Untrusted	Разрешить	VPN for Site-to-Site			Untrusted Trusted
	Правила, разрешающие трафик любого сервиса без ограничений	5	6 /	Allow trusted to untrusted	Разрешить	Trusted			Untrusted
	Двунаправленные правила	0	7 /	Allow from DMZ to Untrusted	Разрешить	DMZ			Untrusted
			8 <u>t</u>	rst	🛚 Запретить				
			9 <u>t</u>	est	<ul> <li>Запретить</li> </ul>				
~			Найдено	э записей: <b>31</b>			~	< 1 из 1 >	» 50 V

≓   КУПОЛ	Главная 🗲 Анализ политик 🗲 Сводка				🗙 Администратор
Управление	🗟 Анализ политик				0
П Рабочий стол	Сводка Оптимизация Очистка Переупорядочивание П	Глобальный поиск			
🔡 Список устройств	Выбор устройства	Политики Анализ политик от 19.06.2024 02:37:53	Обновить		
🕞 Конфигурации	UG test111111111 172.31.142.165 31 nar_1.1.2_ne_trogato	№ Название	Действие Зона источника	Включено Адрес источника	Зона назначения
Санализ политик           Отслеживание измен	172.31.142.95 внех правилах, КС 14.11 172.31.142.30 Сіsco ASA 172.31.142.14	1 123	Untrusted VPN for remote acc Trusted Cluster Запретить Tunnel inspection z	BAD_SEARCH_BLA	Cluster
Се Администратор	test     5       22.22.22.22     2       test2     2       23.23.23.23     2		Management DMZ VPN for Site-to-Site	ENTENSYS_BLACK	
	KC.b-8744.22.11 172.31.142.127 8	2 <u>vvvvc</u>	Sanpeтить Cluster DMZ		DMZ
		3 <u>Block to botnets</u>	Saпретить Trusted		Untrusted
	При нажатии появляется выпадающий список с подключенными устройствами. Также отображается статус доступности	4 Example block RU RKN by IP list	Тrusted Запретить Management DMZ	•	Untrusted
	и IP-адрес для каждого устройства	5 VPN for Site-to-Site to Trusted and Untrusted	✓ Разрешить VPN for Site-to-Site		Untrusted Trusted
	Правила, разрешающие трафик 5 любого сервиса без ограничений 5	6 Allow trusted to untrusted	Разрешить Trusted		Untrusted
	Двунаправленные правила О	7 Allow from DMZ to Untrusted	Разрешить DMZ		Untrusted
		8 <u>trst</u>	🗵 Запретить		
		9 <u>test</u>	🗙 Запретить		
«		Найдено записей: 31		« < 1 из 1 >	» 50 V

Н   КА⊔ОИ	Главная 🗲 Анализ политик 🗲 Сводка									Ş	2 Адм	инистратор
Управление	🗟 Анализ политик											۲
Рабочий стол	Сводка Оптимизация Очис	тка Переупорядочиван	ие	Глобальный поиск								
🔡 Список устройств	Выбор устройства	Всего правил	1	Политики Анализ политик от 20	.11.2024 14:0	08:20 Обновить						
🎝 Конфигурации	Cisco ASA 172.31.142.14	* 1397		Политика	Контекст	Nº	Действие	Включено	Источник	Назначение	Нал	аравление
न्तू Анализ политик	Контекст 🗸	Политики	_	OUTSIDE_access_in_1207241308	admin	Правило 1	Permit		any	ds_object_fqdn_v4 [fqdn]	↓	in
[о] Отслеживание измен	Получите наглядное представление обс прописанных в брандмауэре	всех правилах,		OUTSIDE_access_in_1207241308	admin	Правило 2	Permit		any	8.8.8.8	¥	in
	Запрещающие правила	651		OUTSIDE_access_in_1207241308	admin	Правило 3	× Deny		any	1.1.1.1	Ŷ	in
😂 Администратор	Разрешающие правила	746	. I	OUTSIDE_access_in_1207241308	admin	Правило 4	Permit		any	any	Ŷ	in
	r aspendine npasina	740	1	OUTSIDE_access_in_1207241308	admin	Правило 5	Permit		any	any	$\downarrow$	in
	Входящие правила брандмауэра	622		OUTSIDE_access_in_1207241308	admin	Правило 6	Permit		2001:4860:4860::8888	ds_group_1 [group]	¥	in ,
	Исходящие правила брандмауэра	566		OUTSIDE_access_in_1207241308	admin	Правило 7	× Deny		any	any	Ļ	in
	Отключенные правила	645		OUTSIDE_access_in_1207241308	admin	Правило 8	Permit		ds_group_1 [group]	ds_group_1 [group]	¥	in .
	Правила с отключённым погированием	682		OUTSIDE_access_in_1207241308	admin	Правило 9	Permit		any	any	¥	in
				OUTSIDE_access_in_1207241308	admin	Правило 10	Permit		any	any	¥	in .
	Разрешенные АNY-ANY правила	58		OUTSIDE_access_in_1207241308	admin	Правило 11	Permit		any	any	¥	in .
	Правила, разрешающие трафик любого сервиса без ограничений	26		OUTSIDE_access_in_1207241308	admin	Правило 12	Permit		Host-gVVzp825 [host]	Group-UcujmnLW [group]	¥	in
	Двунаправленные правила	72		OUTSIDE_access_in_1207241308	admin	Правило 13	× Deny		Host-gVVzp825 [host]	Host-NYbaeEQt [host]	Ļ	in
				OUTSIDE_access_in_1207241308	admin	Правило 14	× Deny	По	сле выбора устр	ойство можн	10	
				OUTSIDE_access_in_1207241308	admin	Правило 15	× Deny	отч	смотреть после, іет этого устрой	цний сформиј ства	ООВа	анный
~				Найдено записей: 1397					« ‹	1 из 28 >	»	50 🗸

Н   КАПОИ	Главная > Анализ политик > Сводка								🗙 Администратор
Управление	🗟 Анализ политик								۲
П Рабочий стол	Сводка Оптимизация Очистка Переупорядочивание	Глобальный поиск							
Список устройств	Выбор устройства Всего правил	Политики Анализ политик от 20	.11.2024 14:0	08:20 Обновить					> •••
🎝 Конфигурации	Cisco ASA 172.31.142.14	Политика	Контекст	Nº	Действие	Включено	Источник	Назначение	Направление
<b>-</b> Анализ политик	Контекст Conte Х ЛОЛИТИКИ У	OUTSIDE_access_in_1207241308	admin	Правило 1	Permit		any	ds_object_fqdn_v4 [fqdn]	↓ in ,
Отслеживание измен	☑ Context1 всех правилах,	OUTSIDE_access_in_1207241308	admin	Правило 2	Permit		any	8.8.8.8	↓ in ,
	admin 5	OUTSIDE_access_in_1207241308	admin	Правило 3	× Deny		any	1.1.1.1	↓ in ,
Са Администратор	Context2	OUTSIDE_access_in_1207241308	admin	Правило 4	Permit		any	any	↓ in ,
	0	OUTSIDE_access_in_1207241308	admin	Правило 5	<ul> <li>Permit</li> </ul>		any	any	↓ in 📊
	Можно выполнять фильтрацию	OUTSIDE_access_in_1207241308	admin	Правило 6	Permit		2001:4860:4860::8888	ds_group_1 [group]	↓in ¢
	полученных результатов	OUTSIDE_access_in_1207241308	admin	Правило 7	× Deny		any	any	↓ in ,
	по индивидуальным параметрам для вендора. Например, для Cisco	OUTSIDE_access_in_1207241308	admin	Правило 8	Permit		ds_group_1 [group]	ds_group_1 [group]	↓ in o
		OUTSIDE_access_in_1207241308	admin	Правило 9	<ul> <li>Permit</li> </ul>		any	any	↓in <sub>¢</sub>
	лопрованиси	OUTSIDE_access_in_1207241308	admin	Правило 10	Permit		any	any	Jµin ¢
	Разрешенные ANY-ANY правила 0	OUTSIDE_access_in_1207241308	admin	Правило 11	Permit		any	any	↓ in ,
	Правила, разрешающие трафик любого сервиса без ограничений 0	OUTSIDE_access_in_1207241308	admin	Правило 12	Permit		Host-gVVzp825 [host]	Group-UcujmnLW [group]	↓ in ,
	Двунаправленные правила 0	OUTSIDE_access_in_1207241308	admin	Правило 13	× Deny		Host-gVVzp825 [host]	Host-NYbaeEQt [host]	↓ in γ
		OUTSIDE_access_in_1207241308	admin	Правило 14	× Deny		Host-gVVzp825 [host]	Group-dCjF15mg [group]	↓ in γ
		OUTSIDE_access_in_1207241308	admin	Правило 15	× Deny		Group-56K6tKxk [group]	Group-1ErlGBdG [group]	↓ in v
~		Найдено записей: 1397					« «	1 из 28 >	» 50 V

Н   КА⊔ОУ	Главная 🗲 Анализ политик 🗲 Сводка									🗙 Администратор
Управление	🗟 Анализ политик									۲
Рабочий стол	Сводка Оптимизация Очистка Переупорядочивание	Глобальный поиск								
🔡 Список устройств	Выбор устройства Всего правил	Политики Разрешенные ANY-ANY прав	ила ×	Анализ политик от	20.11.2024 14	08:20 Обно	вить			> ···
р Конфигурации	Cisco ASA 172.31.142.14	Политика н	онтекст	Nº	Действие	Включено	Источник	Назначение	Направление	Сервис назначения
<b>FQ</b> Анализ политик	Контекст — Политики — —	OUTSIDE_access_in_1207241308 a	ıdmin	Правило 4	Permit		any	any	↓ in	👂 tcp
[о] Отслеживание измен	Получите наглядное представление обо всех правилах, прописанных в брандмауэре	OUTSIDE_access_in_1207241308 a	ıdmin	Правило 5	Permit		any	any	↓ in	🔗 icmp
	Запрешающие правида 651	OUTSIDE_access_in_1207241308 a	ıdmin	Правило 9	Permit		any	any	↓ in	PTCCPPUUDDPP [
Ç@ Администратор		OUTSIDE_access_in_1207241308 a	ıdmin	Правило 10	Permit		any	any	↓ in	PICMP_GROUP4_all
	Разрешающие правила 746	OUTSIDE_access_in_1207241308 a	ıdmin	Правило 11	Permit		any	any	↓ in	👂 service_group [grou
	Входящие правила брандмауэра 622	OUTSIDE_access_out_1207241313 a	ıdmin	Правило 1	Permit		any	any	↑ out	👴 tcp
	Истолящие позвила бозилматара 566	OUTSIDE_access_out_1207241313 a	ıdmin	Правило 2	Permit		any	any	↑ out	🔗 ip
	recodrighe nearring openging 500	OUTSIDE_access_out_1207241313 a	ıdmin	Правило 3	Permit		any	any	↑ out	👌 icmp
	Отключенные правила 645	OUTSIDE_access_out_1207241313 a	ıdmin	Правило 4	Permit		any	any	↑ out	tcp/tcp_80-1494 (8 1494)
	Правила с отключённым 682	OUTSIDE_access_out_1207241313 a	idmin	Правило 6	Permit		any	any	↑ out	👂 udp/udp_80 (80)
		OUTSIDE_access_out_1207241313 a	ıdmin	Правило 7	Permit		any	any	↑ out	🔗 tcp-udp-grp [group]
	Разрешенные Аму-Аму правила 58	OUTSIDE_access_out_1207241313 a	ıdmin	Правило 8	<ul> <li>Permit</li> </ul>		any	any	↑ out	👴 test_tcp_grp [group
	При нажатии на категорию	OUTSIDE_access_out_1207241313 a	idmin	Правило 9	Permit		any	any	↑ out	tcp/service_lt (<10)
	в инфографике результаты в отчете также фильтруются	inside_access_in_2005241349 a	Idmin	Правило 5	Permit		any	any	↓ in	👂 tcp
		inside_access_in_2005241349 a	ıdmin	Правило 8	Permit		any	any	↓ in	👂 icmp
		inside_access_in_2005241349 a	ıdmin	Правило 9	Permit		any	any	↓ in	👂 icmp6
		inside_access_in_2005241349 a	ıdmin	Правило 11	<ul> <li>Permit</li> </ul>		any	any	↓ in	👂 icmp/mobile-redire
«		Найдено записей: 58						« «	1 из 2	> >> 50 \

КАЦОЛ	Главная > Анализ политик > Сводка	3									🙁 Администратор
(правление	🗟 Анализ политик										0
бочий стол	Сводка Оптимизация Очис	тка Переупорядочивание	Глобальный поиск								
исок устройств	Выбор устройства	Всего правил	Политики Разрешенные ANY-ANY п	равила × Ана	ализ политик от	20.11.2024 14	:08:20 Обно	вить	ſ		
нфигурации	Cisco ASA 172.31.142.14	1397	Политика	Контекст N	0	Действие	Включено	Источник	Назі а	T XLSX	Экспорт >
низ политик	Контекст 🗸	Политики 🗸	OUTSIDE_access_in_1207241308	admin П	Іравило 4	<ul> <li>Permit</li> </ul>		any	any	⊥ ↓ ir	() Настройка столбцов
еживание измен	Получите наглядное представление обо	о всех правилах,	OUTSIDE_access_in_1207241308	admin П	Іравило 5	Permit		any	any	in	0 iomp
	-		OUTSIDE_access_in_1207241308	admin П	Іравило 9	Permit		any	any	Результа	аты анализа с учетом
шистратор	Запрещающие правила	651	OUTSIDE_access_in_1207241308	admin П	Іравило 10	Permit		any	any	фильтра в XLSX d	ции можно экспортиров рормате
нистратор	Разрешающие правила	746	OUTSIDE_access_in_1207241308	admin П	Іравило 11	Permit		any	any	↓ in	👂 service_group [grou
	Входящие правила брандмауэра	622	OUTSIDE_access_out_1207241313	admin П	Іравило 1	Permit		any	any	↑ out	🔊 tcp
			OUTSIDE_access_out_1207241313	admin П	Іравило 2	Permit		any	any	↑ out	👴 ip
	Исходящие правила брандмауэра	566	OUTSIDE_access_out_1207241313	admin П	Іравило З	Permit		any	any	↑ out	🔗 icmp
	Отключенные правила	645	OUTSIDE_access_out_1207241313	admin П	Іравило 4	Permit		any	any	↑ out	tcp/tcp_80-1494 (8 1494)
	Правила с отключённым	682	OUTSIDE_access_out_1207241313	admin П	Іравило б	Permit		any	any	↑ out	👴 udp/udp_80 (80)
	логированием		OUTSIDE_access_out_1207241313	admin П	Іравило 7	Permit		any	any	↑ out	🔊 tcp-udp-grp [group]
	Разрешенные ANY-ANY правила	58	OUTSIDE_access_out_1207241313	admin П	Іравило 8	Permit		any	any	↑ out	👴 test_tcp_grp [group
	Правила, разрешающие трафик любого сервиса без ограничений	26	OUTSIDE_access_out_1207241313	admin П	Іравило 9	Permit		any	any	↑ out	😔 tcp/service_lt (<10)
		70	inside_access_in_2005241349	admin П	Іравило 5	Permit		any	any	↓ in	👴 tcp
	двунаправленные правила	72	inside_access_in_2005241349	admin П	Іравило 8	Permit		any	any	↓ in	😌 icmp
			inside_access_in_2005241349	admin П	Іравило 9	Permit		any	any	↓ in	🔗 icmp6
			inside_access_in_2005241349	admin П	іравило 11	Permit		any	any	↓ in	👂 icmp/mobile-redire
//			Найдено записей: <b>58</b>						«	< 1	из 2 > » 50 ~

≓   КА⊔ОV	Главная > Анализ политик > Сводка										义 Администратор
Управление	🗟 Анализ политик										۲
Рабочий стол	Сводка Оптимизация Очис	тка Переупорядочивание	Глобальный поиск								
🔡 Список устройств	Чтобы посмотреть вь	іявленные	Политики Разрешенные ANY-ANY п	равила ×	Анализ политик от	т 20.11.2024 14	:08:20 <mark>Обн</mark> о	овить			> ···
🌔 Конфигурации	аномалии в правилах перейти на вкладку «С	, необходимо Оптимизация»	Политика	Контекст	Nº	Действие	Включено	Источник	Назначение	Направление	Сервис назначения
<b>FQ</b> Анализ политик			OUTSIDE_access_in_1207241308	admin	Правило 4	Permit		any	any	↓ in	🔑 tcp
Отслеживание измен	Получите наглядное представление обо прописанных в брандмауэре	всех правилах,	OUTSIDE_access_in_1207241308	admin	Правило 5	Permit		any	any	↓ in	👂 icmp
		651	OUTSIDE_access_in_1207241308	admin	Правило 9	Permit		any	any	↓ in	👂 TTCCPPUUDDPP [c
С© Алминистратор	Запрещающие правила	001	OUTSIDE_access_in_1207241308	admin	Правило 10	Permit		any	any	↓ in	ICMP_GROUP4_all
	Разрешающие правила	746	OUTSIDE_access_in_1207241308	admin	Правило 11	Permit		any	any	↓ in	👴 service_group [grou
	Входящие правила брандмауэра	622	OUTSIDE_access_out_1207241313	admin	Правило 1	Permit		any	any	↑ out	👂 tcp
			OUTSIDE_access_out_1207241313	admin	Правило 2	Permit		any	any	↑ out	🔑 ip
	Исходящие правила брандмауэра	566	OUTSIDE_access_out_1207241313	admin	Правило 3	Permit		any	any	↑ out	🔊 icmp
	Отключенные правила	645	OUTSIDE_access_out_1207241313	admin	Правило 4	<ul> <li>Permit</li> </ul>		any	any	↑ out	e tcp/tcp_80-1494 (8 1494)
	Правила с отключённым	682	OUTSIDE_access_out_1207241313	admin	Правило б	<ul> <li>Permit</li> </ul>		any	any	↑ out	9 udp/udp_80 (80)
	логированием	_	OUTSIDE_access_out_1207241313	admin	Правило 7	Permit		any	any	↑ out	👂 tcp-udp-grp [group]
	Разрешенные ANY-ANY правила	58	OUTSIDE_access_out_1207241313	admin	Правило 8	Permit		any	any	↑ out	👂 test_tcp_grp [group
	Правила, разрешающие трафик любого сервиса без ограничений	26	OUTSIDE_access_out_1207241313	admin	Правило 9	Permit		any	any	↑ out	👂 tcp/service_lt (<10)
		70	inside_access_in_2005241349	admin	Правило 5	Permit		any	any	↓ in	🔊 tcp
	доунаправленные правила	12	inside_access_in_2005241349	admin	Правило 8	Permit		any	any	↓ in	👂 icmp
			inside_access_in_2005241349	admin	Правило 9	Permit		any	any	↓ in	👂 icmp6
			inside_access_in_2005241349	admin	Правило 11	Permit		any	any	↓ in	👂 icmp/mobile-redire
~			Найдено записей: 58						« <	1 из 2	> > 50 ~

∺∣купол	Главная 🗲 Анализ политик 🗲	Оптимизация 🗲 Аномалии политик							2	Администратор	
<ul> <li>КУПОЛ Упровление</li> <li>Рабочий стол</li> <li>Список устройств</li> <li>Конфигурации</li> <li>Конфигурации</li> <li>Анализ политик</li> <li>Отслеживание измен</li> <li>Администратор</li> <li>Тен</li> </ul>	🗟 Анализ полити	к								٥	
🕥 Рабочий стол	Сводка Оптимизация	Очистка Переупорядочиван	ие Глобальный поиск								
Список устройств	Аномалии политик Дубли	ирующие объекты									
👌 Конфигурации	Выбор устройства	Всего аномалий	Аномалии политик	Анализ политик от 29.1	1.2024 08:46:57	Обновить				> ····	
О Анализ политик	Cisco ASA 172.31.142.14	3630	Политика	Контекст	Nº	Описание аномалии		Действие	Включено	Источник	
О Отслеживание измен	Контекст	∨ Политики №	global_access	admin	Правило 3	Правило 157 является избыточным по отношению к правилу 3	→	<ul> <li>Permit</li> </ul>		any	
	Получите наглядное представле прописанных в брандмауэре.	ние об аномалиях в правилах,	global_access	admin	Правило 1	Правило 158 затенено правилом 1 →		<ul> <li>Permit</li> </ul>		any	
😋 Администратор	Теневые	1192	global_access	admin	Правило 3	Правило 158 затенено правилом 3 →		<ul> <li>Permit</li> </ul>		any	
	Избыточные	1802	global_access	admin	Правило 31	Правило 158 группируемо с правилом 31 →	I	× Deny		Group- 1ErlGBdG [group]	
	Обобщенные	288	global_access	admin	Правило 1	Правило 159 является избыточным по отношению к правилу 1	→ 	<ul> <li>Permit</li> </ul>		any	
	Коррелировацина	275	global_access	admin	Правило 3	Правило 159 является избыточным по отношению к правилу 3	→	<ul> <li>Permit</li> </ul>		any	
	Коррелированные	273	global_access	admin	Правило 1	Правило 160 является избыточным по отношению к правилу 1	→	<ul> <li>Permit</li> </ul>		any	
	Группируемые	73	global_access	admin	Правило З	Правило 160 является избыточным по отношению к правилу 3	→	<ul> <li>Permit</li> </ul>		any	
		J	global_access	admin	Правило 1	Правило 161 является избыточным по отношению к правилу 1	→	<ul> <li>Permit</li> </ul>		any	
	После выбора уст отображается инф	роиства рографика	global_access	admin	Правило З	Правило 161 является избыточным по отношению к правилу 3	→	<ul> <li>Permit</li> </ul>		any	
	с выявленными а	аномалиями	global_access	admin	Правило 1	Правило 162 затенено правилом 1 →		<ul> <li>Permit</li> </ul>		any	
			global_access	admin	Правило 3	Правило 162 затенено правилом 3 →		<ul> <li>Permit</li> </ul>		any	
			global_access	admin	Правило 3	Правило 163 затенено правилом 3 →		<ul> <li>Permit</li> </ul>		any	
			global_access	admin	Правило 1	Правило 164 является избыточным по отношению к правилу 1	→	<ul> <li>Permit</li> </ul>		any	
~			Найдено записей: <b>36</b>	30		Провиво 164 орвоетов иоби тошин на во	« «	1	13 <b>73 &gt;</b>	» 50 V	

Н   КА⊔ОѴ	Главная 🗲 Анализ политик 🗲	Оптимизация > Аномалии политик						2	, Администратор
Управление	🗟 Анализ полити	к							۲
Рабочий стол	Сводка Оптимизация	Очистка Переупорядочивание	Глобальный поиск						
Список устройств	Аномалии политик Дубли	ирующие объекты							
Конфигурации	Выбор устройства	Всего аномалий	Аномалии политик	Анализ политик от 29.1	1.2024 08:46:57	Обновить			> •••
Анализ политик	Cisco ASA 172.31.142.14	× <sup>#</sup> 3630	Политика	Контекст	Nº	Описание аномалии	Действие	Включено	Источник н
Отслеживание измен	Контекст	∨ Политики ∨	global_access	admin	Правило 3	Правило 157 является избыточным по → отношению к правилу 3	Permit		any
	Получите наглядное представле прописанных в брандмауэре.	ение об аномалиях в правилах,	global_access	admin	Правило 1	Правило 158 затенено правилом 1 →	Permit		any
🗟 Администратор	Теневые	1192	global_access	admin	Правило 3	Правило 158 затенено правилом 3 →	Permit		any
	Избыточные	1802	global_access	admin	Правило 31	Правило 158 группируемо с правилом 31 →	× Deny		Group- 1ErlGBdG [group]
	Обобщенные	288	global_access	admin	Правило 1	Правило 159 является избыточным по → отношению к правилу 1	Permit		any
	Корревированные	275	global_access	admin	Правило 3	Правило 159 является избыточным по → отношению к правилу 3	Permit		any
	коррелированные	2/5	global_access	admin	Правило 1	Правило 160 является избыточным по → отношению к правилу 1	Permit		any
	Группируемые	73	global_access	admin	Правило 3	Правило 160 является избыточным по → отношению к правилу 3	Permit		any
			global_access	admin	Правило 1	Правило 161 является избыточным по → отношению к правилу 1	Permit		any
			global_access	admin	Правило 3	Правило 161 является избыточным по → отношению к правилу 3	Permit		any
			global_access	admin	Правило 1	Правило 162 затенено правилом 1 →	Permit		any
			global_access	admin	Правило З	Правило 162 затенено правилом 3 →	Permit		any
			global_access	admin	Правило 3	Правило 163 затенено правилом 3 →	Permit		any
			global_access	admin	Правило 1	Правило 164 является избыточным по → отношению к правилу 1	Permit		any
						Прериде 164 придотов нобытонии на во			» <b>FO</b>
~			наидено записей: 363			В отчете зафиксированы	выявленн	ые	» 50 V
						аномалии между правилам	и		

≓   КУПОЛ	Главная 🗲 Анализ политик 🗲	Оптимизация > Аномалии политик						2	Администратор
Управление	🗟 Анализ полити	к							۲
Рабочий стол	Сводка Оптимизация	Очистка Переупорядочивание	Глобальный поиск						
Список устройств	Аномалии политик Дубл	ирующие объекты							
[° Конфигурации	Выбор устройства	Всего аномалий	Аномалии политик Группируемые	× Аналі	из политик от 29.1	1.2024 08:46:57 Обновить			> ···
	Cisco ASA 172.31.142.14	73	Политика	Контекст	Nº	Описание аномалии	Действие	Включено	Источник
[о] Отслеживание измен	Контекст	∨ Политики ∨	global_access	admin	Правило 31	Правило 158 группируемо с правилом 31 →	× Deny		Group- 1ErlGBdG
	Получите наглядное представле прописанных в брандмауэре.	ение об аномалиях в правилах,							[group] Group-
🖉 Администратор	Теневые	1192	OUTSIDE_access_in_1207241308	admin	Правило 15	Правило 16 группируемо с правилом 15 →	× Deny		56K6tKxk [group]
	Избыточные	1802	OUTSIDE_access_in_1207241308	admin	Правило 26	Правило 27 группируемо с правилом 26 →	× Deny		Host- UTgHC2zX [host]
	Обобщенные	288	OUTSIDE_access_in_1207241308	admin	Правило 49	Правило 78 группируемо с правилом 49 →	Permit		Group- zx6HCome [group]
	Коррелированные	275	OUTSIDE_access_in_1207241308	admin	Правило 99	Правило 100 группируемо с правилом 99 →	× Deny		Host- bhd0uCVK [host]
			OUTSIDE_access_in_1207241308	admin	Правило 107	Правило 108 группируемо с правилом 107 →	Permit		Group- UcujmnLW [group]
	отфильтровать по в инфографике	алии можно о клику на категорию	OUTSIDE_access_in_1207241308	admin	Правило 124	Правило 126 группируемо с правилом 124 →	Permit		Host- 3e9HWrld [host]
			OUTSIDE_access_in_1207241308	admin	Правило 109	Правило 149 группируемо с правилом 109 →	✓ Permit		Host- S57yC3sq [host]
			OUTSIDE_access_out_1207241313	admin	Правило 4	Правило 8 группируемо с правилом 4 →	Permit		any
			OUTSIDE_access_out_1207241313	admin	Правило 4	Правило 9 группируемо с правилом 4 →	Permit		any
~			Найдено записей: 73			«	< 1	13 2 >	» 50 V

≓∣купол	Главная 🗲 Анализ политик 🗲 Оп	тимизация 🗲 Аномалии политик						2	Администратор
Управление	🗟 Анализ политик								۲
Рабочий стол	Сводка Оптимизация (	)чистка Переупорядочивание	Глобальный поиск						
Список устройств	Аномалии политик Дублиру	ющие объекты							
Конфигурации	Выбор устройства	Всего аномалий	Аномалии политик Группируемые	× Аналі	из политик от 29.1	1.2024 08:46:57 Обновить			> ···
Анализ политик	Cisco ASA 172.31.142.14	73	Политика	Контекст	Nº	Описание аномалии	Действие	Включено	Источник
Отслеживание измен	Контекст Получите наглядное представлени	Политики  Политики  в об аномалиях в правилах,	global_access	admin	Правило 31	Правило 158 группируемо с правилом 31 →	× Deny		Group- 1ErlGBdG [group]
<sup>3</sup> Администратор	прописанных в брандмауэре. Теневые	1192	OUTSIDE_access_in_1207241308	admin	Правило 15	Правило 16 группируемо с правилом 15 →	× Deny		Group- 56K6tKxk [group]
	Избыточные	1802	OUTSIDE_access_in_1207241308	admin	Правило 26	Правило 27 группируемо с правилом 26 →	× Deny		Host- UTgHC2zX [host]
	Обобщенные	288	OUTSIDE_access_in_1207241308	admin	Правило 49	Правило 78 группируемо с правилом 49 →	Permit		Group- zx6HCome [group]
	Коррелированные	275	OUTSIDE_access_in_1207241308	admin	Правило 99	Чтобы посмотреть детали а	номалии		Host- bhd0uCVK [host]
	труппирусные	75	OUTSIDE_access_in_1207241308	admin	Правило 107	между правилами, неооходи на ссылку в отчете	імо нажа	ть	Group- UcujmnLW [group]
			OUTSIDE_access_in_1207241308	admin	Правило 124	Правило 126 группируемо с правилом 124 →	Permit		Host- 3e9HWrld [host]
			OUTSIDE_access_in_1207241308	admin	Правило 109	Правило 149 группируемо с правилом 109 →	Permit		Host- S57yC3sq [host]
			OUTSIDE_access_out_1207241313	admin	Правило 4	Правило 8 группируемо с правилом 4 →	Permit		any
			OUTSIDE_access_out_1207241313	admin	Правило 4	Правило 9 группируемо с правилом 4 →	Permit		any
~			Найдено записей: <b>73</b>			«	< 1	из 2 >	» 50 V

Н   КА⊔ОУ	Главная 🗲 Анализ политик 🗲 Оп	тимизация	> Аномалии полит	ИК									🗙 Аді	министратор
Управление	🗟 Анализ политик													٥
Рабочий стол	Сводка Оптимизация (	Очистка	Переупорядочив	ание Гло	бальный по	иск								
🔡 Список устройств	Аномалии политик Дублиру	ующие объе	ЭКТЫ											
🗗 Конфигурации	← назад Правило 78 группируемо с правилом 49 Анализ политик от 29.11.2024 08:46:57 Обновить													
<b>FQ</b> Анализ политик	Политика	Контекст	Nº	Действие	Включено	Источник	Назначение	Направление	Сервис назначения	Срабатывания	Пользователи	Логирование	Время	Описание
[6] Отслеживание измен	OUTSIDE_access_in_1207241308	admin	Правило 49	Permit		Group- zx6HCome [group]	Host- 3e9HWrld [host]	↓ in	🔗 tcp/1	0				
<u>С</u> Администратор	OUTSIDE_access_in_1207241308	admin	Правило 78	Permit		Group- kZhm5lT2 [group]	Host- 3e9HWrld [host]	↓ in	👂 tcp/1	0		<ul><li>Alerts</li></ul>		
	OUTSIDE_access_in_1207241308	admin	Рекомендуемое правило	Permit	•	Group- zx6HCome [group] Group- kZhm5IT2 [group]	Host- 3e9HWrld [host]	↓ in	При г 🥲 <sub>tcp</sub> отобр	іросмотре / ражаются п	деталей ан олные пар	омалии аметры п	равил	
~	Найдено записей: 3										« ‹	1 из 1	> »	50 🗸

≓∣купол	Главная 🗲 Анализ политик 🗲 Ог	птимизация	> Аномалии полит	гик									🔍 Аді	иинистратор
Управление	🗟 Анализ политик													۲
Рабочий стол	Сводка Оптимизация	Очистка	Переупорядочие	зание Гло	бальный по	иск								
Список устройств	Аномалии политик Дублир	ующие объ	ЭКТЫ											
🎝 Конфигурации	← назад Правило 78 группируемо с правилом 49 Анализ политик от 29.11.2024 08:46:57 Обновить											> ···		
न्तू Анализ политик	Политика	Контекст	Nº	Действие	Включено	Источник	Назначение	Направление	Сервис назначения	Срабатывания	Пользователи	Логирование	Время	Описание
Отслеживание измен	OUTSIDE_access_in_1207241308	admin	Правило 49	Permit		Group- zx6HCome [group]	Host- 3e9HWrld [host]	↓ in	🔗 tcp/1	0				
Администратор	OUTSIDE_access_in_1207241308	admin	Правило 78	Permit		Group- kZhm5lT2 [aroup]	Host- 3e9HWrld [host]	↓ in	👌 tcp/1	0		<ul><li>Alerts</li></ul>		
	OUTSIDE_access_in_1207241308	admin	Рекомендуемое правило	Permit		Group- zx6HCome [group] Group- kZhm5IT2 [group]	Host- 3e9HWrld [host]	↓ in	🔊 tcp/1	0				
	Для группируемых отображается реко правило	с правил омендуе	і дополните мое к замен	ельно ie										
~	Найдено записей: 3										« ‹	1 из 1	>	50 🗸

#### АНАЛИЗ ПОЛИТИК — ДУБЛИРУЮЩИЕ ОБЪЕКТЫ

≓   КУПОЛ	Главная 🗲 Анализ полити	Главная > Анализ политик > Оптимизация > Аномалии политик											
Управление	🗟 Анализ пол	итик									۲		
Пабочий стол	Сводка Оптимиза	ция Очистка Пе	ереупорядочивание	Глобальный поиск									
🔡 Список устройств	Аномалии политик	Дублирующие объект	ы										
🎝 Конфигурации	Выбор устройства	Для просмотр	а дублирующих	( ) I	к Анализ политик от 29.1	1.2024 08:46:57	Обновить						
<b></b>	Cisco ASA 172.31.142	объектов, кот	орые могут быт	ЪНА МТИ На	Контекст	Nº	Описание аномалии		Действие	Включено	Источник н		
Отслеживание измен	Контекст	соответствую	щую вкладку		admin	Правило 3	Правило 157 является избыточным по отношению к правилу 3	→	Permit		any		
	Получите наглядное пред прописанных в брандмау	ставление об аномалиях эре.	в правилах,	global_access	admin	Правило 1	Правило 158 затенено правилом 1 →		<ul> <li>Permit</li> </ul>		any		
С Администратор	Теневые	1192		global_access	admin	Правило 3	Правило 158 затенено правилом 3 →		Permit		any		
	Избыточные	1802		global_access	admin	Правило 31	Правило 158 группируемо с правилом 31 →		× Deny		Group- 1ErlGBdG [group]		
	Обобщенные	288		global_access	admin	Правило 1	Правило 159 является избыточным по отношению к правилу 1	→	<ul> <li>Permit</li> </ul>		any		
	Kopperinopaululue	275		global_access	admin	Правило З	Правило 159 является избыточным по отношению к правилу 3	→	<ul> <li>Permit</li> </ul>		any		
	Коррелированные	275		global_access	admin	Правило 1	Правило 160 является избыточным по отношению к правилу 1	→	<ul> <li>Permit</li> </ul>		any		
	Группируемые	73		global_access	admin	Правило З	Правило 160 является избыточным по отношению к правилу 3	→	<ul> <li>Permit</li> </ul>		any		
				global_access	admin	Правило 1	Правило 161 является избыточным по отношению к правилу 1	→	<ul> <li>Permit</li> </ul>		any		
				global_access	admin	Правило З	Правило 161 является избыточным по отношению к правилу 3	→	Permit		any		
				global_access	admin	Правило 1	Правило 162 затенено правилом 1 →		<ul> <li>Permit</li> </ul>		any		
				global_access	admin	Правило 3	Правило 162 затенено правилом 3 →		<ul> <li>Permit</li> </ul>		any		
				global_access	admin	Правило З	Правило 163 затенено правилом 3 →		<ul> <li>Permit</li> </ul>		any		
				global_access	admin	Правило 1	Правило 164 является избыточным по отношению к правилу 1	→	Permit		any		
"				Найдено записей: 3	3630		Поречес 164 серестро чебыточин на во	«	: <b>1</b>	13 <b>73 &gt;</b>	» 50 V		

#### АНАЛИЗ ПОЛИТИК — ДУБЛИРУЮЩИЕ ОБЪЕКТЫ

≓∣купол	Главная > Анализ политик > Оптимизация > Дублирующие объекты	🔍 Администратор
Управление	🗟 Анализ политик	0
🔓 Рабочий стол	Сводка Оптимизация Очистка Переупорядочивание Глобальный поиск	
Список устройств	Аномалии политик Дублирующие объекты	
👌 Конфигурации	Выбор устройства Cisco ASA 172.31.142.14 V Контекст V Тип объекта V	
а Анализ политик	Помогает найти объекты сети/службы, имеющие одинаковый набор IP-адресов/служб, но разные имена объектов.	
о] Отслеживание измен	Данные от 29.11.2024 08:47:38 Обновить	
Со Администратор	V Совпадение 1: tcp source eq 2 destination eq 1 admin	
	Совпадение 2: host 1.2.3.4 admin	
	Совпадение 3: subnet 1.2.3.0 255.255.255.0 admin	
	Название объекта Связанные правила	
	ds_object_network_v4 • OUTSIDE_access_in line 6 extended permit object tcp_20 object-group-user test_user_group any object ds_object_network_v4 log disable (hitcnt=0) 0x7a5dd788	
	test_network_obj • global_access line 2 extended permit object single_dup_serv_obj_1 any object test_network_obj (hitcnt=0) 0x3c56d725	
	После выбора устройства отображается отчет, содержащий список одинаковых настроек у различных объектов	
~		

#### АНАЛИЗ ПОЛИТИК — ДУБЛИРУЮЩИЕ ОБЪЕКТЫ

Н   КА⊔О∨	Главная > Анализ политик > Оптимизация > Дубли	ірующие объекты	义 Администратор							
Управление	🗟 Анализ политик		0							
Рабочий стол	Сводка Оптимизация Очистка Переуп	орядочивание Глобальный поиск								
🔡 Список устройств	Аномалии политик Дублирующие объекты									
🕞 Конфигурации	Выбор устройства Cisco ASA 172.31.142.14 У Контекст	✓ Тип объекта ✓								
- Q Анализ политик	Помогает найти объекты сети/службы, имеющие одинако	рый набор IP-адресов/служб, но разные имена объектов.								
Отслеживание измен	Данные от 29.11.2024 08:47:38 <b>Обновить</b>									
Са Администратор	V Совпадение 1: tcp source eq 2 destination e	q 1 admin								
	V Совпадение 2: host 1.2.3.4 admin									
	Совпадение 3: subnet 1.2.3.0 255.255.255.0 admin									
	Название объекта Са	зязанные правила								
	ds_object_network_v4 •	OUTSIDE_access_in line 6 extended permit object tcp_20 object-group-user test_user_group any object ds_object_network_v4 log disable (hitcnt=0) 0x7a5dd788								
	test_network_obj •	global_access line 2 extended permit object single_dup_serv_obj_1 any object test_network_obj (hitcnt=0) 0x3c56d725								
	Можно выявить объекты с од параметрами, но различными и посмотреть, где и как эти об применяются в правилах	цинаковыми п названиями, бъекты								

#### АНАЛИЗ ПОЛИТИК — НЕИСПОЛЬЗУЕМЫЕ ПРАВИЛА

#### Главная > Анализ политик > Оптимизация > Дублирующие объекты 义 Администратор Управление ම 🗟 Анализ политик Переупорядочивание Глобальный поиск Оптимизация Очистка Сводка Рабочий стол 🔡 Список устройств Для того, чтобы посмотреть неиспользуемые Аномалии политик Дубл правила, необходимо перейти на вкладку 🖪 Конфигурации Выбор устройства «Очистка» ---Cisco ASA 172.31.142.14 - Анализ политик Помогает найти объекты сети/службы, имеющие одинаковый набор IP-адресов/служб, но разные имена объектов. [0] Отслеживание измен. Данные от 29.11.2024 08:47:38 Обновить V Совпадение 1: tcp source eq 2 destination eq 1 admin 🕼 Администратор Совпадение 2: host 1.2.3.4 admin Совпадение 3: subnet 1.2.3.0 255.255.255.0 admin Название объекта Связанные правила ds\_object\_network\_v4 OUTSIDE\_access\_in line 6 extended permit object tcp\_20 object-group-user test\_user\_group any object ds\_object\_network\_v4 log disable (hitcnt=0) 0x7a5dd788 test\_network\_obj global\_access line 2 extended permit object single\_dup\_serv\_obj\_1 any object test\_network\_obj (hitcnt=0) 0x3c56d725

 $H \odot T G | KAUOV$ 

#### АНАЛИЗ ПОЛИТИК — НЕИСПОЛЬЗУЕМЫЕ ПРАВИЛА 🗄 🗅 Т С | КУПОЛ

Н   КА⊔ОУ	Главная 🗲 Анализ политик 🗲 С	)чистка <b>&gt;</b> Неи	іспользуемые пр	авила						<u> </u>	дминистратор
Управление	🗟 Анализ политик	(									٥
Рабочий стол	Сводка Оптимизация	Очистка Г	Тереупорядочи	івание Глоб	альный пои	ск					
Список устройств	Неиспользуемые правила	Неназначенн	ые интерфейсь	ы Неназнач	енные объе	кты					
👌 Конфигурации	Выбор устройства Cisco ASA 172.31.142.14	√ Конт	гекст	~	Перио 01.08	д .2024 18:10 → 15.10.2025 18:	10 📋 💽 Учитывать тол	тько количество ср	рабатываний 🕐		
оданализ политика Справля в справля в с	Получите наглядное представлен	ие обо всех неи	спользуемых пра	авилах за заданн	ый период вр	емени.					
Отслеживание измен	Правила Данные от 15.11	.2024 10:59:53	Обновить							<	:/>
а Администратор	Политика	Контекст	Nº	Действие	Включено	Источник	Назначение	Направление	Сервис назначения	Срабатывания	Пользов
	Context1_global_access	Context1	Правило 3	Permit		any	any		<pre>tcp/c_1_dup_service_two (2)</pre>	0	
	Context1_global_access	Context1	Правило 2	<ul> <li>Permit</li> </ul>		апуб	апуб		<pre>tcp/c_1_dup_service_two (2)</pre>	0	
	Context1_global_access	Context1	Правило 1	Permit		net_obj [host]	апуб		tcp/c_1_dup_service (2)	0	
	global_access	admin	Правило 2	<ul> <li>Permit</li> </ul>		any	test_network_obj [subnet]		<pre>tcp/single_dup_serv_obj_1 (1)</pre>	0	
	global_access	admin	Правило 1	Permit		any	any		PM_INLINE_PROTOCOL_2 [group]	0	
	mgmt_access_in	admin	Правило 15	Permit		any	any	↓ in	👂 UDP_GROUP1 [group]	0	
	mgmt_access_in	admin	Правило 14	Permit		any	single_dup_net_obj_1 [host]	↓ in	👂 tcp/ssh (22)	0	
	mgmt_access_in	admin	Правило 13	Permit		group_with_groups [group]	test_host_obj [host]	↓ in	👂 tcp-udp/1	0	
	mgmt_access_in	admin	Правило 12	Permit		U_NETWORK [group]	any	↓ in	👂 tcp-udp/1	0	
	mgmt_access_in	admin	Правило 11	Permit		any	DM_INLINE_NETWORK_1 [group]	↓ in	SERVICE_GROUP4 [group]	0	⊴ dm_i
	mgmt_access_in	admin	Правило 10	Permit		ds_object_host_v6 [host]	ds_object_host_v6 [host]	↓ in	ip_serv_group2 [group]	0	J
~	Найдено записей: <b>83</b>			_				После в правил за опре	зыбора устройства а, которые не сраб деленный период	і отображаі атывали	ются

## АНАЛИЗ ПОЛИТИК — НЕИСПОЛЬЗУЕМЫЕ ПРАВИЛА 🗄 🗅 Т С | КУПОЛ

≓∣купол	Главная > Анализ политик > Очист	тка 🗲 Неиспользуемые пра	авила							🔍 Адмі	инистратор
Управление	🗟 Анализ политик										۲
П Рабочий стол	Сводка Оптимизация Очи	истка Переупорядочи	вание Глобальн	ый поиск							
冒 Список устройств	Неиспользуемые правила Нен	назначенные интерфейсь	и Неназначенны	е объекты							
С Конфигурации	Выбор устройства Cisco ASA 172.31.142.14	🗸 Контекст	~	Период 01.08.2024 18:10 —	15 <mark>10.2025 18:</mark>	10 📋 💽 Учит	ывать толь	ко количест	во срабатываний ⑦		
	Получите наглядное представление о	бо всех неиспользуемых пра	вилах за заданный пер	Сегодня	« <	Окт 2025	»»	18:10			
ој отслеживание измен	Правила Данные от 15.11.202	4 10:59:53 Обновить		Последние 24 часа Последние 7 дней	Пн Вт	Ср Чт Пт Сб Во	2 15	10			
🖉 Администратор	Политика	Контекст №	Действие Вклн	Последние 30 дней	29 30	1 2 3 4 5	10	12	ие Сервис назначения	Срабатывания П	Іользов
	Context1_global_access	Context1 Правило 3	Permit 🤇		13 14	<b>15</b> 16 17 18 19	18 9 19	13 14	<pre>tcp/c_1_dup_service_two (2)</pre>	0	
	Context1_global_access	Context1_global_access Context1 Правило 2 🔽 Permit 🧰 20 21 22 23 24	22 23 24 25 26	5 20	15 16	<pre>tcp/c_1_dup_service_two (2)</pre>	0 0 0				
	Context1_global_access	Context1 Правило 1	Permit 🤇		27 28	<b>29 30 31</b> 1 2	21 22	17	tcp/c_1_dup_service (2)	0	
	global_access	admin Правило 2	Permit 🤇		3 4	5 6 7 8 9	23	18	<pre>tcp/single_dup_serv_obj_1 (1)</pre>	0	
	global_access	admin Правило 1	Permit 🤇					ок	DM_INLINE_PROTOCOL_2 [group]	0	
	mgmt_access_in	admin Правило 15	Permit	Для выявле	ения неис	спользуемых	прави	1	UDP_GROUP1 [group]	0	
	mgmt_access_in	admin Правило 14	Permit 🤇	можно зада	ть перио,	д самостояте	пьно		👂 tcp/ssh (22)	0	
	mgmt_access_in	admin Правило 13	Permit 🤇	или выорат	ъ из пред	цопределеннь	ых знач	ении	🔊 tcp-udp/1	0	
	mgmt_access_in	admin Правило 12	Permit 🤇	U_NETWORK [g	group]	any		↓ in	🔊 tcp-udp/1	0	
	mgmt_access_in	admin Правило 11	Permit 🤇	any		DM_INLINE_NETWOR [group]	RK_1	↓ in	SERVICE_GROUP4 [group]	0 2	<u>d</u> m_i
	mgmt_access_in	admin Правило 10	Permit 🤇	ds_object_host	_v6 [host]	ds_object_host_v6 [h	ost]	↓ in	👌 ip_serv_group2 [group]	0	
	Найдено записей: <b>83</b>								« < <u>1</u> и:	3 2 → » 50	$\overline{}$

# АНАЛИЗ ПОЛИТИК — НЕНАЗНАЧЕННЫЕ ИНТЕРФЕЙСЫ 🗄 🗅 Т 🔾 | КУПОЛ

Н   КА⊔ОУ	Главная 🗲 Анализ политик 🗲	Очистка > Неи	спользуемые прави	іла						<u> </u>	дминистратор	
Управление	🗟 Анализ полити	к									0	
Рабочий стол	Сводка Оптимизация	Очистка П	Іереупорядочива	ние Глоб	бальный пои	іск						
💾 Список устройств	Неиспользуемые правила	Неназначенны	ые интерфейсы	Неназнач	енные объе	кты						
🕞 Конфигурации	Выбор устройства	Для того	о, чтобы по	смотрет	гьне нас	троенные						
न्तू Анализ политик	Cisco ASA 172.31.142.14	рівсо ASA 172.31.142.14 к зонами интерфейсы, необходимо перейти 5.10.2025 18:10 🗎 Унитерать Голоко количество Срасство Срасство Срасство Срасство Срасство Срасство Срасство Вании 🐨										
[0] Отслеживание измен	і юлучите наглядное представле		зототвующу		Any							
	Правила Данные от 15.1	11.2024 10:59:53	Обновить							<	:/> •••	
Са Администратор	Политика	Контекст	Nº	Действие	Включено	Источник	Назначение	Направление	Сервис назначения	Срабатывания	Пользов	
	Context1_global_access	Context1	Правило 3	Permit		any	any		<pre>tcp/c_1_dup_service_two (2)</pre>	0		
	Context1_global_access	Context1	Правило 2	Permit		any6	any6		<pre>tcp/c_1_dup_service_two (2)</pre>	0		
	Context1_global_access	Context1	Правило 1	Permit		net_obj [host]	any6		tcp/c_1_dup_service (2)	0		
	global_access	admin	Правило 2	Permit		any	test_network_obj [subnet]		<pre>tcp/single_dup_serv_obj_1 (1)</pre>	0		
	global_access	admin	Правило 1	Permit		any	any		DM_INLINE_PROTOCOL_2 [group]	0		
	mgmt_access_in	admin	Правило 15	Permit		any	any	↓ in	👂 UDP_GROUP1 [group]	0		
	mgmt_access_in	admin	Правило 14	Permit		any	single_dup_net_obj_1 [host]	↓ in	👴 tcp/ssh (22)	0		
	mgmt_access_in	admin	Правило 13	Permit		group_with_groups [group]	test_host_obj [host]	↓ in	👂 tcp-udp/1	0		
	mgmt_access_in	admin	Правило 12	Permit		U_NETWORK [group]	any	↓ in	👂 tcp-udp/1	0		
	mgmt_access_in	admin	Правило 11	Permit		any	DM_INLINE_NETWORK_1 [group]	↓ in	SERVICE_GROUP4 [group]	0	≗ dm_i	
	mgmt_access_in	admin	Правило 10	Permit		ds_object_host_v6 [host]	ds_object_host_v6 [host]	↓ in	ip_serv_group2 [group]	0		
	Найдено записей: <b>83</b>								« < 1 и	32 > »	50 🗸	

# АНАЛИЗ ПОЛИТИК — НЕНАЗНАЧЕННЫЕ ИНТЕРФЕЙСЫ 🗄 🗅 Т 🖸 🛛 КУПОЛ

Н   КУПОЛ	Анализ политик 🔸 Очистка						Ф 🕺 Смирнов
Управление	🗟 Анализ полити	к					\$
Рабочий стол	Сводка Оптимизация	Очистка Переупорядоч	нивание Глобальный по	ИСК			
Список устройств	Неиспользуемые правила	Неназначенные интерфей	сы Неназначенные объ	екты			
Анализ политик Сканер уязвимостей	Выбор устройства <b>UserGate_v6</b> 10.229.0.143	~					
В Администратор	Получите наглядное представле Интерфейсы Данные о	ние обо всех неназначеных инте лт 27.03.2024 09:26:00 Обнови	ерфейсах				
	Имя интерфейса	Ір-адрес	Тип	Режим	Разрешенные службы		
	Ethernet0/3	192.168.0.1/24	Physical Interface	DHCP			
	Ethernet0/4	192.168.1.1/24	Physical Interface	DHCP			
	Ethernet0/4.10	10.0.112.1/24	VLAN				
	Ethernet0/4.20	10.0.112.1/24	VLAN				
	После выбора уст отображаются не интерфейсы устр Найдено записей: 4	тройства в отчете назначенные юйства				•	« < 1 из 1 > » 10 v
~							

## АНАЛИЗ ПОЛИТИК — НЕНАЗНАЧЕННЫЕ ОБЪЕКТЫ 🗄 С Т С | КУПОЛ

Н   КУПОЛ	Анализ политик 🔸 Очистка						Ф. 🞗 Смирнов
Управление	🗟 Анализ политик	(					鐐
Рабочий стол	Сводка Оптимизация	Очистка Переупорядочива	ние Глобальный по	иск			
Список устройств	Неиспользуемые правила	Неназначенные интерфейсы	Неназначенные объ	екты			
Анализ политик Сканер уязвимостей	Выбор устройства UserGate_v6 10.229.0.143		ля того, чтобы бъекты на устр а соответствую	посмотреть ойствах, нес	не назначенные обходимо перейти ху		
Администратор	Получите наглядное представлен Интерфейсы Данные от	ие обо всех неназначеных ин 27.03.2024 09:26:00 Обновить		цую вклад	57	,	
	🗌 Имя интерфейса	Ір-адрес	Тип	Режим	Разрешенные службы		
	Ethernet0/3	192.168.0.1/24	Physical Interface	DHCP			
	Ethernet0/4	192.168.1.1/24	Physical Interface	DHCP			
	Ethernet0/4.10	10.0.112.1/24	VLAN				
	Ethernet0/4.20 Найдено записей: 4	10.0.112.1/24	VLAN				« < 1 из 1 > » 10 у
	паидено записеи: 4						
~~							

#### АНАЛИЗ ПОЛИТИК — НЕНАЗНАЧЕННЫЕ ОБЪЕКТЫ 🗄 🗅 Т С | КУПОЛ

Н   КА⊔ОУ	Главная 🗲 Анализ политик 🗲 Очистка 🗲 Неназн	наченные объекты		🔍 Администратор
Управление	🗟 Анализ политик			۲
Рабочий стол	Сводка Оптимизация Очистка Пер	еупорядочивание Глобальный поиск		
🔡 Список устройств	Неиспользуемые правила Неназначенные	интерфейсы Неназначенные объекты		
🕞 Конфигурации	Выбор устройства			
🗔 Анализ политик	Usergate 7 10.229.0.136			
о Отслеживание измен	Получите наглядное представление обо всех неназн	аченных объектах.		
	Объекты Данные от 29.11.2024 16:19:07	бновить		
🔇 Администратор	Имя объекта	Тип	Сведения об объекте	
	Radmin	Сервис	tcp:4899	
	Radius	Сервис	tcp:1645-1646, udp:1645-1646	
	Quick UDP Internet Connections	Сервис	udp:443, udp:80	
	Postgres SQL	Сервис	tcp:5432	
	POP3S	Сервис	pop3s:995	
	РОРЗ	Сервис	pop3:110	
	OpenVPN	Сервис	tcp:1194, udp:1194	
	NTP	Сервис	udp:123	
	NetBIOS	Сервис	udp:138, udp:137, tcp:139	
	MySQL	Сервис	tcp:3306	
	MS SQL	Сервис	tcp:1433-1434	
	Mail Agent	Сервис	tcp:2041-2042, tcp:34-347	
		Сервис	st	
~	Найдено записей: <b>47</b>	После ві отображ которые	ыбора устройства в отчета каются все возможные объекты, е не используются ни в одной	« < 1 из 1 > » 50 ~
		политик	e	

≓∣купол	Главная > Анализ политик > Очистка > Неназн	аченные объекты		义 Администратор
Управление	🗟 Анализ политик			0
Пабочий стол	Сводка Оптимизация <b>Очистка</b> Пер	еупорядочивание Глобальный поиск		
🔡 Список устройств	Неиспользуемые правила Неназнач Д	пя того, чтобы посмотреть		
🕞 Конфигурации	Выбор устройства На	еобходимо перейти на вкладку		
🗟 Анализ политик	Озегдате 7 10.229.0.136 « Получите наглядное представление обо всех неназн	Іереупорядочивание» аченных объектах.	)	
Отслеживание измен	Объекты Данные от 29.11.2024 16:19:07 С	бновить		
С Администратор	Имя объекта	Тип	Сведения об объекте	
	Radmin	Сервис	tcp:4899	
	Radius	Сервис	tcp:1645-1646, udp:1645-1646	
	Quick UDP Internet Connections	Сервис	udp:443, udp:80	
	Postgres SQL	Сервис	tcp:5432	
	POP3S	Сервис	pop3s:995	
	POP3	Сервис	pop3:110	
	OpenVPN	Сервис	tcp:1194, udp:1194	
	NTP	Сервис	udp:123	
	NetBIOS	Сервис	udp:138, udp:137, tcp:139	
	MySQL	Сервис	tcp:3306	
	MS SQL	Сервис	tcp:1433-1434	
	Mail Agent	Сервис	tcp:2041-2042, tcp:34-347	
		Сервис	st	
	Найдено записей: 47			$\ll$ < 1 из 1 > » 50 $\checkmark$
~				

	Анализ политик 🔸 Переупорядочивание	🗘 🔍 Смирнов				
Управление	🗟 Анализ политик	¢				
🏠 Рабочий стол	Сводка Оптимизация Очистка Переупорядочивание Глобальный поиск					
🔡 Список устройств						
<b>Г</b> Конфигурации	Выбор устройства Изериод UserGate_v6 10.229.0.143 / 01.11.2024 10:00 📋 — 30.11.2024 10:00 📋					
- Анализ политик	В результате анализа частоты срабатывания правил за определенный период система предлагает вам изменить порядок правил для повышения производительности брандмауэра					
Отслеживание измен	Правила 10.11.2024 09:26:00 Обновить					
🔇 Администратор	№ Название Рекомендация смены порядка Кол-во срабатываний Эффективность					
	6 Allow from DMZ to Untrusted + 5 11 475 76%					
	25 <u>Block RU RKN by IP botlist</u> + 14 6 496 53%					
	30 <u>Block from botnets</u> ↑ 26 3 521 37%					
	31 <u>Block IPBlackList</u> + 30 1 146 21%					
	После выбора устройства отображается отчет с рекомендуемыми для смены позиции правилами					
	Найдено записей: 3 « < 1	из 1 > » 10 ~				

🗟 Анализ политик					¢
Сводка Оптимизация Очистка	Переупорядочивание Глобаль	ный поиск			
Выбор устройства Период UserGate_v6 10.229.0.143 V 01.11.	Выбор устройства Период UserGate_v6 10.229.0.143 V 01.11.2024 10:00 📋 — 30.11.2024 10:00 🛱				
В результате анализа частоты срабатывания п	равил за определенный период система	предлагает вам изменить по	рядок правил для повы	шения производительности брандмауэра	
Правила 10.11.2024 09:26:00 Обно	ить				
№ Название	Рекомендация смены порядка	Кол-во срабатываний	Эффективность	ן	
6 <u>Allow from DMZ to Untrusted</u>	<b>↑</b> 5	11 475	76%		
25 <u>Block RU RKN by IP botlist</u>	<b>↑</b> 14	6 496	53%	_	
30 <u>Block from botnets</u>	<b>↑</b> 26	3 521	37%		
31 <u>Block IPBlackList</u>	<b>↑</b> 30	1 146	21%		
Найдено записей: 3	Расчет рекоменда основывается на правил. Наиболее следует ставить в	аций для смены количестве сраб срабатываемы выше в списке пр	порядка батываний е правила равил		« < 1 из 1 > » 10 ~
	Канализ политик         Сводка       Оптимизация       Очистка         Выбор устройства       Период       01.11.2         Врезультате анализа частоты срабатывания п       01.11.2       01.11.2         В результате анализа частоты срабатывания п       01.11.2       01.11.2         Правила       10.11.2024 09:26:00       06ное         №       Название       0         6       Allow from DMZ to Untrusted       0         25       Block from botnets       0         30       Block IPBlackList       0         Найдено записей:       3       1	Кализ политик         Сводка         Отимизация         Очистка         Период         Поблы           Выбор устройства	Карана политик         Сводка         Отимизация         Очистка         Гереупорядочивание         Глобальный поиск           Выбор устройства UserGate_v6 10.229.0.143         Пали 2024 10:00         —         30.11.2024 10:00         —         30.11.2024 10:00         —         30.11.2024 10:00         —         30.11.2024 10:00         —         30.11.2024 10:00         —         —         Выбор устройства UserGate_v6 10.229.0.143         Период 10.11.2024 10:00         —         30.11.2024 10:00         —         30.11.2024 10:00         —         —         —         —         —         —         —         —         —         —         —         …         —         …	Кализ политик           Свадка         Оптимизация         Очестка         Передпорадочивание         Гобальный поиск           Выбор устройства              П.11.2024 10.00               з.0.1.2024 10.00              Выбор устройства              П.11.2024 10.00               з.0.1.2024 10.00                 Ваника частоты срабатывания правил за определенный период система предлагает вам изменить порядок правил для повы                 П.11.2024 09:26:00             Обновить               Рекомендация смены порядка	KANANA ROMUKIK           Yanga Oranga

	Анализ политик > Переупорядочивание	Ф 🗙 Смирнов
Управление	🗟 Анализ политик	鐐
ሰ Рабочий стол	Сводка Оптимизация Очистка Переупорядочивание Глобальный поиск	
🔡 Список устройств		
🖪 Конфигурации	Выбор устройства UserGate_v6 10.229.0.143 01.11.2024 × 🗄 — 30.11.2024 10:00 🗎	
न्तू Анализ политик	В результате анализа частоты срабать Сегодня « < Ноя 2024 > >> 15:43	
Отслеживание измен	Правила 10.11.2024 09:26:00 Последние 24 часа Пн Вт Ср Чт Пт Сб Вс 15 43 Последние 7 дней 16 44	
	№ Название Последние 30 дней 28 29 30 31 1 2 3 10 17 45 ктивность	
	6 Allow from DMZ to Unt 11 12 13 14 15 16 17 10 47	
	25 <u>Block RU RKN by IP bot</u> 18 19 20 21 22 23 24 20 <sup>48</sup>	
	30         Block from botnets         25         26         27         28         29         30         21         49           30         25         26         27         28         29         30         22         50	
	31         Block IPBlackList         2         3         4         5         6         7         8         23         51	
	ОК	
	Также есть возможность выбрать период, за который анализировать срабатывания правил	
	Найдено записей: <b>3</b>	> » 10 v
~		

#### АНАЛИЗ ПОЛИТИК БЕЗОПАСНОСТИ

Н   КА⊔ОИ	Главная 🗲 Анализ политик 🗲 Переупорядо	ивание		♀ test@test.ru
Управление <ul> <li>Рабочий стол</li> <li>Список устройств</li> <li>Конфигурации</li> <li>Анализ политик</li> </ul>	Выбор устройства         У           120 172.31.142.125         У           В результате анализа частоты срабатывания в	Переупорядочивание Глобальный поиск Период 11.04.2024 00:00 → 11.04.2024 10:52 ⊟ Анализ политик от 11.04.2024 10:52:4 правил за определенный период система предлагает вам изменить порядок правил для по	ции по переупорядочиванию правил 17 Обновить овышения производительности брандмауэра	Ø ···
<u>С</u> Администратор	№ Название 13 <u>ALLOW</u>	Рекомендация смены порядка 1	31	ность
~	Найдено записей: 1		« < <u>1</u> из 1	> > 50 V

# ГЛОБАЛЬНЫЙ ПОИСК

Задача: быстрый поиск всех правил на всех устройствах по нашим критериям запроса.

*Кейс*: быстро отозвать доступ у субподрядчика к инфраструктуре, которому он был временно представлен. Для этого необходимо найти все правила *на всех устройствах*, по которым был представлен доступ этому субподрядчику.
∺∣купол	Главная 🗲 Анализ полит	ик 🗲 Глобальный пои	ск						义 Администратор
Управление	🗟 Анализ пол	итик	_						0
Рабочий стол	Сводка Оптимиза	ция Очистка	Переупорядочивание Гл	обальный поиск					
🔡 Список устройств									
🔀 Конфигурации	Поиск ×	< Сбросить •••	Правила Анализ полит	ик от 19.06.2024 02:37:52	Обновить				
- Анализ политик	Простой	Расширенный	Устройство	🔷 Вендор	Название правила	Действие	Включено ≑	Источник	Назначе
[0] Отслеживание измен	Вендор	~						DUTIVET_DLACK_LIST	Апу
	Varra e e e e e		UG V6	uil. UserGate	VPN for Site-to-Site to	<ul> <li>accept</li> </ul>		Зона	Зона
(a	устроиство		Karuara		Trusted and Listrusted			VPN for Site-to-Site	Untrus
Администратор	Не учитывать зн	ачения any	как находи устройств	пь параметры в ?	правилах различі	ных		Адрес Any	Адрес
	Источник	~	Лля поиск			4 ont		20112	2010
			среди всех	сподключенных	устройств,	n ept		Any	Untrus
	Назначение	~	необходим	ю перейти на вкл	адку «Глобальнь	ый		Адрес	Truste
	Сервис	~	поиск» в р	азделе «Анализ г	олитик»			Any	DMZ
					lest	drop		Зона	Зона
	Приложение	~						Any	Any
	Пользователи	~						Agpec BOTNET_BLACK_LIST newtest	Адрес
	Действие	~	Континент 4 - ЦУС	😚 Код Безопасности	<u>first</u>	block		Any	1.1.1.1
	Включено	~		С Кол Безопасности	second	block		4.00	
	Номер правила			Cor Rod Besonachoern	Second	DIOCK		Any	8.8.8.
	Найт	и	Найдено записей: <b>1476</b>					« < 1 из 30 >	» 50 V
~									

≓   КУПОЛ	Главная 🗲 Анализ поли	итик 🗲 Глобальный по	иск						义 Администратор
Управление	🗟 Анализ по	олитик							۲
Пабочий стол	Сводка Оптимиз	зация Очистка	Переупорядочивание Глоба	альный поиск					
🔡 Список устройств	Поиск	× Сбросить •••							
🕞 Конфигурации			Правила Анализ политик	от 19.06.2024 02:37:52 Обн	ОВИТЬ				
न्तू Анализ политик	Простой	Расширенный	Устройство 💠	Вендор 🔶	Название правила	🗘 Действие 🗧	Включено ≑	Источник	Назначе
О Отслеживание измен	Вендор	~						DUTINET_DLAUN_LIST	Апу
	Vernečerne			"UserGate	VPN for Site-to-Site to	<ul> <li>accept</li> </ul>		Зона	Зона
(a	Устроиство				Trusted and Untrusted			VPN for Site-to-Site	Untrus
Администратор	Не учитывать :	значения any						Адрес	Any
	Источник	~		:	Tostlan	accent		Зона	Зона
				nii: UserGate	restien	accept		Any	Untrus
	Назначение	~						Адрес	Truste
	Сервис	~						Any	DMZ
			H UG V6	" <mark>i</mark> l <sup>#</sup> UserGate	test	× drop		Зона	Зона
	Приложение	~						Any	Any
	Пользователи	~						Agpec	Адрес
	Действие	~	🔡 <u>Континент 4 - ЦУС</u>	😚 Код Безопасности	first	block		Any	1.1.1.1
	Включено	~	]						
	На вклалке «	Спобальный г	оиск» в блоке слев	Код Безопасности	second	block		Any	8.8.8.
	представлен	ы параметры	, по которым можно						
	искать прави	ила						« < 1 из 30 >	» 50 V

## $H \subset \bot C | KAUOV$

купол	Главная 🗲 Анализ политик	: <b>&gt;</b> Глобальный пои	ск						🔍 Админи
ение	🗟 Анализ поли	тик							
стол	Сводка Оптимизаці	ия Очистка	Переупорядочивание Глоб	альный поиск					
устройств	Поиск ×	Сбросить	Правила Анализ политик	от 19.06.2024 02:37:52 Обн	овить				
	Простой	Расширенный	Verežere	D		<b>T</b> -č	D		
ание измен	Вендор	~	устроиство	вендор —	Название правила 🚽	Деиствие	включено 🚽		Апу
	Устройство	~	H UG V6	u <mark>¦l<sup>n</sup></mark> UserGate	VPN for Site-to-Site to Trusted and Untrusted	<ul> <li>accept</li> </ul>		Зона VPN for Site-to-Site	Зона Untru
гратор	Не учитывать знач	чения any						Адрес	Адрес Any
	Источник	~	H UG V6	"¦ <sup>ju</sup> UserGate	Testlen	🖌 accept		Зона	Зона
	Назначение	~						Адрес	Trust
	Сервис	~		1 LloorCato	tost	drap		2042	Зона
	Приложение	~		nji: UserGate	lest			Any	Any
	Пользователи	~						BOTNET_BLACK_LIST newtest	Алу
	Действие	~	На <u>Континент 4 - ЦУС</u>	😚 Код Безопасности	first	block		Any	1.1.1
	Включено	~	В         Континент 4 - ЦУС	<b>ഗ്രാ</b> Код Безопасности	second	block		Any	8.8.8
	Номер правила Найти		Найдено записей: 1476				В осно резуль различ	вной части экрана ото тат поиска среди прае ных устройств	бражает ил
//									

	Главная > Анализ политик > Глобальный поис	ск					义 Администратор
Управление	🗟 Анализ политик						۲
Пабочий стол	Сводка Оптимизация Очистка Г	Переупорядочивание Глобальный пои	іск				
<ul> <li>Список устройств</li> <li>Конфигурации</li> </ul>	Поиск × Сбросить …	Правила Анализ политик от 19.06.2024	4 02:37:52 Обновить				
	Простой Расширенный	🔶 Вендор	Название правила	Действие 🍦	Включено ≑	Источник	Назначение
Отслеживание измен	Вендор 🗸	ат 4 - ЦУС 🔅 Код Безопасности	first	block		Any	1.1.1.1
С Администратор	Устройство    Не учитывать значения any	<u>нт 4 - ЦУС</u> 😚 Код Безопасности	Название2	pass		Any	Any
	Источник 🗸	нт 4 - ЦУС 🔅 Код Безопасности		pass		Any	Any
	Назначение 1.1.1.1 × ∨	A whether Cisco	Правило_1	✓ permit		any	any
	Сервис ір × ∨	A deal Cisco	Правило_1	× deny		any	any
	После ввода значений для поиска и нажатия на кнопку «Найти»	4 due Cisco	Правило_2	✓ permit		any	any
	в отчеты отражаются только релевантные	A ebee Cisco	Правило_2	✓ permit		any	any
	значения	A ender Cisco	Правило_3	× deny		any	1.1.1.1
	Номер правила	غیث Cisco	Правило_3	✓ permit		any	any
~	Найти	Найдено записей: 21					« < 1 из 1 > » 50 ∨

≓   КУПОЛ	Главная 🗲 Анализ политик 🗲 Глобальный поис		🔍 Администратор
Управление	🗟 Анализ политик		۲
Рабочий стол	Сводка Оптимизация Очистка Г	ереупорядочивание Глобальный поиск	
<ul> <li>Список устройств</li> <li>Конфигурации</li> </ul>	Поиск × Сбросить …	Правила Анализ политик от 19.06.2024 02:37:52 Обновить	
न्तू Анализ политик	Дополнительно можно отфильтровать	💠 Вендор 💠 Название правила 💠 Действие 💠 Включено 💠 Источник	Назначение
[6] Отслеживание измен	результаты, чтобы отображались конкретные значения	A the Cisco Правило_3 🗙 deny on any	1.1.1.1
Се Администратор	Не учитывать значения any	A the Cisco Правило_29 Permit on any	DM_INLINE_NETWORK_:
	Источник 🗸		
	Назначение 1.1.1.1 × ∨		
	Сервис ір × ∨		
	Приложение 🗸		
	Пользователи 🗸		
	Действие 🗸		
	Включено 🗸		
	Номер правила		
	Найти	Найдено записей: 2 « <	1 из 1 > » <b>50</b> ∨
~			

≓   КУПОЛ	Главная 🗲 Анализ политик 🗲 Глобальный поис		义 Администратор
Управление	🗟 Анализ политик		٥
Рабочий стол	Сводка Оптимизация Очистка Г	ереупорядочивание Глобальный поиск	
<ul> <li>Список устройств</li> <li>Конфигурации</li> <li>Конфигурации</li> </ul>	Поиск × Сбросить ••• Простой Расширенный	Правила         Анализ политик от 19.06.2024 02:37:52         Обновить	назначение
[о] Отслеживание измен	Также возможен поиск значений среди всех	A deny any any	1.1.1.1
<u>С</u> Администратор	полей. Для этого необходимо перейти к расширенному поиску	A dds Cisco Правило_29 v permit on any	DM_INLINE_NETWORK_:
	Источник 🗸		
	Назначение 1.1.1.1 × ∨		
	Сервис ір × ∨		
	Приложение 🗸		
	Пользователи 🗸		
	Действие 🗸		
	Включено 🗸		
	Номер правила		
	Найти	Найдено записей: 2	$\ll$ $<$ 1 H3 1 $>$ $>$ 50 $\vee$
~			

≓∣купол	Главная > Анализ политик > Глобальный поиск						义 Администратор
Управление	🗟 Анализ политик						۲
П Рабочий стол	Сводка Оптимизация Очистка Пе	реупорядочивание Глоб	бальный поиск				
<ul> <li>Список устройств</li> <li>Конфигурации</li> </ul>	Поиск × Сбросить …	Правила Анализ политин	к от 19.06.2024 02:37:52 Обнов	ИТЬ			
न्तू Анализ политик	Простой Расширенный Ввелите запрос	Вендор	Название правила	Действие	🗄 Включено 崇	Источник	Назначение
Отслеживание измен	www.ya.ru	teres Cisco	Правило_5	✓ permit		any	any
Са Администратор	Найти	disco Cisco	Правило_6	✓ permit		fqdn_group [group]	any
		enter Cisco	Правило_6	✓ permit		any	any
	для расширенного поиска необходимо ввести значение	disco Cisco	Правило_6	✓ permit		ds_group_1 [group]	ds_group_1 [group]
	в текстовом поле и нажать на кнопку «Найти»	tere Cisco	Правило_6	× deny		any	any
		tere Cisco	Правило_6	✓ permit		2001:4860:4860::8888	ds_group_1 [group]
		tisco Cisco	Правило_6	✓ permit		any	any
		etere Cisco	Правило_7	✓ permit		2001:db8:ac10:fe01:fe02::	any
		duale Cisco	Правило_7	✓ permit		net_group2 [group]	net_group2 [group]
		Найдено записей: <b>136</b>				~	< 1 изз » » 50 ∨
~							

≓   КУПОЛ	Главная 🗲 Анализ политик 🗲 Глобальный пои	СК					义 Администратор
Управление	Анализ политик						۲
Рабочий стол	Сводка Оптимизация Очистка I	Переупорядочивание Глоб	бальный поиск				
Список устройств	Поиск × Сбросить …		( of 10.06.2024.02:27:52	HTT.			
L <sup>6</sup> конфигурации	Простой Расширенный	Правила Анализ политик	00008				
ГО Анализ политик	Введите запрос	🔷 Вендор	Название правила	Действие	Включено	Источник	Назначение
о Отслеживание измен	Не учитывать значения апу	diale Cisco	Правило_5	✓ permit		any	any
Са Администратор	Найти	eteter Cisco	Правило_6	✓ permit		fqdn_group [group]	any
		-duale Cisco	Правило_6	✓ permit		any	any
		diale Cisco	Правило_6	✓ permit		ds_group_1 [group]	ds_group_1 [group]
		eteter Cisco	Правило_6	× deny		any	any
		esco Cisco	Правило_6	V permit		2001:4860:4860::8888	ds_group_1 [group]
		duth Cisco	Правило_6	V permit		any	any
		etere Cisco	Правило_7	V permit		В результатах пои	ска выделяются ячейки,
		etado Cisco	Правило_7	🗸 permit		в которых было на из запроса	йдено значение
		Найдено записей: 136				«	< 1 из 3 > » 50 ∨
~							

≓   КУПОЛ	Главная 🗲 Анализ политик 🗲 Глобальный поиск							
Управ∧ение	🗟 Анализ политик						0	
Рабочий стол	Сводка Оптимизация Очистка Пе	ереупорядочивание Глоб	бальный поиск					
Список устройств Конфигурации	Поиск × Сбросить …	Правила Анализ политик	: от 19.06.2024 02:37:52 Обнова	пь				
	Простой Расширенный	🔶 Вендор	🔶 Название правила	Действие	Включено 荣	Источник	Назначение	
[о] Отслеживание измен	Введите запрос www.ya.ru	duale Cisco	Правило_1	🗸 permit		any	ds_object_fqdn_v4 [fqdn]	
<u><u></u> Администратор</u>	<ul> <li>Не учитывать значения апу</li> <li>Найденные значение также</li> </ul>	elude. Cisco	Правило_5	× deny		net_group2 [group]	net_group2 [group]	
	можно отфильтровать для просмотра конкретных	disco Cisco	Правило_5	🗸 permit		any	ds_object_fqdn_v4 [fqdn]	
	объектов	etter Cisco	Правило_6	✓ permit		2001:4860:4860::8888	ds_group_1 [group]	
		duale Cisco	Правило_6	✓ permit		ds_group_1 [group]	ds_group_1 [group]	
		diale Cisco	Правило_7	✓ permit		net_group2 [group]	net_group2 [group]	
		dute Cisco	Правило_8	✓ permit		ds_group_1 [group]	ds_group_1 [group]	
		dealer Cisco	Правило_11	✓ permit		any	DM_INLINE_NETWORK_1 [group]	
		disco Cisco	Правило_18	yermit		any	ds_object_fqdn_v4 [fqdn]	
		Найдено записей: 11		_			« < 1 из 1 > » 50 ∨	
~~								

≓∣ КУПОЛ	Главная 🗲 Анализ п	юлитик 🗲 Глобальный п	тоиск					🔍 Администратор
Управление	🗟 Анализ	политик						0
Рабочий стол	Сводка Опти	мизация Очистка	Переупорядочивание Гло	бальный поиск				
Список устройств	Поиск	Х Сбросить 🚥	Правила Анализ полити	κ οτ 19.05 2024 02·37·52 <b>Οδ</b> μο	рить			
	Простой	Расширенный				A Duran A		
<ul> <li>Отслеживание измен</li> </ul>	Введите запрос www.ya.ru		ettebr Cisco	Правило_1	треrmit		any	ds_object_fqdn_v4 [fqdn]
	🚺 Не учитыва	ать значения any						ds object fada v4 lfada
Са Администратор		Найти	esco Cisco	Правило_5	× deny		net_group2 [group]	address net_group2 (group) www.ya.ru ip_version 4
			eterte Cisco	Правило_5	✓ permit		any	5.255.255.242 77.88.55.242 77.88.44.242
			the Cisco	Правило_6	✓ permit		2001:4860:4860::8888	При наведении курсора на объекты в отчетах отображаются параметры
			duth Cisco	Правило_6	🗸 permit		ds_group_1 [group]	этого объекта
			ettere Cisco	Правило_7	✓ permit		net_group2 [group]	net_group2 [group]
			eace Cisco	Правило_8	✓ permit		ds_group_1 [group]	ds_group_1 [group]
			tere Cisco	Правило_11	✓ permit		any	DM_INLINE_NETWORK_1 [group]
			tere Cisco	Правило_18	✓ permit		any	ds_object_fqdn_v4 [fqdn]
			Найдено записей: 11					« < 1 из 1 > » 50 ~

≓∣купол	Главная 🗲 Анализ политик 🗲 Глобальный по	оиск					🔍 Администратор
Управление	🗟 Анализ политик						0
П Рабочий стол	Сводка Оптимизация Очистка	Переупорядочивание Гл	обальный поиск				
🔡 Список устройств	Поиск × Сбросить …						
🌔 Конфигурации	Простой Расширенный	Правила Анализ полит	ик от 19.06.2024 02:37:52 Обно	ОВИТЬ			
न्तू Анализ политик	Ввелите запрос	Вендор	Название правила	Действие	Включено 崇	Источник	Сохраненные запросы
[0] Отслеживание измен	www.ya.ru	ettele Cisco	Правило_1	✓ permit		any	🛧 Экспорт
	Не учитывать значения any						<ul><li>Настройка столбцов</li></ul>
😂 Администратор	Найти	diade Cisco	Правило_5	× deny		net_group2 [group]	net_group2 [group]
				-			Также есть возможность
		disto Cisco	Правило_5	✓ permit		any	сохранить отчет с найденными и отфильтрованными
		diate Cisco	Правило_6	✓ permit		2001:4860:4860::8888	правилами
		diade Cisco	Правило_6	✓ permit		ds_group_1 [group]	ds_group_1 [group]
		etter Cisco	Правило_7	✓ permit		net_group2 [group]	net_group2 [group]
		ender casco Cisco	Правило_8	✓ permit		ds_group_1 [group]	ds_group_1 [group]
		entre Cisco	Правило_11	✓ permit		any	DM_INLINE_NETWORK_1 [group]
		dute Cisco	Правило_18	✓ permit		any	ds_object_fqdn_v4 [fqdn]
		Найдено записей: 11					« < 1 из 1 > » 50 ∨
«							







≓   КА⊔ОУ	Главная 🗲 Список устройств		义 Администратор
Управление	<ul> <li>Список устройств</li> <li>17</li> </ul>	Отключены Перезагрузка 0	
П Рабочий стол			
🔡 Список устройств	Все группы	Добавить 🗸 🚊 …	
🖪 Конфигурации	□	172.31.142.148	
_	$\Box \equiv \bullet \underline{asdf2}$	172.31.142.86	
- Анализ политик	✓ □ CheckPoint	6	
Отслеживание измен	□	10.229.0.221	
	□ 垦 ● <u>CP 170</u>	10.229.0.170	
	CheckPoint MS	10.229.0.56	
🔇 Администратор	□	10.229.0.53	
_	□ <b>&amp; ●</b> 220	10.229.0.220	Все устроиства
	CheckPoint 222	10.229.0.222	
		2	Устройств Кластеры
	устройства необходимо нажать на его	172.31.142.165	30
	название в списке	10.229.0.143	
		2	Image: white the second se
	□ 🗮 ● <u>KC-dev-17.10</u>	172.31.142.194	S CheckPoint: 3 Infotecs: 2 O Ideco: 1
	$\square \coloneqq KC_{dev1}$	172.31.142.102	👗 Eltex: 1 🛛 🗮 Купол.Сети: 10
	> ОФИС МОСКВА	2	🚸 Код Безопасности: 2 🛛 🌺 HUAWEI: 1
	∨ □ Рязань	7	E Fortigate: 1
	Infotecs ViPNet	172.31.142.81	🚺 Фактор-ТС: 1
	🔲 🖦 😐 фывфыв	1.1.1.1	
		172.31.142.39	
	Eltex	10.229.0.164	
	🗌 🔅 • <u>Континент 4 - ЦУС</u>	172.31.142.243	
	🔲 🌺 🔹 <u>HUAWEI</u>	172.31.142.240	
	Dionis NX	10.229.0.199	
~	Найдено устройств: 30 Найдено групп: 7 <b>Свернуть все</b>		

≓∣купол	Главная > Список устройств > Ра	义 Администратор							
Управление	CheckPoint 222	IP-адр 10.22	ec 9.0.222	Seндор CheckPoint					
Рабочий стол					<b>.</b>				
🔡 Список устройств	(i) Внесены изменения которые еще	е не установлен	ы на устройс	тво Установить политику	(!) Опубликовать	изменения От	менить изменения		
🕞 Конфигурации	🗐 Политики								
न्तू Анализ политик	Mawaatanaŭ avnau	Межсе	гевой экран	: policy_2 policy_2 Network	~				+ Добавить \cdots
	межсетевой экран		Nº	Name	Action	Enabled	Source	Destination	Services & Applications
C-3	policy_1								a_tcp_10 a_tcp_20-50
(A	policy_2								a_tcp_any_dns AH A( cachefsd CP_rtm CU
администратор	Standard							interoperable .domain.ruasac2_	dest-unreach echo-reply
	🖉 Статус задач		1	Drop from Groups to hosts	× Drop		group3 group2 group1 group4_a	h323 gw CP_default_Office_Mode_addresses_poo	ftp-pasv FW1_ica_mgm FW1_uaa group_with_gr
							ose_device	I IPv6 Link Local Hosts	H323 home-agent-addr
									igmp Madster MS-SQL-Monitor_UDP r
									NoBackO pop-3 rip-re
									sip_dynamic_ports Terr
									#hashtags 1000memor 115-audio 1337x.org
									360 Mobile Manager 45
			2	<u>Cleanup rule</u>	× Drop		None	Any	51.com-music 51GuGu-
									app-site Alcohol & Tobac
									Entertainment ex.com
			3	Reject Any to Domain Clone	× Reject		Any	.domain.ru Clone	None
			4	Drop empty traffic	× Drop		None	Отображается список прав	ил, который
		Найден	о записей: 8					подгружается с устроиства	
<									

≓∣купол	Главная 🗲 Список устройств 🗲 Расц	ширенные настройки Che	ckPoint > Межсетевой экран					🖉 Администрато
Управление	CheckPoint 222	<ul> <li>IP-адрес</li> <li>10.229.0.222</li> </ul>	Seндор CheckPoint					
Рабочий стол								
Список устройств	<ol> <li>Внесены изменения которые еще н</li> </ol>	е установлены на устрой	СТВО Установить политику	() Опубликоват	ь изменения От	менить изменения		
🚴 Конфигурации								
-	Политики	Межсетевой экра	H: policy_2 policy_2 Network	$\sim$				+ Добавить …
Q Анализ политик	Межсетевой экран 🖍		Name	Action	Enabled	Course	Destination	Convises & Applications
о] Отслеживание измен	policy_1	LN≚	Name	Acuon	Enabled	Source	Destination	Services & Applications
	policy 2							a_tcp_10 a_tcp_20-50
~	policy_z							cachefsd CP_rtm CU
Администратор	Standard						interoperable .domain.ruasac2_	dest-unreach echo-reply
		поцифика				group3 group2	h323 gw	ftp-pasv FW1_ica_mgm
	вендора, поэтому для	я CheckPoint	Drop from Groups to hosts	× Drop		group1 group4_any	CP_default_Office_Mode_addresses_poo	FW1_uaa group_with_g
	устройств отображае	тся список				ose_device	I IPv6 Link Local Hosts	H323 home-agent-addr
	групп и слоев							igmp Madster
								MS-SQL-Monitor_UDP r
								sin dynamic ports
								"headtana 1000mana
								#nashtags 1000memor
								360 Mobile Manager 45
		□ 2	Cleanup rule	× Drop		None	Anv	51.com-music 51GuGu
				_				6rounds 8Tracks Abi
								app-site Alcohol & Tobac
								Entertainment ex.com
		3	Reject Any to Domain Clone	× Reject		Any	.domain.ru_Clone	None
		4	Drop empty traffic	× Drop		None	None	None
		Найдено записей:	8					

≓   КА⊔ОИ	Главная 🗲 Список устройств 🗲 Расц	🔍 Администратор						
Управление	CheckPoint 222	<ul> <li>IP-адрес</li> <li>10.229.0.222</li> </ul>	вендор           CheckPoint					
Рабочий стол								
В Список устройств	<ol> <li>Внесены изменения которые еще не</li> </ol>	е установлены на устройс	Установить политику	Опубликовать и	зменения От	менить изменения		
Конфигурации	🗐 Политики 🖍	Межсетевой экран	policy_2 policy_2 Network	~				+ Добавить 🚥
	Межсетевой экран 🖍	Nº	Name	Action	Enabled	Source	Destination	Services & Applications
о Отслеживание измен	policy_1							a tcp 10 a tcp 20-50
(@	policy_2							a_tcp_any_dns AH A( cachefsd CP_rtm CU
администратор	Standard						interoperable .domain.ruasac2_	dest-unreach echo-reply
	🖉 Статус задач	_			_	group3 group2	h323 gw	ftp-pasv FW1_ica_mgm
		1	Drop from Groups to hosts	× Drop		group1 group4_any	CP_default_Office_Mode_addresses_poo	FW1_uaa group_with_g
			Чтобы измени	ть правило		ose_device	IPv6_Link_Local_Hosts	igmn Madster
			необходимо н	ажать на его	, D			MS-SOL-Monitor_UDP r
			название в таб	блице				NoBackO pop-3 rip-re
								sip_dynamic_ports Terr
								#hashtags 1000memor
								115-audio 1337x.org
								360 Mobile Manager 45
		2	Cleanup rule	× Drop		None	Any	51.com-music 51GuGu-
								6rounds 8Tracks Αbι
								app-site Alcohol & Tobac
								Entertainment ex.com
		3	Reject Any to Domain Clone	× Reject		Any	.domain.ru_Clone	None
		4	Drop empty traffic	× Drop		None	None	None
		Найдено записей: 8	3					
*								

Н   КА⊔ОУ	Главная > Список устройств > Расши	ренные настройки CheckPoint 🗲 Детальная карточ	ка правила Checkpoint	× A	дминистратор
Управление	CheckPoint 222	IP-адрес         •         Вендор           10.229.0.222         •         CheckPoint			
П Рабочий стол					
Список устройств	📃 Политики 🖍	← Назад Drop from Groups to hosts	В открывшемся экране	··· Services + Добавить ···	
🗗 Конфигурации	Межсетевой экран 🖍	Информация	отображаются настроики выбранного правила		
<b>F</b> Q Анализ политик	policy_1				88
Отслеживание измен	policy_2	Name A	ction Включено	a_tcp_20-50	₽
	Standard	Comments		a_tcp_any_dns	
🔇 Администратор	🖉 Статус задач			AH 🗞 🗌	
		Source + Добавить	Destination + Добавить	AOL 🕹	
		group3 ×	interoperable ×	🗌 🕫 archie	1 1
		group2 ×	.domain.ruasac2_ ×	Cachefsd	1 1
		group1 ×	h323 gw ×	CP_rtm	
		group4_any ×	CP_default_Office_Mode_addresses_pool ×	CU-SeeMe	
		ose_device ×	IPv6_Link_Local_Hosts ×	dest-unreach	
		Install On			
		Policy Targets +		echo-reply	
				FIBMGR	
		A Tracking		🗌 🖉 ftp-pasv	
		Track Alert	~	GP FW1_ica_mgmt_tools	
				🗌 👶 FW1_uaa	
		<ul> <li>Extend settings</li> </ul>		aroup_with_group	
~					

Н   КА⊔ОУ	Главная > Список устройств > Расшир	ренные настройки CheckPoint > Детальная карточка правила Checkpoint	🔍 Администра	атор
Управление	CheckPoint 222	IP-адрес 10.229.0.222 Сектор CheckPoint		
Рабочий стол				
Список устройств	🗐 Политики 🖍	← Назад Drop from Groups to hosts	Services + Добавить	
🎝 Конфигурации	Межсетевой экран 🖍	Информация		11
न्तू Анализ политик	policy_1			
о Отслеживание измен	policy_2	Name Action Drop from Groups to hosts I Drop Bключено	□	11
	Standard	Comments	a_tcp_any_dns	
С Администратор	🔊 Статус задач		HA 🗞	Ш
		Source + Добавить Для того, чтобы изменить	🗋 🔗 AOL	Ш
		а настроику источника правила, необходимо нажать на кнопку	🗋 👌 archie	Ш
		group2 × «Добавить»	Cachefsd	ш
		group1 × h323 gw ×	CP_rtm	ш
		group4_any X CP_detaurt_Umice_woode_addresses_pool X	CU-SeeMe	Ш
		USE_UEVICE X IPVO_LIIIK_LUCAL_HUSIS X	🗌 🔊 dest-unreach	11
		Install On	echo-reply	11
		Policy Targets +		ш
		∧ Tracking		Ш
				11
		Track Alert None None	FW1_ica_mgmt_tools	
		∧ Extend settings	🗌 🔊 FW1_uaa	
		Litera occurgo	aroup_with_group	
~				



Н   КУПОЛ	Главная > Список устройств > Расшир	енные настройки CheckPoint > Детальная карточка правила Checkpoint	Q AJ	дминистратор
Управ∧ение	CheckPoint 222	IP-адрес 10.229.0.222 Секроіпt		
Рабочий стол				
🔡 Список устройств	🔲 Политики 🖍	← Назад Drop from Groups to hosts	Services + Добавить …	
📘 Конфигурации	Межсетевой экран 🖍	Информация		
<b>F</b> Q Анализ политик	policy_1			88
отслеживание измен	policy_2	Name Action Drop from Groups to hosts 🗾 Drop У 💽 Включено	□ 🤌 a_tcp_20-50	Þ
	Standard	Comments	a_tcp_any_dns	
🔇 Администратор	🔊 Статус задач		HA 🔍	
_		Source + Добавить Destination + Добавить	AOL	
		group3 × interoperable ×	🗌 🖉 archie	
		group2 × .domain.ruasac2_ ×	🗌 🔊 cachefsd	1 1
		group1 × >> h323 gw ×	CP_rtm	L II
		group4_any × CP_default_Office_Mode_addresses_pool ×	CU-SeeMe	1 11
		ose_device × IPv6_Link_Local_Hosts ×		- 11
		ExternalZone × После выбора объекта и сохранения, он отображается		
		Install On изменения необходимо нажать на кнопку «Сохранить»	🦳 , © echo-reply	
		Policy Targets +	BIBMGR	
			🔲 🕫 ftp-pasv	
		∧ Tracking	SW1_ica_mgmt_tools	
		Track Alert none	🗌 🔗 FW1_uaa	
~		Сохранить Отменить		

Н   КУПОЛ <sup>Управление</sup>	Главная > Список устройств > Расшир CheckPoint 222	енные настройки CheckPoint > Стальная картонка правила Checkpoint Политика успешно обновлена × 10.229.0.222 С После изменения правила появляется	Q Ад	министратор
Рабочий стол		соответствующее уведомление. Теперь изменение будет отображаться также в списке правил устройства		
🔠 Список устройств	📃 Политики 🖍	← Назад Drop from Groups to hosts	, Services + Добавить ···	0
🗗 Конфигурации	Межсетевой экран 🔦	Информация		
न्तू Анализ политик	policy_1			88
О Отслеживание измен	policy_2	Name Action Drop from Groups to hosts Z Drop Ключено	🔲 🖉 a_tcp_20-50	Þ.
	Standard	Comments	🔲 🖉 a_tcp_any_dns	
С Алминистратор	🔊 Статус задач		на 💁	
		Source + Добавить Destination + Добавить	🗌 👶 AOL	
		group3 $\times$ interoperable $\times$	🗌 👌 archie	
		group2 × .domain.ruasac2_ ×	🗌 🕫 cachefsd	
		group1 × >>> h323 gw ×	CP_rtm	
		group4_any $\times$ CP_default_Office_Mode_addresses_pool $\times$		
		ose_device $\times$ IPv6_Link_Local_Hosts $\times$	U-SeeMe	
		ExternalZone ×	🔲 🔊 dest-unreach	
			🔲 👌 echo-reply	
			🗌 🕫 FIBMGR	
			🗌 👌 ftp-pasv	
		∧ Tracking	FW1_ica_mgmt_tools	
		Track Alert none	🗌 🔊 FW1_uaa	
			🔲 🧔 group_with_group	
~		<ul> <li>Extand entringe</li> </ul>		

≓   КУПОЛ	Главная > Список устройств > Расширенные настройки CheckPoint > Межсетевой экран										
Управление	CheckPoint 222  F <sup>-agpec</sup> 10.229.0.222  F <sup>-adpec</sup> CheckPoint BeHdop CheckPoint										
Рабочий стол											
🔡 Список устройств	Внесены изменения которые еще не	е установлены на устроиство	Установить политику	публиковать изменен	Отменит	гь изменения					
🕞 Конфигурации	Политики										
		Межсетевой экран: polic	cy_2 policy_2 Network	$\sim$				+ Добавить 😶			
	Межсетевой экран 🖍	□ Nº	Name	Action	Enabled	Source	Destination	Services & Applications			
С Отолеживание измен	policy_1							a_tcp_10 a_tcp_20			
	policy_2							a_tcp_any_dns AH			
<u>€</u> Администратор	Standard	□ 1	1 <u>Drop from Groups to hosts</u>	× Drop		group3 group2 group1 group4_any coc_dente ExternalZone Изменение ото со специфико	interoperable .domain.ruasac2_ h323 gw CP_default_Office_Mode_addresses_poo I IPv6_Link_Local_Hosts тображается в таблице, но ой вендора CheckPoint, не	dest-unreach echo ftp-pasv FW1_ica_ FW1_uaa group_w H323 home-agent- igmp Madster В СООТВЕТСТВИИ БОХОДИМО			
						опуоликовать устройстве	изменения для их примен	тения на			
		2	<u>Cleanup rule</u>	× Drop		None	Any	360 Mobile Manager 51.com-music 510 6rounds 8Tracks app-site Alcohol & 1 Entertainment ex.co			
		3	Reject Any to Domain Clone	× Reject		Any	.domain.ru_Clone	None			
		4	Drop empty traffic	× Drop		None	None	None			
		Найдено записей: 8									
~											

≓∣купол	Главная > Список устройств > Расширенные настройки CheckPoint > Межсетевой экран								
Управление	CheckPoint 222	<ul> <li>IP-адрес</li> <li>10.229.0.222</li> </ul>	6* Вендор CheckPoint						
🔓 Рабочий стол									
Список устройств	<ol> <li>Внесены изменения которые еще в</li> </ol>	не установлены на устройство	Установить политику	публиковать изме	нения Отмени	ть изменения			
👌 Конфигурации	Для того, чтобы изме	нения внеслись н	а устройство,						
 Сд. Анализ политик	неооходимо нажать н	а кнопку «установ	вить политику»	~				+ Добавить 😶	
ОТСЛЕЖИВАЦИЕ ИЗМЕЦ	межсетевой экран	□ Nº	Name	Action	Enabled	Source	Destination	Services & Applications	
	policy_1							a_tcp_10 a_tcp_20	
	policy_2							a_tcp_any_dns AH	
С Администратор	Standard							cachefsd CP_rtm	
						group3 group2	interoperable .domain.ruasac2_	ftp-pasy FW1 ica	
	🖉 Статус задач	1	Drop from Groups to hosts	× Drop		group1 group4_any	CP_default_Office_Mode_addresses_poo	FW1_uaa group_w	
						ose_device	1	H323 home-agent-	
						ExternalZone	IPv6_Link_Local_Hosts	igmp Madster	
								MS-SQL-Monitor_UDF	
								NoBackO pop-3	
								sip_dynamic_ports	
								#hashtags 1000m	
								115-audio 1337X.c	
			Cleanup rule	Drop		None	Any	51 com-music 510	
			<u>oleanap raie</u>	Diob		Hone	ZNIY	6rounds 8Tracks	
								app-site Alcohol & 1	
								Entertainment ex.co	
		3	Reject Any to Domain Clone	× Reject		Any	.domain.ru_Clone	None	
		4	Drop empty traffic	× Drop		None	None	None	
		Найдено записей: 8							
<i>u</i>									

	Главная 🗲 Список устройств 🗲 Расш	Главная > Список устройств > Расширенные настройки CheckPoint > Межсетевой экран											
Управление	CheckPoint 222	<ul> <li>IP-адрес</li> <li>10.229.0.222</li> </ul>	вендор CheckPoint					Название сессии * admin_43 2024-11-28T16:14:52.214Z					
П Рабочий стол							_	Описание					
🔡 Список устройств	<ol> <li>Внесены изменения которые еще не</li> </ol>	О внесены изменения которые еще не установлены на устроиство Установить политику О опубликовать изменения Отменить изменения											
ြ Конфигурации	📃 Политики 🖍		<b>⇔Выполнить проверку</b>										
न्तू Анализ политик	Межсетевой экран 🔥		Найдены незначительные ошибки										
Отслеживание измен	policy_1	Nº	Name	Action	Enabled	Source	Destination	Что бы продолжить нажмите "Опубликовать"					
	policy_2							Unknown Access Rule contains an object of type 'None' in the Source, Destination, Service & Applications columns.					
🔄 Администратор	иинистратор Standard		Drop from Groups to hosts	Crop		group3 group2 group1 group4_any ose_device ExternalZone	interoperable . h323 gw CP_default_Office I IPv6_Link_Local_	This rule will never be matched. Unknown Access Rule contains an object of type 'None' in the Source, Destination columns. This rule will never be matched. Unknown Access Rule contains an object of type 'None' in the Source, Destination columns. This rule will never be matched.					
		2	<u>Cleanup rule</u>	× Drop		None	Any	<ul> <li>Controlown         Access Rule contains an object of type 'None' in the Source, Destination columns. This rule will never be matched.     </li> <li>Cunknown         Access Rule contains an object of type 'None' in the Source, Destination columns. This rule will never be matched.     </li> <li>Cunknown         Access Rule contains an object of type 'None' in the Access Rule contains an object of type 'None' in the Matched.     </li> </ul>					
		3	Reject Any to Domain Clone	× Reject		Any	.domain.ru_Clone	Source column. This rule will never be matched.					
		4	Drop empty traffic	Drop		None	None	Access Rule contains an object of type 'None' in the					
~		Найдено записей: 8	Появляется экр аналогично экра продолжения за необходимо нах	ан подтверж ану при рабо прузки изме кать на кноп	дения и оте с устр нений на ку «Опуб	публикации изме ойством CheckP конечные узлах, ликовать и прод	нений, oint. Для олжить»	Service & Applications column. This fore will never be matched. ▲ Unknown Асселе Dula contains on chiest of time 'klope' in the Опубликовать и продолжить Отменить					



	Главная > Список устройств > Расширенные настройки CheckPoint > М устатовой акодина Задача на установку успешно создана Х							
П Рабочий стол	CheckPoint 222	<ul> <li>IP-adpec</li> <li>10.229.0.222</li> </ul>	сне После этог устройство	о начнется ), и появито	процесс : я соответ	загрузки изменен тствующее уведо	ний на рмление	
	Внесены изменения которые еще не	е установлены на устройство	Установить политику 🕕 С	публиковать измен	ения Отменит	гь изменения		
Список устройств								
📘 Конфигурации	🔲 Политики 🖍							
- Анализ политик	Межсетевой экран 🔹	Межсетевой экран: polic	cy_2 policy_2 Network	~				+ Добавить •••
. Отслеживание измен		□ Nº	Name	Action	Enabled	Source	Destination	Services & Applications
С отслежниците номен С Администратор	policy_1 policy_2 Standard Ф Статус задач	. 1	Drop from Groups to hosts	× Drop		group3 group2 group1 group4_any ose_device ExternalZone	interoperable .domain.ruasac2_ h323 gw CP_default_Office_Mode_addresses_poo I IPv6_Link_Local_Hosts	a_tcp_10 a_tcp_20 a_tcp_any_dns AH cachefsd CP_rtm dest-unreach echo ftp-pasv FW1_ica_ FW1_uaa group_w H323 home-agent igmp Madster MS-SQL-Monitor_UDF NoBackO pop-3 sip_dynamic_ports
		2	<u>Cleanup rule</u> Reject Any to Domain Clone	× Drop × Reject		None	Any .domain.ru_Clone	#hashtags     1000m       115-audio     1337x.c       360 Mobile Manager       51.com-music     510       6rounds     8Tracks       app-site     Alcohol & T       Entertainment     ex.cd       None
		4	Drop empty traffic	× Drop		None	None	None
		Найдено записей: 8						
«								

≓   КУПОЛ	Главная > Список устройств > Расширенные настройки CheckPoint > Межлетерой экони Задача на установку успешно создана Х								
Управление	CheckPoint 222	<ul> <li>IP-адрес</li> <li>10.229.0.222</li> </ul>	Вендор CheckPoint						
Пабочий стол									
🔡 Список устройств	Внесены изменения которые еще не	установлены на устройство	Установить политику	публиковать изме	Отменит	ь изменения			
[ 👌 Конфигурации FQ Анализ политик	<ul> <li>Политики</li> <li>Межсетевой экран</li> </ul>	<b>Межсетевой экран:</b> poli	cy_2 policy_2 Network	~				+ Добавить …	
о Отслеживание измен	policy 1	N⁰	Name	Action	Enabled	Source	Destination	Services & Applications	
<u>С</u> Администратор	роіюу_1 policy_2 Standard	□ 1 чения задачи воз взделе	Drop from Groups to hosts	× Drop		group3 group2 group1 group4_any ose_device ExternalZone	interoperable .domain.ruasac2_ h323 gw CP_default_Office_Mode_addresses_poo I IPv6_Link_Local_Hosts	a_tcp_10 a_tcp_20 a_tcp_any_dns AH cachefsd CP_rtm dest-unreach echo ftp-pasv FW1_ica_ FW1_uaa group_w H323 home-agent igmp Madster MS-SQL-Monitor_UDF NoBackO pop-3 sip_dynamic_ports	
		<ul> <li>2</li> <li>3</li> <li>4</li> </ul>	Cleanup rule Reject Any to Domain Clone Drop empty traffic	× Drop × Reject × Drop		None Any None	Any .domain.ru_Clone None	#hashtags     1000m       115-audio     1337x.c       360 Mobile Manager       51.com-music     510       6rounds     8Tracks       app-site     Alcohol & 1       Entertainment     ex.co       None     None	
«		Найдено записей: 8							

≓∣купол	Главная 🖒 Список устройств 🖒 Расширенные настройки CheckPoint 🖒 Статус задач					义 Администратор
Управление	CheckPoint 222   BeHdop CheckPoint CheckPoint					
Рабочий стол	0.1					
🔠 Список устройств	Внесены изменения которые еще на в несены изменения которые еще на в на в несены изменения которые еще на в на в несены изменения которые еще на в на в на в не в на в на	е установлены на устроиство Установить политику	(!) Опубликовать изменения	Отменить изменения		
🕞 Конфигурации	🗐 Политики		В процессе			
<del> </del>	Межсетевой экран 🔺	отатус задач все псудачно успешно	впроцессе			
Отслеживание измен	policy_1	Задача 	Статус	Дата создания		
	policy_2	Policy Installation - policy_1	В процессе	28.11.2024 18:54:00		
С Администратор	Standard		впроцессе	20.11.2024 15.10.00		
	🖉 Статус задач	В данном разделе отображан	отся созданные			
		задачи на применение измен	ений, а также их			
		статус и время выполнения				
*						

Н ∣ КУПОЛ	Главная Список устройств Раси	ииренные настройки CheckPoint 🗲 Статус задач		义 Администратор
Управление	С Для того, чтоб устройства, до	ы посмотреть настройки другого остаточно перейти обратно в спис	ок	
Рабочий стол	устройств			
Список устройств	Внесены изменения которые еще н	е установлены на устроиство Установить политику	Опубликовать изменения	
🕞 Конфигурации	🔳 Политики 🖍			
न्तू Анализ политик	Межсетевой экран	Статус задач Все Неудачно Успешно	В процессе	
Отслеживание измен	policy_1	Sagava	Статус Дата создания	20
	policy_2	Policy Installation - policy_1 Policy installation - policy_2	В процессе 28.11.2024 19:34.	00
С Администратор	Standard			
	🖉 Статус задач			
*				

Установка глобальной политики межсетевого взаимодействия.

Кейс 1: мы хотим запретить доступ из публичной зоны в DMZ и обратно. Если где-то появится политика, противоречащая этой глобальной политике, то мы хотим об этом узнать и получить рекомендации по устранению.

Кейс 2: мы хотим контролировать отсутствие «дыр» в политиках, которые могут позволить проникнуть в инфраструктуру. Для этого нам нужно обязательно понимать контекст всех устройств.

Н   КА⊔ОУ	Отслеживание изменений		🗘 🔍 Смирнов
Управление	С Отслеживание изменений Трекеры Контроль зон Контроль пол	і інтик МЭ	
🏠 Рабочий стол			
🔡 Список устройств	Матрицы зон безопасности Сетевые зон	ы	
📘 Конфигурации	Список зон + Добавить	Подсети SecurityZone1	+ Добавить \Xi 🚥
न्तू Анализ политик	Q Поиск	Тип IP-адрес	
Отслеживание измен	Trusted	Хост 10.112.1.3	
Со Алминистратор	Untrusted	Как осуществлять проверку нарушений зонального комплаенса правилами?	
	Management	В НОТА КУПОЛ.Управление реализована возможность составлять требований к проходящему по сети трафику на основе зон безопасности,	
	SecurityZone1	а также для сопоставлять эти требовании с правилами межсетевого экрана	
	MDZ	Диапазон 192.178.1.1 - 192.178.1.142	
	ZoneCluster1	Диапазон 192.178.2.1 - 192.178.2.142	
	ZoneCluster2		
	SecurityZone2		
	SevurityZone3		
	LocalZone		
~	LocalZone3	Найдено записей: 7	« < 1 из 1 > » 10 v

Н   КА⊔О∨	Отслеживание изменений							ф 🛛 Смирнов
Управление	🖸 Отслеживание изменений							
🟠 Рабочий стол	Трекеры Контроль зон	Контроль поли	тик МЭ					
🔡 Список устройств	Матрицы зон безопасности	Сетевые зоны						
🕞 Конфигурации	Список зон	Для нача	па необходимо оп	пределить зоны и вход	дящие в них подсети, чтоб рикретной зоне. Пля этого	бы нало	+ до	бавить = …
- Q Анализ политик	Q. Поиск	перейти н	а вкладку «Сетев	вые зоны»		Падо		
Отслеживание измен	Trusted		Хост	10.112.1.3				
	Untrusted		Хост	10.112.2.3		$\searrow$		
Администратор	Management		Хост	10.112.3.3				
	SecurityZone1		Подсеть	10.112.4.1/24				
	MDZ		Диапазон	192.178.1.1 - 192.178.1.142				
	ZoneCluster1		Диапазон	192.178.2.1 - 192.178.2.142				
	ZoneCluster2							
	SecurityZone2							
	SevurityZone3							
	LocalZone							
~	LocalZone3		Найдено записей: 7				≪ < 1 из	1 > » 10 ~

≓   КУПОЛ	Отслеживание изменений		Ф 🖇 Смирнов
Управление С Рабочий стол	Отслеживание изменений Трекеры Контроль зон Контроль пол	итик МЭ	
Список устройств	Матрицы зон безопасности Сетевые зон	si	
🗜 Конфигурации	Список зон + Добавить	Подсети SecurityZone1	🕂 Добавить \Xi 🚥
- Q Анализ политик	Q. Поиск	Пип IP-адрес	
Отслеживание измен	Trusted	<b>X</b> oct 10.112.1.3	
Co A	Untrusted	<b>X</b> OCT 10.112.2.3	
а Администратор	Management	Xoct 10.112.3.3	
	SecurityZone1	Подсеть 10.112.5.1/24	
	MDZ	Диапазон 192.178.1.1 - 192.178.1.142	
	ZoneCluster1	Диапазон 192.178.2.1 - 192.178.2.142	
	ZoneCluster2		
	SecurityZone2		
	SevurityZone3		
	LocalZone	В блоке слева отображаются созданные ранее зоны, которые в последстви <u>и будут</u>	
~	LocalZone3	использоваться в зональном анализе	« < <u>1</u> из 1 > » <u>10</u> ч

Н   КА⊔ОѴ	Отслеживание изменений		Ф 🔍 Смирнов		
Управление Пабочий стол	Отслеживание изменений Трекеры Контроль зон Контроль пол	итик МЭ			
🔡 Список устройств	Матрицы зон безопасности Сетевые зон	ы			
📘 Конфигурации	Список зон + Добавить	Подсети SecurityZone1	+ Добавить = …		
	Q Поиск	Тип IP-адрес			
Отслеживание измен	Trusted	О Хост 10.112.1.3			
	Untrusted	О Хост 10.112.2.3			
а Администратор	Management	Хост         10.112.3.3			
	SecurityZone1	Подсеть 10.112.5.1/24			
	MDZ	Диапазон 192.178.1.1 - 192.178.1.142			
	ZoneCluster1	Диапазон 192.178.2.1 - 192.178.2.142			
	ZoneCluster2	У каждой зоны есть набор IP-адресов, которь	е будут учитываться в анализе		
	SecurityZone2				
	SevurityZone3				
	LocalZone				
~	LocalZone3	Найдено записей: 7	« < 1 из 1 > » 10 v		
Н   КА⊔ОУ	Отслеживание изменений				🗘 🔗 Смирнов
--------------------------	--	--------------------	-----------------------------	-------------------------------	---------------------
Управление	🖸 Отслеживание изменений				
🏠 Рабочий стол	Трекеры Контроль зон Контроль поли	итик МЭ			
🔡 Список устройств	Матрицы зон безопасности Сетевые зонь	I			
<b>Го</b> Конфигурации	Для того, чтобы добавить зоны в а	анализ, перейдите			+ Добавить \Xi 🚥
<b>FQ</b> Анализ политик	на вкладку «матрицы зон безопас Q Поиск	ности»	IP-адрес		
Отслеживание измен	Trusted	Хост	10.112.1.3		
	Untrusted	Хост	10.112.2.3	$\langle \mathcal{F} \rangle$	
🗳 Администратор	Management	Хост	10.112.3.3		
		Подсеть	10.112.4.1/24		
	SecurityZone1	Подсеть	10.112.5.1/24		
	MDZ	Диапазон	192.178.1.1 - 192.178.1.142		
	ZoneCluster1	Диапазон	192.178.2.1 - 192.178.2.142		
	ZoneCluster2				
	SecurityZone2				
	SevurityZone3				
	LocalZone				
~	LocalZone3	Найдено записей: 7			« < 1 из 1 > » 10 v

Н ∣ КА⊔ОУ	Отслеживание изменений	Отслеживание изменений												
Управление П Рабочий стол	Отслеживание изменений Трекеры Контроль зон Контроль полит	ітик МЭ												
  Список устройств	ойств Матрицы зон безопасности Сетевые зоны													
Конфигурации	Список матриц Все матрицы С конфликта	ами				+ Добавить \Xi 🚥								
Отслеживание измен	П Название	Размер Устройства	Статус анализа	Последний анализ	Конфликты	Описание								
	Mатрица требований по зонам Cluster	🗰 6x6 🔛 5	🕢 Успешно	30.11.2024 15:47:00	<u>(</u> ) 15	Данная матрица отображает эталонные значения поли								
😋 Администратор	<b>Требования основных зон для UserGate</b>	🗰 5x5 🔡 3	🐼 Успешно	101.12.2024 10:34:00	() 7	В матрице отражены основные требования, предьявля								
—	Mатрица LocalZone	🌐 15x15 🛛 🏭 1	🛞 Ошибк	02.12.2024		Проверка всех зон на соответствие внутри Cisco 🛱 …								
	Mатрица для трафика по CheckPoint	1 7x7	× Анализ не Невозмо для выпо	жно подключиться к устройствам олнения анализа		В матрице настраиваются связи для проверки проходя								
	На этой вкладке отображается таб ранее матрицами. Также есть возм информацию по проведению анал	блица с уже созданными можность посмотреть пиза и статус выполнени	я			« < 1 из 1 > » 10 ~								
~	Найдено записей: <b>3</b>					≪ < 1_из1 > :								

Н ∣ КА⊔ОУ	Отслеживание изменений						Ф 🖇 Смирнов							
Управление	Отслеживание изменений Трекеры Контроль зон Контроль полит	Отслеживание изменений Трекеры Контроль зон Контроль политик МЭ												
Писок устройств	Матрицы зон безопасности Сетевые зоны													
[З Конфигурации = Анализ политик	Список матриц Все матрицы С конфликтан	ами					+ Добавить \Xi 🚥							
отслеживание измен	Название	Размер	Устройства	Статус анализа	Последний анализ Для созд	ания матрицы для з	онального анализа,							
	Mатрица требований по зонам Cluster	🗰 6x6	5	🕑 Успешно	Нажмите 30.11.2024 15:4	на кнопку «дооавит	Б»							
🔇 Администратор	<b>Требования основных зон для UserGate</b>	5x5	3	🕗 Успешно	1.12.2024 10:34:00	7 В матрице отра	ажены основные требования, предьявля							
	Mатрица LocalZone	15x15	88 1	🛞 Ошибка	02.12.2024	Проверка всех	зон на соответствие внутри Cisco 🛛 🛱 🛶							
	Mатрица для трафика по CheckPoint	🗰 7x7	88 1	× Анализ не проводился		В матрице наст	граиваются связи для проверки проходя							
	Найдено записей: 3						« < 1 из 1 > » 10 ч							
~														

# $\exists \Box \Box \Box \Box | \mathsf{KAUOV}$

Н ∣ КА⊔ОИ	Отслеживание изменений	Добавить матрицу зон ×							
Управление	Отслеживание изменений							Название * Демонстрационная матрица	
🏠 Рабочий стол	Трекеры Контроль зон Контроль полит	тик МЭ					_	Сетевые зоны * Trusted × Untrusted ×	
🔡 Список устройств	Матрицы зон безопасности Сетевые зоны							Management × SecurityZone1 ×	
🔓 Конфигурации			✓ Trusted						
	Список матриц Все матрицы С конфликта		Untrusted DB:						
Отслеживание измен	Название	Размер У	Устройства	Статус анализа	Последний анализ	Конфликты	Описан	Management	
	Mатрица требований по зонам Cluster	🗰 6x6	<b>H</b> 5	🕗 Успешно	30.11.2024 15:47:00	() 15	Данная	SecurityZone1	
🖉 Администратор	<u>Требования основных зон для UserGate</u>	₩ 5x5	3	🕗 Успешно	01.12.2024 10:34:00	() 7	В матри	MDZ	
	Mатрица LocalZone	🌐 15x15	88 1	😣 Ошибка	02.12.2024		Провер		
	Матрица для трафика по CheckPoint	1 7x7	88 1	× Анализ не проводился			выбрать сетевые зоны, укажите		
								название и устройство для анализа. После этого нажмите на кнопку «Сохранить»	
	Найдено записей: 3								
~								Сохранить Отмена	

Н   КУПОЛ	Отслеживание изменений						Ф 🖇 Смирнов
Управление Пабочий стол	Отслеживание изменений Трекеры Контроль зон Контроль полити	к МЭ					
Список устройств	Матрицы зон безопасности Сетевые зоны						
FQ Анализ политик	Список матриц Все матрицы С конфликтами	И					+ Добавить \Xi 🚥
Отслеживание измен	Название	Размер	Устройства	Статус анализа	Последний анализ	Конфликты	Описание
	Демонстрационная матрица	🗰 4x4	88 1	× Анализ не проводился			Данная матрица позволяет определить требования к у
😋 Администратор	Новая матрица отобразится в таблице матриц. Для перехода детальной настройке матрицы, нажмите на ее название		3	Успешно	30.11.2024 15:47:00	() 15	Данная матрица отображает эталонные значения поли
		к	<b>##</b> 1	🕗 Успешно	101.12.2024 10:34:00	(!) 7	В матрице отражены основные требования, предьявля
		15	88 1	😣 Ошибка	02.12.2024		Проверка всех зон на соответствие внутри Cisco ASA
	Mатрица для трафика по CheckPoint	₩ 7x7	6	× Анализ не проводился			В матрице настраиваются связи для проверки проходя
	Найдено записей: <b>3</b>						« < 1 из 1 > » 10 ~
~	· · · · · · · · · · · · · · · · · · ·						

≓∣КУПОЛ	Отслеживание изменени	й > Матрица 1											
Управление	🖸 Отслеживание изменений												
Рабочий стол	Трекеры Контро	Трекеры Контроль зон Контроль политик МЭ											
Список устройств	Матрицы зон безопа	Матрицы зон безопасности Сетевые зоны											
Конфигурации	← Назад Демонстрационная матрица Анализ еще не проводился Анализировать												
Отслеживание измен		Назначение	=										
	Источник \Xi	Trusted	Untrusted	Management	SecurityZone1								
Администратор	Trusted	→	≯	≯	₹								
	Untrusted	≯	→	≯	≯								
	Management	≯	≯	Ð	₩								
	SecurityZone1	≯	≯	×	₽								
	Матрица ото	ображается в	виде ячеек, гд	де									
	каждая ячей зоной источ	іка представл іника и зоной	яет связь меж назначения	кду									
~~													

≓∣купол	Отслеживание изменени	й > Матрица 1											
Управление	🗵 Отслежив	ание измене	ений										
<b>С</b> Рабочий стол	Трекеры Контро	ль зон Контрол	њ политик МЭ										
🔡 Список устройств	Матрицы зон безопасности Сетевые зоны												
Конфигурации По Анадиа долитик	← Назад Демонстрационная матрица Анализ еще не проводился Анализировать												
Отслеживание измен		Назначение =											
	Источник =	Trusted	Untrusted	Management	SecurityZone1								
🖄 Администратор	Trusted	→	₹	₹	≯								
	Untrusted	≯	Для настр выберите	ойки связи м соответствун	ежду зонами, ощую ячейку								
	Management	≯	≯	$\rightarrow$	≯								
	SecurityZone1	≯	×	⇒	⇒								
~													

## $\exists \Box \Box \Box \Box | \mathsf{KAUOV}$

Н   КУПОЛ	Отслеживание изменени	й > Матрица 1	Настройка связи между зонами 🛛 🗙					
Управление П Рабочий стол	Отслежие Трекеры Контро	зание измени оль зон Контро	<b>ЭНИЙ</b> ль политик МЭ				<ul> <li>→ Источник Trusted</li> <li>⊚ Назначение Untrusted</li> </ul>	
🔡 Список устройств 🄀 Конфигурации	Матрицы зон безопа	сности Сетевь	іе зоны				Тип доступа → Открытое подключение	
Анализ политик           Отслеживание измен		<ul> <li>→ ● Частичное подключение</li> <li>→ Подключение запрещено</li> </ul>						
😂 Администратор	Источник = Trusted	Trusted →	Untrusted	Management	SecurityZone1		Описание Сервисы	
	Untrusted	∢		*	≯		Блокировать Разрешить Список сервисов	
	Management	≯	≯	€	H		tcp = 1-100 × udp = 1-100 × http × Дополнительные условия	
	SecurityZone1	≯	≯	≯	Ð		<ul><li>Явный источник</li><li>Явное назначение</li></ul>	
						В настройках связи между зонами можно указать требования к проходящему трафику. Для сохранения изменений необходимо	💿 Явная служба	

Н   КА⊔ОУ	Отслеживание изменений 🔸 Матрица 1									
Управление А Рабочий стол	С Отслеживание изменений Трекеры Контроль зон Контроль политик МЭ									
Список устройств	Матрицы зон безопасности Сетевые зоны									
[3] Конфигурации = Анализ политик	← Назад Демонстрационная матрица Анализ еще не проводился Анализировать									
Отслеживание измен	Назначение = Исто IHI Trusted → Untrusted Jsted Minagement SecurityZone1									
🔗 Администратор	Частичное подключение Trusted PA3PEШИТЪ: tcp = 1-100 udp = 1-100 ↓ ↓ ↓ ↓									
	Untruster http > > > >									
	Мапа После применения изменений, ячейка в матрице обновляется. Для того, чтобы посмотреть настройки									
	Secu связи, необходимо навести курсор на									
~										

Н ∣ КА⊔ОИ	Отслеживание изменени	Отслеживание изменений > Матрица 1												
Управление П Рабочий стол	Отслежие Трекеры Контро	зание измено оль зон Контро	<b>ЕНИЙ</b> ль политик МЭ											
Список устройств	Матрицы зон безопа	Матрицы зон безопасности Сетевые зоны												
Га Конфигурации Го Анализ политик	← Назад Демонстрационная матрица Анализ еще не проводился Анализировать После того, как матрица и связи настроены, можно приступать к зональному анализу. Для этого надо													
Отслеживание измен		Назначение =		Management	SecurityZone1	нажать на кнопку «Анализировать»	J							
С Администратор	Источник = Trusted	→	→											
	Untrusted	≯	→	→	≯									
	Management	₹	为	→	₹									
	SecurityZone1	→	₹	→	→									
«														

Н ∣ КА⊔ОИ	Отслеживание изменени	й > Матрица 1					🗘 🙁 Смирнов						
Управление Правочий стол	Отслежие Трекеры Контро	ание измено оль зон Контро	<b>ЕНИЙ</b> ль политик МЭ										
🔡 Список устройств	Матрицы зон безопасности Сетевые зоны												
<ul> <li>Конфигурации</li> <li>Анализ политик</li> </ul>	<ul> <li>← Назад Демонстрационная матрица</li> <li>① Найдено <u>6 конфликтов</u>   Анализ от 27.11.2024 09:26:00</li> <li>Результаты зонального анализа отображаются в заголовке матрицы, а также в ячейках связи. Найденные конфликты отображают несоответствия правил МЭ на устройстве, заданным с помощью зон требованиям</li> </ul>												
отслеживание измен	Источник =	Trusted	Untrusted	Management	SecurityZone1	на устройстве, заданным с помощью зон требованиям							
Са Администратор	Trusted	→	<b>–</b> <sup>0</sup>	<b>6</b> 0	€0								
	Untrusted	≯	→	→	₽								
	Management	₹	≯	Ð	₹								
	SecurityZone1	→	Ð	<b>_</b> 0	→								
~													

Н ∣ КА⊔ОѴ	Отслеживание изменений > Матрица 1												
Управление П Рабочий стол	ий стол к устройств Матрицы зон безопасности Сетевые зоны												
 В Список устройств													
Ца Конфигурации Ед Анализ политик	← Назад Демоно	трационная матри	<b>ца</b> () Найдено <u>6</u>	<u>конфликтов</u>   Аналі	из от 27.11.2024 09:26	00 Анализировать							
Отслеживание измен	Источник =	<b>Назначение</b> = Trusted	Untrusted	Management	SecurityZone1								
Са Администратор	Trusted	→	<b>_</b>	<b>-</b> 0	<b>1</b>								
	Untrusted	≯	Для просм на ячейку	отра конфлик матрицы	та, необходим	о нажать							
	Management	≯	≯	→	≯								
	SecurityZone1	→	<mark>€</mark> 0	<b>-</b> 0	→								
~													

# $\exists \Box \Box \Box \Box | \mathsf{KAUOV}$

≓∣купол	Отслеживание изменени	й > Матрица 1				Разрешение конфликт	та			×
Управление	🖸 Отслежие	вание измен	ений			→ Источник Trusted	Назначение           Untrusted			
🏠 Рабочий стол	Трекеры Контро	оль зон Контро	оль политик МЭ			Параметр связи	Связь в матрице	Анализ правил	Принятие изменений	
🔡 Список устройств	Матрицы зон безопа	сности Сетевь	ые зоны			Тип доступа	🔸 Частичное подключение	🔸 Частичное подключение	Частичное	~
[] Конфигурации	-					Сервисы	• Разрешить	• Разрешить	Разрешить	~
Q Анализ политик	← Назад Демон	страционная матр	ица 🕛 Найдено	<u>6 конфликтов</u>   Ана	ализ от 27.11.2024 09:26:00	Список сервисов	₀ <sup>©</sup> tcp = 1-100 ₀ <sup>©</sup> udp = 1-100	₀ <sup>©</sup> tcp = 1-35635 ₀ <sup>©</sup> udp	tcp=1-35635 × udp=1-100 ×	~
Отслеживание измен	Источник =	<b>Назначение</b> <del>П</del> Trusted	Untrusted	Management	SecurityZone1		¦å http	₀⁰ http ₀⁰ https	http × https ×	
🖉 Администратор					- 0	Явный источник				
	Trusted	$\rightarrow$	<b>-</b>			Явное назначение				
	Untrusted	₩	⇒	€	<b>₩</b>	Явная служба				
	Management	≯	⇒	→	₹	На экране разр о текущей связ	ешения отображается и в матрице и фактичес	нформация кой связи		
	SecurityZone1	→	<b>→</b> <sup>0</sup>	<b>-</b> 0	→	между зонои по	о обнаруженному прави	пу		
~						Принять изменения	Отмена			

Н   КА⊔ОѴ	Отслеживание изменени	й > Матрица 1				Разрешение конфликта ×					
Управление	🖸 Отслежив	ание измене	ений			→ Источник Trusted	<ul> <li>Назначение</li> <li>Untrusted</li> </ul>				
ሰ Рабочий стол	Трекеры Контро	оль зон Контро	ль политик МЭ			Параметр связи	Связь в матрице	Анализ правил	Принятие изменений		
🔡 Список устройств	Матрицы зон безопа	сности Сетевь	іе зоны			Тип доступа	🔸 Частичное подключение	→ Частичное подключение	Частичное 🗸		
🔓 Конфигурации						Сервисы	• Разрешить	• Разрешить	Разрешить 🗸		
	← Назад Демон	страционная матр	ица 🕛 Найдено	о <u>6 конфликтов</u>   Ана	лиз от 27.11.2024 09:26:00	Список сервисов	• tcp = 1-100	o tcp = 1-35635	tcp=1-35635 ×		
. Отслеживание измен		Назначение =	-				o <sup>g</sup> udp = 1-100	ु <sup>©</sup> udp ु <sup>©</sup> http	udp=1-100 × V		
	Источник =	Trusted	Untrusted	Management	SecurityZone1			o <sup>©</sup> https	nttp × nttps ×		
<b>С</b> а Алминистратор						Явный источник					
	Trusted	<b>→</b>	<b></b>			Явное назначение					
	Untrusted				<b>_</b> 0	Явная служба					
	ondusted										
	Management	₩	≯	$\rightarrow$	≯			Есть возможность принять обнаруженно			
		_			_			правило за требова между зонами. Посл	ние, или изменить связь le выбора новых		
	SecurityZone1	$\rightarrow$	<b>→</b>		<b>→</b>			параметров связи, н конфликт, нажав на	еобходимо разрешить кнопку «Принять		
								изменения»			
~						Принять изменения	Отмена				

Н ∣ КА⊔ОИ	Отслеживание изменени	Отслеживание изменений > Матрица 1									
Управление Пабочий стол	Отслеживание изменений Трекеры Контроль зон Контроль политик МЭ										
🔡 Список устройств	Матрицы зон безопа										
🚦 Конфигурации = д Анализ политик	← Назад Демонстрационная матрица ① Найдено <u>6 конфликтов</u>   Анализ от 27.11.2024 09:26:00 Анализировать										
Отслеживание измен		Назначение \Xi									
Са Администратор	Источник =	Trusted	Untrusted	Необ	Необходимо изменить настройки в правилах,						
	Trusted	→	E <sup>0</sup>								
	Untrusted	K	Ð			Скачать отчет и закрыть					
	Management	K	≯	Ð	K	После разрешения конфликта, появится возможность скачать отчет и посмотреть правила, в которые необходимо внести изменения					
	SecurityZone1	→	<b>₽</b>	<b>-</b> 0	Ð						
~											

Задача 1: Вернуть систему к состоянию «До нелигитимных/ошибочных/несоответствующих политикам изменений» в случае их изменения сотрудниками компании или злоумышленником.

*Кейс:* Что-то в работе устройства/сети пошло не так, и нужно быстро откатить инфраструктуру к рабочему состоянию.

Задача 2: Сравнить разные версии политик на одном или разных устройствах между собой. *Кейс:* понять, почему сотрудник потерял доступ к ресурсу.

 $H \circ T \circ H \circ T \circ$ 

Н   КА⊔ОѴ	Главная > Конфигурации > Резервні	ые копии				2 admin
Управление	Конфигурации					
Рабочий стол	Резервные копии Избранное	Сравнение				
Список устройств	Устройства					+ Добавить = …
Конфигурации	🗌 Устройство 🍦	ІР-адрес	≑ Вендор	≑ Дата последней загрузки ≑		
न् <sub>Q</sub> Анализ политик	UserGatev7	10.229.0.194	"j <mark>i</mark> " UserGate	02.10.2024 17:55:59		
	CiscoASA	172.31.142.14	cisco Cisco	03.10.2024 00:47:18		
Администратор	UserGatev6	172.31.142.174	uji UserGate	03.10.2024 08:52:38		
	CheckPoint Gateway	10.229.0.117	CheckPointGateway			
	Continent4 - CUS	172.31.142.242	🗞 Код Безопасности			
	CheckPoint SMS	10.229.0.224	😍 CheckPoint			
		В раздел	е «Резервные копии»	хранятся все конфигурации,		
		которые	были собраны с подк	люченных устройств.		
		Полдерж	ивается два режима с	сбора конфигураций:		
		Автол				
		• Ручна	я загрузка	1/1/V		
u	Найдено записей: 6				« <	1 из 1 > » 50 ∨

≓   КА⊔ОУ	Главная > Конфигурации > Резервные копии	Настройка хранилища 🛛 🗙 🗙
Управление	В Конфигурации	Кол-во хранимых копий на устройстве 1000
Рабочий стол	Резервные копии Избранное Сравнение	90 дн
🔡 Список устройств	Устройства	Частота сбора автобэкапов
🌔 Конфигурации	🔲 Устройство 🗢 IP-адрес 🗢 Вендор 🇢 Дата последней загрузки 🗘	частота автоматического сохранения конфигураций с поддерживаемых устройств
FQ Анализ политик	UserGatev7 10.229.0.194 👘 UserGate 📋 02.10.2024 17:55:59	1 🗘 Дней 🗡
	CiscoASA 172.31.142.14 tito Cisco 🛱 03.10.2024 00:47:18	
	UserGatevó     Настройка расписания для сбора конфигураций       CheckPoint Gateway     10.229.0.117	
	Сontinent4 - CUS 172.31.142.242 Соколасности	
**	Найдено записей: 6	Сохранить Отменить

≓∣ КУПОЛ	Главная 🗲 Конфигурации 🗲 Резервные колии		2 admin
Управление	В Конфигурации	Загрузить конфигурацию	
Рабочий стол	Резервные копии Избранное Сравн		
🔡 Список устройств	Устройства	Ð	+ Добавить \Xi 🚥
[ В Конфигурации	Устройство	Переместите сюда файлы	
	UserGatev7 10.229	или	
	CiscoASA 172.3	Выбрать файл	
<u><u><u></u> Администратор</u></u>	UserGatevó 172.3		
	CheckPoint Gateway 10.229	Устройство * Контекст * Версия ОС *	
	Continent4 - CUS 172.3	etete CiscoASA (172.31.142.14) admin 9.12	
	CheckPoint SMS 10.229	Описание	
		Сохранить Отменить	
		Ручная загрузка файлов конфигураций	
<i>"</i>	Найдено записей: 6		« < 1 из 1 > » 50 ч

#### $\exists \Box \Box \Box \Box | \mathsf{KAUOV}$

хупол	Главная 🖒	Конфигурации > Резервные н	копии ус	Главная > Конфигурации > Резервные копии устройства											
вление	C K	онфигурации													
ій стол	Резервные копии Избранное Сравнение														
сустройств	← Назад	← Назад 🗰 Cisco ASA 172.31.142.14													
турации	Конфи	гурации												+ Добавить	. <del>.</del> .
политик		Название	Å	Тип	\$	Контекст	\$	Версия ОС	\$	Размер файла 🏻 🌲	Дата добавления	\$	Описание	\$	
ивание измен		admin context.txt		Загружена вручную		admin		9.12		469 Кб	03.12.2024 15:31:10		admin context		
		cisco_Context2_config_auto_back	up.cfg	Загружена автоматическ	и	Context2		9.1		5 K6	03.12.2024 14:50:08				
истратор		cisco_Context1_config_auto_back	up.cfg	Загружена автоматическ	и	Context1		9.1		4 Кб	03.12.2024 14:50:04				
		cisco_admin_config_auto_backup.	<u>cfg</u>	Загружена автоматическ	и	🖺 admin		9.1		468 Кб	📋 03.12.2024 14:50:01				
		cisco_Context2_config_auto_back	up.cfg	Загружена автоматическ	и	Context2		9.1	Дл: их	я всех загруженн просмотра	ных конфигураций д	осту	лен функцис	нал	
		cisco_Context1_config_auto_back	up.cfg	Загружена автоматическ	и	Context1		9.1		4 Кб	02.12.2024 17:01:30				
		cisco_admin_config_auto_backup.	cfg	Загружена автоматическ	и	admin		9.1		468 Кб	02.12.2024 17:01:27				
		cisco_Context2_config_auto_back	up.cfg	Загружена автоматическ	и	Context2		9.1		5 K6	29.11.2024 08:45:38				
		cisco_Context1_config_auto_back	up.cfg	Загружена автоматическ	и	Context1		9.1		4 Кб	29.11.2024 08:45:35				
		cisco_admin_config_auto_backup.	cfg	Загружена автоматическ	и	admin		9.1		468 Кб	29.11.2024 08:45:31				
		cisco_Context2_config_auto_back	up.cfg	Загружена автоматическ	и	Context2		9.1		5 Кб	20.11.2024 14:06:33				

# $\exists \Box \Box \Box \Box | \mathsf{KAUOV}$

∺   КУПОЛ	Главная 🗲 Конфигурации 🗲 Резервные копии	устройства				Просмотр конфигурации cisco_admin_config_auto_backup.cfg			
Управ∧ение ∩ Рабочий стол	Конфигурации Резервные копии Избранное Сравнов	: Saved : : Serial Number: JMX172180D3 : Hardware: ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz : ASA Version 9.1(7)32 <context></context>							
Список устройств	← назад :::::: Сізсо ASA 172.31.142.14			! terminal width 511 hostname ciscoasa					
С Конфигурации	Конфигурации					domain-name wr enable password V.4uENRzFUL&cwtA encrypted names ! interface Ethernet0/0			
о] Отслеживание измен	Название 💠	Тип 💠	Контекст	Версия ОС \$	Размер	nameif OUTSIDE security-level 0 ip address 172.31.142.14 255.255.255.0			
	<u>admin context1xt</u> <u>cisco_Context2_config_auto_backup.cfg</u>	Загружена вручную Загружена автоматически	Context2	9.12	409 Ko 5 K6	! interface Ethernet0/1 nameif INSIDE security-level 100			
С Администратор	cisco_Context1_config_auto_backup.cfg	Загружена автоматически Загружена автоматически	Context1	9.1	4 K6 468 K6	ip address 172.31.143.15 255.255.255.0 ! interface Management0/0 nameif Management			
	<u>cisco_Context2_config_auto_backup.cfg</u>	Загружена автоматически	Context2	9.1	5 Кб	security-level 0 no ip address			
	<u>cisco_Context1_config_auto_backup.cfg</u>	Загружена автоматически	Context1	9.1	4 K6	! time-range test absolute start 10:27 18 January 2024			
	cisco_Context2_config_auto_backup.cfg	Загружена автоматически	Context2	9.1	5 K6	! time-range test2 absolute start 08:08 15 February 2024			
	<u>cisco_Context1_config_auto_backup.cfg</u>	Загружена автоматически	Context1	9.1	4 Кб	periodic weekend 3:00 to 23:59 periodic daily 0:00 to 23:59 periodic Wednesday Friday Saturday 0:00 to 23:59			
	cisco_admin_config_auto_backup.cfg	Загружена автоматически	음음 Context2	9.1	468 K6	periodic Wednesday 0:00 to Friday 23:59 ! time-range test3			
	cisco_Context1_config_auto_backup.cfg	Загружена автоматически	Context1	9.1	4 Кб	absolute start 11:10 25 March 2024 end 11:10 25 March 2025 ! time-range test4			
<u> </u>	Найдено записей: 35					absolute end 11:11 25 March 2026 ! time-range test5 absolute end 11:12 25 March 2028 periodic weekend 0:00 to 23:50			

# СРАВНЕНИЕ КОНФИГУРАЦИЙ

Н ∣ КА⊔ОѴ	Главная > Конфигурации > Сравнение		ф 🔍 Смирнов
Управление	В Конфигурации		
Рабочий стол	Резервные копии Избранное Срав	нение	
Список устройств	Конфигурация 1		
🕞 Конфигурации	Устройство Вендор	Раздел «Сравнение конфигураций» позволяет обнаружить несанкционированные изменения в конфигурациях устройств.	
	Устроиство * Cisco ASA 172.31.142.14	Для сравнения необходимо выбрать две конфигурации	
Отслеживание измен	Контекст admin	(сравнение возможно как в рамках одного устройства, так и разных устройств одного вендора).	
Со Администратор	Конфигурация * cisco_admin_config_auto_backup.cfg v 18.11.2024, 10:05		
	Конфигурация 2 текущая Устройство Вендор Устройство *	В качестве первой конфигурации выбираем ту, с которой хотели бы сравнить текущую конфигурацию.	
	Cisco ASA 172.31.142.14	Заполните параметры для сравнения	
	Контекст V	Вторая конфигурация проставляется автоматически на основе выбранных параметров. Она считается текущей конфигурацией.	
	Конфигурация * cisco_admin_config_auto_backup.cfg v 02.12.2024, 17:01		
	Параметры сравнения		
	Сравнение Глобальные настройки		
	Сравнить	При нажатии на «Сравнить» запускается процесс сравнения.	
~			

# СРАВНЕНИЕ КОНФИГУРАЦИЙ

≓∣ КУПОЛ	Главная 🕻 Конфигурации 🕻 Сравнение		义 Смирнов
Управление	🔉 Конфигурации		
Ф Рабочий стол	Резервные копии Избранное Срав	нение	
🔡 Список устройств	Устройство *		
🕃 Конфигурации	Cisco ASA 172.31.142.14	Сравнение 🕂 8 🔀 3 💽 Показывать только отличия Переключение в режим просмотра полной конфигурации	
- Анализ политик	Контекст admin		
Отслеживание измен	Конфигурация * cisco_admin_config_auto_backup_2024 ∨ 03.12.2024, 16:37	Конфигурация 1       Конфигурация 2         1317       object-group protocol protocol	
Администратор	Конфигурация 2 текущая	+ 1318 protocol-object ip + 1319 protocol-object udp + 1320 protocol-object top	
	Устройство Вендор	+     1321     protocol-object icmp       +     1322     protocol-object ssh	
	Сівсо ASA 172.31.142.14	x 1325 access-list mgmt_access_out extended permit ip host 170.36. 250.14 interface OUTSIDE log warnings interval 88 + 1331 access-list mgmt_access_out extended permit ip host 173 16.25 interface OUTSIDE log warnings interval 88	. 165 .
	admin Конфигурация *	<pre>x 1327 access-list mgmt_access_out extended permit object protocol_obj any any log critical</pre>	
	cisco_admin_config_auto_backup_2.cfg V 03.12.2024, 16:38	× 1330 access-list outside_access_out extended permit object service_protocol_name host 141.196.79.149 any log alerts + 1334 access-list outside_access_out extended permit object service_tcp host 141.196.79.149 any log alerts	
	Параметры сравнения	Раскрыть все 127 строк	
	Сравнение Глобальные настройки		
	Сравнить		

# СРАВНЕНИЕ КОНФИГУРАЦИЙ

Н   КА⊔О∨	Главная 🗲 Конфигурации 🗲 Сравнение		义 Смирнов
Управление	Конфигурации		
🟠 Рабочий стол	Резервные копии Избранное Сра	внение	
🔡 Список устройств	Конфигурация 1		
🔀 Конфигурации	Устройство Вендор	Сравнение 🕂 8 🔀 3 💽 Показывать только отличия	Быстрая навигация по найденным отличиям 🔹 🔿 🗸
	Устройство * Сіѕсо ASA 172.31.142.14		
<b>5</b> .2 -	Контекст	Конфигурация 1	Конфигурация 2
о Отслеживание измен	admin	1323 port-object range www 90	I3∠9 port-object range www.90
	Конфигурация *	1324 access-list mgmt_access_out remark description	1330 access-list mgmt_access_out remark description
	cisco_admin_config_auto_backup_2024 V	access-list mgmt_access_out extended permit ip host 170.36	access-list mgmt_access_out extended permit ip host 173.165.
😂 Администратор	03.12.2024, 16:37	250. 14 interface OUTSIDE log warnings interval 88	16.25 interface OUTSIDE log warnings interval 88
	Конфигурация 2 текущая	access-list mgmt_access_out extended permit tcp object-group- 1326 er DM_INLINE_USER_1 any any object-group TCP_GROUP_all log er rs	-us access-list mgmt_access_out extended permit tcp object-group-us rro 1331 er DM_INLINE_USER_1 any any object-group TCP_GROUP_all log erro rs
	Устройство Вендор	<pre>x 1327 any any log critical</pre>	obj
	Cisco ASA 172.31.142.14	access-list mgmt_access_out extended permit object-group TCPU 1328 any any log	JDP access-list mgmt_access_out extended permit object-group TCPUDP
	admin	access-list mgmt_access_out extended permit object-group PROT 1329 GROUP2 any any log	TO1333 GROUP2 any any log
	Конфигурация * cisco_admin_config_auto_backup_2.cfg v 03.12.2024, 16:38	<pre>x 1330 x 13</pre>	+ 1334 access-list outside_access_out extended permit object service_tcp host 141.196.79.149 any log alerts
		1331 access-list outside_access_out remark New	1334 access-list outside_access_out remark New
	Параметры сравнения	1332 access-list outside_access_out remark Test12345	1335 access-list outside_access_out remark Test12345
	Сравнение	1333 access-list outside_access_out remark Test12345	1336 access-list outside_access_out remark Test12345
	Глобальные настройки		

# КАРТА СЕТИ

Задачи:

- Проанализировать маршрут прохождения трафика, чтобы понять, доступен ли он или нет, и если нет, то почему.
- Провести анализ векторов атак определить, компенсируют ли политики ИБ наличие известных уязвимостей.

Кейс 1: «дебаг» политик, когда пользователь потерял доступ к ресурсу.

Кейс 2: анализ возможности доступа к уязвимому ресурсу.

#### КАРТА СЕТИ — ПОСТРОЕНИЕ МАРШРУТОВ



#### КАРТА СЕТИ — СОЗДАНИЕ МАРШРУТА

#### $H \odot \bot G | KAUOV$



#### КАРТА СЕТИ — СОЗДАНИЕ МАРШРУТА

#### $H \odot T G | KYNOV$



#### КАРТА СЕТИ — НАСТРОЙКИ МАРШРУТА



#### КАРТА СЕТИ — ПРОСМОТР МАРШРУТОВ

#### $\exists \Box \Box \Box | \mathsf{KYHOV}$



#### КАРТА СЕТИ — ПРОСМОТР МАРШРУТОВ

#### 



# ЦЕНТР ЗАПРОСОВ

Предположим, что каждая задача отлично работает сама по себе, но теперь нужно связать несколько сотрудников между собой.

Задача: автоматизация рассмотрения заявок на доступы,а именно:

- анализ поступивших заявок на соответствие политикам
- ускорение процесса предоставления доступа (система рекомендует правило, автоматизация применения изменений)
- контроль возможных ошибок до применения политик на устройствах
- унификация процесса и согласование.

Н	$\bigcirc$	T	C	Η	$\bigcirc$	T	$\mathbb{C}$
$\bigcirc$	Т	$\bigcirc$	Η	$\bigcirc$	Т	$\bigcirc$	H
T	$\mathbb{C}$	Η	$\bigcirc$	Т	$\bigcirc$	Η	$\bigcirc$
$\mathbb{C}$	Η	$\bigcirc$	Т	$\bigcirc$	Η	$\bigcirc$	T
Η	$\bigcirc$	Т	$\mathbb{C}$	Η	$\bigcirc$	Т	$\Box$
$\bigcirc$	T	$\bigcirc$	Η	$\bigcirc$	Т	$\bigcirc$	Н
Т	$\mathbf{C}$	Η	$\bigcirc$	Т	$\mathbb{C}$	Η	$\bigcirc$
$\mathbb{C}$	Η	$\bigcirc$	T	$\bigcirc$	Η	$\bigcirc$	Т
Н	$\bigcirc$	T	$\mathbb{C}$	Н	$\bigcirc$	T	$\Box$
$\bigcirc$	T	$\bigcirc$	Η	$\bigcirc$	Т	$\mathbb{C}$	Н
T	$\mathbf{C}$	Η	$\bigcirc$	T	$\mathbb{C}$	Η	$\bigcirc$
$\mathbb{C}$	H	$\bigcirc$	Т	C	H	С	Т
H	$\bigcirc$	T	C	H	$\bigcirc$	T	C

#### ЦЕНТР ЗАПРОСОВ — РАБОЧИЕ ПРОЦЕССЫ

≓∣ КУПОЛ	Центр запросов				🗘 🙁 Смирнов
Управление Пабочий стол	Центр запросов           Запросы         Рабочие процессы				
🔡 Список устройств	Процессы Черновики				+ Добавить \Xi 🚥
<b>Го</b> Конфигурации	П Название	Тип	<b>ä</b> . <sup>9</sup>		
न्तू Анализ политик	Новый процесс	Общий		ія процесса мониторинга сет	
Отслеживание измен	Управление задачами и проектами	Изменения досту		зервное копирование конфи	
С Центр запросов	Анализ и планирование	Изменения досту		гемы мониторинга уязвимос	
🖁 Карта сети	Обеспечение безопасности	Общий	запроса	реализация процедур реагир	
Ø Уязвимости	Управление рисками	Изменения объен	Прежде чем мы начнем работать с запросом, необходимо	гемы мониторинга уязвимос	
	Анализ эффективности работы	Общий		ія процесса мониторинга сет	
<b>Са</b> Алминистратор	Обеспечение безопасности	Общий	настраиваемое готовое автоматизированное решение для	тивности и результативност	
	Анализ и планирование	Пользовательски	управления изменениями купол. управления	зервное копирование конфи	
	Управление задачами и проектами	Общий	Начать	ія процесса мониторинга сет	
	Управление задачами и проектами	Общий	🗙 Устаревший 📄 01.01.2022 15:43 Автоматиза	ция процесса мониторинга сет	
*	Найдено записей: 3				« < 1 из 1 > » 10 ~

#### ЦЕНТР ЗАПРОСОВ — РАБОЧИЕ ПРОЦЕССЫ

≓∣ КУПОЛ	Центр запросов					Ф Я СМИ	ірнов
Управление	ъ Центр запросов						
<b>П</b> Рабочий стол	Запросы Рабочие процессы						
🔡 Список устройств	Процессы Черновики					+ Добавить =	
<b>Го</b> Конфигурации	Название	Тип	Статус	Дата создания	Описание	Чтобы начать создание рабочего процесса, нажмите «+Лобавить»	
<b>-</b> С Анализ политик	<u>Новый процесс</u>	Общий	👴 Активный	1.01.2022 15:43	Автоматизация процесса мониторинга сет		_
Отслеживание измен	Управление задачами и проектами	Изменения доступа	÷, Неактивный	01.01.2022 15:43	Регулярное резервное копирование конфи		
<b>С</b> Центр запросов	Анализ и планирование	Изменения доступа	🔆 Неактивный	01.01.2022 15:43	Создание системы мониторинга уязвимос		
<b></b> Карта сети	Обеспечение безопасности	Общий	🔆 Неактивный	01.01.2022 15:43	Разработка и реализация процедур реагир		
Ø Уязвимости	Управление рисками	Изменения объекта	🔆 Неактивный	01.01.2022 15:43	Создание системы мониторинга уязвимос		
	Анализ эффективности работы	Общий	👴 Активный	01.01.2022 15:43	Автоматизация процесса мониторинга сет		
🗳 Администратор	Обеспечение безопасности	Общий	👌 Активный	01.01.2022 15:43	Оценка эффективности и результативност		
	Анализ и планирование	Пользовательский	🔆 Неактивный	01.01.2022 15:43	Регулярное резервное копирование конфи		
	Управление задачами и проектами	Общий	🗙 Устаревший	01.01.2022 15:43	Автоматизация процесса мониторинга сет		
	<u>Управление задачами и проектами</u>	Общий	🗙 Устаревший	01.01.2022 15:43	Автоматизация процесса мониторинга сет		
	Найлено записей: 3					« ( 1 up 1 ) » 10	
	Hangeno bannoch. O						

#### **ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ** ⊣ С ⊤ С | КУПОЛ

Н ∣ КА⊔ОУ	Центр запросов > Процесс 1					
Управление	🕞 Создать рабочий процесс					
🏠 Рабочий стол	Настройки процесса					
🔡 Список устройств	Haapauwa *					
[ 👌 Конфигурации	Изменение доступа	Этап. создание запроса				
<b>-</b> Анализ политик	Описание	Название этапа * Создание запроса				
Отслеживание измен	безопасности сети, включая правила доступа и защиту от атак	Описание этапа				
🔓 Центр запросов	О Использовать шаблон					
📱 Карта сети	Тип рабочего процесса					
Ø Уязвимости	Общий	Название * Срок выполнения 🗄 Описание * Срок действия 🗎 Устройство 🗸 🕂 Файл Вложение 🐮 Ссылка на внешний запрос				
	Мы могли бы выбрать один из готовых шаблонов, но в этой	🗱 Пользовательское поле •••• 🗱 Новое поле •••				
Со Администратор	демонстрации мы создадим новый рабочий процесс с нуля	+ Добавить поле				
	Утверждение	<ul> <li>Ответственные</li> </ul>				
	🗄 Согласование 🔓 🥶 💽	Тип назначения Тип выполнения				
	Внедрение	Все выбранные Параллельное				
	Проверка	Список пользователей * + Добавить •••				
		Добавьте ответственных				
~	Запустить рабочий процесс Отменить В чернов	ики				

#### **ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ** ⊣ С ⊤ С | КУПОЛ

Н   КА⊔ОУ	Центр запросов > Процесс 1	Ф 🗙 Смирнов		
Управление	🕞 Создать рабочи			
<b>П</b> Рабочий стол	Настройки процесса			
🔠 Список устройств	Название *			
[ 👌 Конфигурации	Изменение доступа		Этап. Создание запроса	цуолировать этап
<b>FQ</b> Анализ политик	Описание Создание и регулярное обновление политик безопасности сети, включая правила доступа и защиту от атак		Название этапа * Создание запроса	
Отслеживание измен			Описание этапа	
🔓 Центр запросов	О Использовать шаблон			
🖁 Карта сети	Тип рабочего процесса	~	~ Поля	
Ø Уязвимости	На		Название *	
	Этапы	+ Добавить	+ Добавить поле	
Администратор	Создание запроса		Добавляем поля, которые	
			потреоуются для оораоотки запроса	
				1.44
			Список пользователеи *	+ дооавить •••
			~	
			Добавьте ответственных	
			+ Добавить	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Запустить рабочий процесс Отм	в чернови	СИ	
#### **ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ** $\bowtie$ $\Box$ $\Box$ $\Box$ $\Box$ $\Box$ $\forall$ $\Box$ $\Box$

Н   КА⊔ОѴ	Центр запросов > Процесс 1		Добавить поле ×
Управление	🕞 Создать рабочий процесс		Тип поля Изменение доступа  × ^
<b>П</b> Рабочий стол	Настройки процесса		Текстовое поле
Список устройств Конфигурации	Название * Измецение поступа	Этап: Создание запроса	Множественный выбор Изменение доступа
	Описание	Название этапа * Создание запроса	Объект
Отслеживание измен	Создание и регулярное основление политик безопасности сети, включая правила доступа и защиту от атак	Описание этапа	Устроиство
Центр запросов	О Использовать шаблон	^ Поля	доступа»
Уязвимости	Тип рабочего процесса 🗸 🗸	Название *	
С Администратор	Этапы + Добавить	+ Добавить поле	
	Создание запроса	Ответственные	
		Тип назначения Тип выполнения Все выбранные Параллельное	·
		Список пользователей *	
		2	
		Добавьте ответственных	
		+ Добавить	
			Добавить Отмена

#### **ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ** $\bowtie$ $\Box$ $\Box$ $\Box$ $\Box$ $\Box$ $\forall$ $\Box$ $\Box$

Volumentary         Image: Comparing particulary         Image: Comparing parting particulary         Image:		Центр запросов > Процесс 1		Настраиваем и добавляем поле «Изменение доступа»
<ul> <li>Product of the formation project of the p</li></ul>	Управление	🕞 Создать рабочий процесс		Тип поля Изменение доступа
<ul> <li>Concervence of a procession of a</li></ul>	Рабочий стол	Настройки процесса		Подсказка
+ добавить	<ul> <li>Ш Список устройств</li> <li>Конфигурации</li> <li>□ Анализ политик</li> <li>□ Отслеживание измен</li> <li>□ Центр запросов</li> <li>∴ Карта сети</li> <li>⊙ Уязвимости</li> <li>∴ Администратор</li> </ul>	Настройки процесса Название * Изменение доступа Описание Создание и регулярное обновление политик безопасности сети, включая правила доступа и защиту от атак Использовать шаблон Тип рабочего процесса Этапы + Добавить Создание запроса	Этат: Содание запроса         Флоние запа         Описание запа         • Поля         Название *         • Добавить поле         • Ответственные         Ти название ма         Все выбранные       У пыполнения         Слисок пользователей *	<ul> <li>Обязательно для заполнения</li> <li>Разрешить редактирование</li> <li>Выполнение анализа рисков</li> <li>Выполнение анализа политик</li> <li>Использование топологий</li> <li>Настройки NAT</li> </ul>
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		+ Добавить	Добавить Отмена

Н   КА⊔ОУ	Центр запросов > Процесс 1	Ф 🖇 Смирнов
Управление	🕞 Создать рабочий процесс	
Рабочий стол	Настройки процесса	
Список устроиств Конфигурации	Название * Изменение доступа	Этап: Создание запроса
न्तू Анализ политик	Описание Создание и регулярное обновление политик	Название этапа * Создание запроса
отслеживание измен С Центр запросов	оезопасности сети, включая правила доступа и защиту от атак	Описание этапа
<b></b> Карта сети	Тип рабочего процесса 🗸	Поля
(9) Уязвимости	Этапы + добавить	Название* Пописание •••• Номонстике доступа •••• Настраиваем пользователей, которые будут ответственны за обработку запроса на данном этапе
<b>С</b> а Администратор	Создание запроса	^ Ответственные
		Тип назначения Все выбранные Тип выполнения Параллельное
		Список пользователей *
		24
		Добавьте ответственных + Добавить
~	Запустить рабочий процесс Отменить В чернови	

Н   КА⊔ОИ	Центр запросов > Процесс 1		ф 🞗 Смирнов
Управление	🕞 Создать рабочий процесс		
Рабочий стол	Настройки процесса		
<ul> <li>Список устроиств</li> <li>Конфигурации</li> </ul>	Название * Изменение доступа	Этап: Создание запроса	🛛 Дублировать этап 🛛 🚥
<b>F</b> Q Анализ политик	Описание Создание и регулярное обновление политик	Название этапа * Создание запроса	
Отслеживание измен	безопасности сети, включая правила доступа и защиту от атак	Описание этапа	
🖁 Карта сети	<ul> <li>использовать шаблон</li> <li>Тип рабочего процесса</li> </ul>	л Поля	
Ø Уязвимости	Этапы + Добавить	Название * Списание ••• Изменение доступа ••• Секция	
🖉 Администратор	Создание запроса	<ul> <li>+ Добавить поле</li> <li>Ответственные</li> </ul>	
		Тип назначения Тип выполнения Казана Каз	
		Список пользователей *	+ Добавить 😶
		2	
		Добавьте ответственных	
~	Запустить рабочий процесс Отменить В чернові	Мы уже выбрали тип назначения и выполнения, поэтому далее нажимаем кнопку «+Добавить», чтобы выбрать необходимых пользователей	

≓∣купол	Центр запросов > Процесс 1		Добавить пользователей	×
Управление	🕞 Создать рабочий процесс		Название Имя пользователя Сервер Имя домен	на
Рабочий стол	Настройки процесса		✓ vgruzdev Груздев Василий Локальный	
Список устройств Конфигурации	Название * Изменение доступа	Этап: Создание запроса	dsmirnov Дмитрий Смирнов Локальный	
	Описание Создание и регулярное обновление политик	Название этапа * Создание запроса	<ul> <li>аргізоч Призов Дмитрии Локальный</li> <li>Группа 1</li> </ul>	
[ð] Отслеживание измен	безопасности сети, включая правила доступа и защиту от атак	Описание этапа	dsmirnov Дмитрий Смирнов Astra LDAP domain_sm	iirnov
- Центр запросов - Карта сети	О Использовать шаблон	^ Поля	удизисти удили         удизисти и сородного	lirnov
<b>ම</b> Уязвимости	Тип рабочего процесса 🗸 🗸	Название * Описание •••• Изменение доступа	dsmirnov Дмитрий Смирнов Локальный	_
🔇 Администратор	Этапы + добавить	+ Добавить поле	akalashnikov     Калашников Андрей     Active Directory     domain_sm       vgruzdev     Груздев Василий     Astra LDAP     domain_sm	nirnov
	Создание запроса	<ul> <li>Ответственные</li> <li>Тип назначения</li> <li>Тип выполнени</li> </ul>	ия	
		Все выбранные Параллельно	oe	
		Список пользователей *		
		4		
			Выбрано записей: 2 из 47 <u>Снять выделение</u> « < 1 из 5 > » 10	
«			Добавить Отмена Отмена Отмена Отмечаем необходимых пользователей и нажима кнопку «Добавить»	аем

Н   КУПОЛ	Центр запросов > Процесс 1		🛕 🔍 Смирнов
Управление	🕞 Создать рабочий процесс		
Рабочий стол	Настройки процесса		
ЕН Список устроиств           Конфигурации	Название * Изменение доступа	Этап: Создание запроса	🕒 Дублировать этап 🛛 …
FQ Анализ политик	Описание Создание и регулярное обновление политик	Название этапа * Создание запроса	
отслеживание измен С Центр запросов	оезопасности сети, включая правила доступа и Защиту от атак	Описание этапа	
<b></b> Карта сети	Тип рабочего процесса 🗸	л Поля	
Ø Уязвимости	Этапы + Добавить	Название * Пописание •••• Название *••• Название *•••• Название *••• Название *•••• Название *••••• Название *••••• Название *••••• Название *••••• Название *•••••••••• Название *••••••••••••••••••••••••••••••••••••	
Са Администратор	Создание запроса	<ul> <li>Ответственные</li> </ul>	
	Также добавляем и настраиваем	Тип назначения Тип выполнения Сарадованные Парадлельное	
	неооходимые этапы	Список пользователей *	+ Добавить 🚥
		ii orgruzdev Груздев Василий et orgruphic dsmirnov	
		👬 🖵 дмитрий Смирнов	
~	Запустить рабочий процесс Отменить В черновин		

#### **ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ** $\bowtie$ $\Box$ $\Box$ $\Box$ $\Box$ $\Box$ $\forall$ $\Box$ $\Box$

Н   КА⊔ОѴ	Центр запросов > Процесс 1		🗘 🔗 Смирнов				
Управление	🕞 Создать рабочий процесс						
П Рабочий стол	Настройки процесса						
<ul> <li>Список устроиств</li> <li>Конфигурации</li> </ul>	Название * Изменение доступа	Этап: Создание запроса	🕒 Дублировать этап 🛛 🚥				
FQ Анализ политик	Описание Создание и регулярное обновление политик безопасности сети, включая правила достипа и	Название этапа * Создание запроса					
С Центр запросов	защиту от атак	Описание этапа					
Карта сети Уязвимости	Тип рабочего процесса 🗸 🗸	▲ Поля Название * Полисание *** Пзменение доступа ****					
	Этапы + Добавить	+ Добавить поле					
🕰 Администратор	Создание запроса	<ul> <li>Ответственные</li> </ul>					
	Обработка	Тип назначения Тип выполнения Все выбранные Параллельное					
	завершение	Список пользователей *	+ Добавить …				
		иgruzdev Груздев Василий					
		🗱 🗆 dsmirnov Дмитрий Смирнов					
	После нажимаем кнопку «Запустить рабочий процесс», чтобы использоват его для обработки запросов	ь					
~	Запустить рабочий процесс Отменить В чернови	ки					

#### ЦЕНТР ЗАПРОСОВ — ЗАПРОСЫ

### $\exists \Box \Box \Box \Box | \mathsf{KAUOV}$

Н   КА⊔О∨	Центр запросов									¢	🔍 Смирнов
Управление П Рабочий стол	<b>Ъ Центр</b> Запросы Ра	запросов абочие процессы									
Список устройств	Все запросы	Мои запросы Черновики Архии	3							+ Добавить	s <b>∓ …</b>
📘 Конфигурации	🗌 Номер	Название	э	ά.			ecc	Назначено	Последнее изменение	Создатель	Создано 1
न्तू Анализ политик	136117	Сетевой экран блокирует приложение	E			•		Призов Д.А.		🝳 Чекунов С.В.	1.01.2
Отслеживание измен	136117	Открыть порты открыть для cSNA	E	A? N.		1.5	риком	义 Призов Д.А.	1.01.2022 15:43	🔍 Чекунов С.В.	📋 01.01.2
С Центр запросов	136117	Новое правило в firewall151	Как созд	ать запрос			риком	义 Призов Д.А.	01.01.2022 15:43	🔍 Чекунов С.В.	<b>Ö</b> 01.01.2
🖁 Карта сети	136117	<u>Блокировка DMZ</u>	После того,	как был создан	рабочий процес	с, мы можем		义 Призов Д.А.	1.01.2022 15:43	🔍 Смирнов А.Д.	📋 01.01.2
Ø Уязвимости	136117	Новое правило в firewall151	приступить	к созданию зап	роса		жтом	义 Призов Д.А.	01.01.2022 15:43	义 Чекунов С.В.	<b>Ö</b> 01.01.2
	136117	Открыть порты открыть для cSNA	8			Начать		义 Призов Д.А.	1.01.2022 15:43	义 Чекунов С.В.	1.01.2
😋 Администратор	136117	Сетевой экран блокирует приложение	<u>.</u>	• - p - p,	-			义 Призов Д.А.	01.01.2022 15:43	义 Чекунов С.В.	1.01.2
	136117	Новое правило в firewall151	🇱 Новый	Низкий	0	Общий		义 Призов Д.А.	1.01.2022 15:43	🔍 Чекунов С.В.	1.01.2
	136117	Новое правило в firewall151	🇱 Новый	Высокий	0	Общий		Призов Д.А.	01.01.2022 15:43	义 Чекунов С.В.	📋 01.01.2
	136117	Сетевой экран блокирует приложение	🔽 Выполнено	Низкий	0	Общий		义 Призов Д.А.	01.01.2022 15:43	义 Чекунов С.В.	1.01.2
«	Найдено записей:	: 15							~	< 1 из 2 >	» 10 ~

#### $H \odot \bot \Box |$ КУПОЛ

≓∣ КУПОЛ	Центр запросов								Ţ	🔍 Смирнов
Управление	ъ Центр	запросов								
🏠 Рабочий стол	Запросы Ра	бочие процессы								
🔡 Список устройств	Все запросы	Мои запросы Черновики Архив							+ Добавить	÷
<b>Го</b> Конфигурации	🗌 Номер	Название	Этап	Приоритет	Комментарии	Рабочий процесс	Назначено	Нажмите кнопку чтобы начать со	«+Добавить», здание запроса	Создано 1
<b>-</b> Анализ политик	136117	Сетевой экран блокирует приложение	🔅 Новый	Высокий	📮 З	Общий	Призов Д.А.	01.01.2022 15:43	义 Чекунов С.В.	📋 01.01.2
Отслеживание измен	136117	<u>Открыть порты открыть для cSNA</u>	В работе	Средний	🟳 1	Работа с трафиком	Призов Д.А.	01.01.2022 15:43	🔍 Чекунов С.В.	01.01.2
С Центр запросов	136117	Новое правило в firewall151	🔅 Новый	Низкий	0	Работа с трафиком	Призов Д.А.	1.01.2022 15:43	🔍 Чекунов С.В.	01.01.2
<b>Р</b> Карта сети	136117	<u>Блокировка DMZ</u>	🔅 Новый	Низкий	0	Общий	Призов Д.А.	01.01.2022 15:43	🔍 Смирнов А.Д.	01.01.2
Ø Уязвимости	136117	Новое правило в firewall151	🔅 Новый	Низкий	0	Работа с объектом	Призов Д.А.	01.01.2022 15:43	🔍 Чекунов С.В.	01.01.2
	136117	Открыть порты открыть для cSNA	🔅 Новый	Низкий	0	Общий	Призов Д.А.	01.01.2022 15:43	🔍 Чекунов С.В.	<b>Ö</b> 01.01.2
🕼 Администратор	136117	Сетевой экран блокирует приложение	🔅 Новый	Средний	<b>D</b> 5	Общий	Призов Д.А.	01.01.2022 15:43	🔍 Чекунов С.В.	<b>Ö</b> 01.01.2
	136117	Новое правило в firewall151	🔅 Новый	Низкий	D 0	Общий	义 Призов Д.А.	01.01.2022 15:43	🔍 Чекунов С.В.	📋 01.01.2
	136117	Новое правило в firewall151	🔅 Новый	Высокий	D 0	Общий	Призов Д.А.	01.01.2022 15:43	🝳 Чекунов С.В.	📋 01.01.2
	136117	Сетевой экран блокирует приложение	И Выполнено	Низкий	0	Общий	Призов Д.А.	01.01.2022 15:43	义 Чекунов С.В.	📋 01.01.2

Найдено записей: 15

« < 1 из 2 > » 10 ~

Найдено записей: 15

#### $H \odot T G | KYNOV$

≓∣ КУПОЛ	Центр запросов					¢	🔍 Смирнов
Управление	<ul> <li>Центр запросов</li> <li>Запросы Рабочие процессы</li> </ul>						
<b>ြ)</b> Рабочий стол		r					
🔡 Список устройств	Все запросы Мои запросы Черновики Ар					+ Добавить	÷
🎝 Конфигурации	Номер Название	Создать запрос Выберите рабочий процесс		Назначено	Последнее изменение	Создатель	Создано 1
FQ Анализ политик	П 136117 Сетевой экран блокирует приложение	Q. Поиск		义 Призов Д.А.	01.01.2022 15:43	🝳 Чекунов С.В.	<b>Ö</b> 01.01.2
Отслеживание измен	136117         Открыть порты открыть для cSNA			义 Призов Д.А.	1.01.2022 15:43	🔍 Чекунов С.В.	🛱 01.01.2
С Центр запросов	136117         Новое правило в firewall151	Изменение доступа Создание и регулярное обновление политик безопасности се	Изменения объекта	义 Призов Д.А.	01.01.2022 15:43	🝳 Чекунов С.В.	<b>Ö</b> 01.01.2
🖁 Карта сети	136117         Блокировка DMZ	Управление задачами и проектами	Изменения объекта	义 Призов Д.А.	1.01.2022 15:43	🔍 Смирнов А.Д.	📋 01.01.2
Ø Уязвимости	136117         Новое правило в firewall151	Анализ и планирование	Изменения доступа	义 Призов Д.А.	01.01.2022 15:43	义 Чекунов С.В.	<b>Ö</b> 01.01.2
	136117         Открыть порты открыть для cSNA	Обеспечение безопасности	Общий	🙁 Призов Д.А.	01.01.2022 15:43	义 Чекунов С.В.	6 01.01.2
🔇 Администратор	136117 Сетевой экран блокирует приложение			🙁 Призов Д.А.	01.01.2022 15:43	🔍 Чекунов С.В.	6 01.01.2
	136117         Новое правило в firewall151	управление рисками	Общии	义 Призов Д.А.	1.01.2022 15:43	🔍 Чекунов С.В.	📋 01.01.2
	136117         Новое правило в firewall151	Анализ эффективности работы	Пользовательский	Призов Д.А.	01.01.2022 15:43	🝳 Чекунов С.В.	런 01.01.2
	П 136117 Сетевой экран блокирует приложение		Отмена Продолжить	义 Призов Д.А.	01.01.2022 15:43	📯 Чекунов С.В.	<b>Ö</b> 01.01.2
		Выберите раннее созданный рабоч	ний процесс				

« < 1 из 2 > » 10 ~

≓∣купол	Центр запросов 🚿 Добавить запро	oc			Ф 🖇 Смирнов
Управление	🕞 Создать запрос			Заполните поля запроса необходимой информацией	
<b>П</b> Рабочий стол	Детали запроса				
🔡 Список устройств 🅞 Конфигурации	Приоритет: 💿 🛔 Низкий	🔿 Средний 🔿 Выс	окий		
<b>FQ</b> Анализ политик	Название				
[6] Отслеживание измен	Описание *				
<ul> <li>Центр запросов</li> <li>Карта соти</li> </ul>	^ Изменение доступа				
Марта сети Уязвимости	Устройство Checkpoint2151	~			
	Действие	Источник	Назначение	Сервис	
🖄 Администратор		✓ + Добавить	+ Добавить	+ Добавить	
	Комментарий				
	+ Добавить изменение доступа				
~	Отправить Отменить В ч	ерновики			

	Центр запросов 🔹 Добавить	запрос	После заполнения отправьте запрос	После заполнения полей необходимой информацией, отправьте запрос на обработку, предварительно выбрав необходимых участников для спелующего этала обработки		×
правление	🕞 Создать запрос		песоходимых уче	спиков для следнощего зтапа сорасотки	Ответственный Чекунов С.В.	~
Рабочий стол	Детали запроса				Комментарий	
<ul> <li>Список устройств</li> <li>Конфигурации</li> </ul>	Приоритет: 💿 🛔 Низки	ій 🔿 Средний 🔿 🛛 Высог	кий			
<b>FQ</b> Анализ политик	Название Сетевой экран блокирует п	риложение				
Отслеживание измен	Описание * Сетевой экран блокирует п безопасности.	риложение, потому что оно пытается получить	доступ к определённым ресурсам или по	ортам, которые были заблокированы в настройках		
- Центр запросов - Карта сети	<ul> <li>Изменение доступа</li> </ul>	a				
<b>@</b> Уязвимости	Устройство Checkpoint2151	~				
	Действие	Источник	Назначение	Сервис		
😤 Администратор	Accept	<ul> <li>✓</li> <li>192.168.1.1</li> <li>NAT: 255.255.125.1:888</li> <li>192.168.1.1/255.255.255.0</li> <li>NAT: 255.255.125.1:888</li> <li>+ Добавить</li> </ul>	192.168.1.1 + Добавить	₀ <sup>©</sup> DNS + Добавить		
	Комментарий					
	+ Добавить изменение до	оступа				
~					Отправить Отмена	J

₩   КУПОЛ <sub>Управление</sub>	Центр запросов 🔸 Задача на lorem ipsum dolor sit amet							
	← ि Сетевой экр Низкий приоритет	ан блокирует приложение						
<ul><li>Рабочий стол</li><li>Список устройств</li></ul>	Запрос #136117 Взять в ра	боту Вернуть на предыдущий этап	Х Отклонить		🔎 Чат			
🔓 Конфигурации	Создатель Смирнов Д.А.							
🛱 Анализ политик	⑦ Создание запроса	Обработка	Завершение					
Отслеживание измен	Описание запроса							
🕞 Центр запросов	Сетевой экран блокирует прилох	кение, потому что оно пытается получить дост	уп к определённым ресурсам или портам, н	оторые были заблокированы в настройках безопасн	ости.			
🖁 Карта сети	<ul> <li>Изменение доступа</li> </ul>							
Ø Уязвимости	न्तू Анализ еще не проводило	ся Провести анализ						
	Действие	Источник	Назначение	Сервис				
	Accept	<b>192.168.1.1</b> NAT: 255.255.125.1:888 <b>192.168.1.1/255.255.255.0</b> NAT: 255.255.125.1:888	192.168.1.1	<sub>o</sub> o dns				
~	Комментарий Необходимо разрешить доступ по указанным параметрам, чтобы МЭ не блокировал приложение, при необходимости проведите анализ данных Проведите анализ по запросу изменения межсетевого доступа, чтобы получить информацию о возможных аномалиях и предложения по обновлению необходимых компонентов конфигурации устройств							

Н ∣ КУПОЛ	Центр запросов > Задача на lorem ipsum dolor sit a	amet	Анализ политик Х					
Управление	<ul> <li>Сетевой экран блокиру</li> <li>Низкий приоритет</li> </ul>	ует приложение						
<ul><li>Рабочий стол</li><li>Список устройств</li></ul>	Запрос #136117 Взять в работу Вернуть н	на предыдущий этап Х Отклонить	<ul> <li>Рекомендации</li> <li>В Checkpoint 1</li> </ul>					
<b>Го</b> Конфигурации	Создатель Смирнов Д.А.		<ul> <li>Аccess Control Policy</li> <li>Добавить новый сетевой объект host 192.168.1.1</li> </ul>	G C				
<b>F</b> Q Анализ политик	⑦ Создание запроса	Обработка Завершен	☐ Добавить новый сервисный объект DNS					
Отслеживание измен	Описание запроса		Low Security Policy					
С Центр запросов	Сетевой экран блокирует приложение, потому что с	оно пытается получить доступ к определённым	Добавить новый сетевой объект host 192.168.1.1					
🖁 Карта сети	<ul> <li>Изменение доступа</li> </ul>		Checkpoint 12					
Ø Уязвимости		ультаты Обновить анализ	<ul> <li>Outbound Policy</li> <li>Добавить новый сетевой объект host 192.168.1.1</li> </ul>					
Co	Действие Ист	очник Назнач	Добавить новый сервисный объект DNS					
Администратор	Accept 19: NA 19: NA	2.168.1.1 192.1 T: 255.255.125.1:888 2.168.1.1/255.255.255.0 T: 255.255.125.1:888						
~	Комментарий Необходимо разрешить доступ по указанным пара Просмотрите список реком конфигураций, и при необх конечным устройствам, ил	метрам, чтобы МЭ не блокировал приложение, п пендаций по изменению кодимости примените их к и изучите список аномалий,	Применить выбранные рекомендации Отмена	Применить все рекомендации				

¦ КУПОЛ Управление	Центр запросов > Задача на lorem ipsum dolor sit amet	Анализ политик Х					
	Сетевой экран блокирует приложение Низкий приоритет	Рекомендации Аномалии 11					
<ul><li>Рабочий стол</li><li>Список устройств</li></ul>	Запрос #136117 Взять в работу Вернуть на предыдущий этап Х Отклонить	<ul> <li>Рекомендации</li> <li>В Checkpoint 1</li> </ul>					
Конфигурации	Создатель Смирнов Д.А.	<ul> <li>Ассеss Control Policy</li> <li>Добавить новый сетевой объект host 192.168.1.1</li> <li>Добавить новый сервисный объект DNS</li> </ul>					
С Отслеживание измен	Описание запроса Соработка Завершен Описание запроса Сетевой экран блокирует приложение, потому что оно пытается получить доступ к определённым (	<ul> <li>Добавить новое правило Правило 1 как №23 Показать правило</li> <li>Low Security Policy</li> <li>Побавить числы й сетерей сбысить best 102 168 1 1</li> </ul>					
<ul> <li>Карта сети</li> <li>Уязвимости</li> </ul>	<ul> <li>Изменение доступа</li> <li>Анализ от 25.05.24.15:43</li> <li>Смотреть результаты</li> <li>Обновить анализ</li> </ul>	<ul> <li>Adodaburb Hobbin Cerebon object host 192.166.1.1</li> <li>Checkpoint 12</li> <li>Outbound Policy</li> </ul>					
Се Администратор	Действие Источник Назнач	<ul> <li>Добавить новый сетевой объект host 192.168.1.1</li> <li>Добавить новый сервисный объект DNS</li> </ul>					
	<ul> <li>Accept</li> <li>192.168.1.1</li> <li>NAT: 255.255.125.1:888</li> <li>192.168.1.1/255.255.255.0</li> <li>NAT: 255.255.125.1:888</li> </ul>						
	Комментарий Необходимо разрешить доступ по указанным параметрам, чтобы МЭ не блокировал приложение, г						
«	Просмотрите список рекомендаций по изменению конфигураций, и при необходимости примените их к конечным устройствам, или изучите список аномалий, которые могут возникнуть при внесении изменений	Применить выбранные рекомендации Отмена Применить все рекомендации					

Н ∣ КА⊔ОѴ	Центр запросов > Задача на I	lorem ipsum dolor sit amet	Комментарии События ×		
Управление	← 🕞 Сетевой эк Низкий приоритет	хран блокирует приложение			Пользователь Чекунов С.В. создал задачу 5 мая 2024 15:43
<ul><li>Рабочий стол</li><li>Список устройств</li></ul>	Запрос #136117 Взять в	работу Вернуть на предыдущий этап Х	<ul> <li>Пользователь Призов Д.А. изменил статус на: Статус</li> <li>5 мая 2024 15:43</li> </ul>		
[ <b>]</b> Конфигурации	Создатель Смирнов Д.А.		Пользователь Призов Д.А. внес изменения в поле Назначение Исходное значение:		
• Q Анализ политик	<ul> <li>Создание запрос</li> <li>Описание запроса</li> <li>Сетевой экран блокирует прил</li> </ul>	а Обработка Обработка	Новое значение: 192.168.1.1 5 мая 2024 15:43		
<ul> <li>Центр запросов</li> <li>Карта сети</li> </ul>	<ul> <li>Изменение доступа</li> </ul>				
Ø Уязвимости		3 Смотреть результаты Обновить анализ			
<b>С</b> Администратор	Действие	Источник	Назначение	Сервис	
	Accept	<b>192.168.1.1</b> NAT: 255.255.125.1:888 <b>192.168.1.1/255.255.255.0</b> NAT: 255.255.125.1:888	192.168.1.1	o <sup>©</sup> dns	
	Комментарий				
	Необходимо разрешить достуг	п по указанным параметрам, чтобы МЭ не блокирова	ал приложение, при необходимости пр	оведите анализ данных	
*					Просмотрите детальную историю изменений запроса

#### $\exists \Box \Box \Box \Box | \mathsf{KAUOV}$

∺∣ КУПОЛ	Центр запросов > Задача на lor	em ipsum dolor sit amet			<b>Комментарии</b> События	×		
Управление	← ⓑ Сетевой экр Низкий приоритет	ан блокирует приложение						
<ul><li>Рабочий стол</li><li>Список устройств</li></ul>	Запрос #136117 Взять в ра	боту Вернуть на предыдущий этап 🛛 🔿						
Конфигурации	Создатель Смирнов Д.А.							
-Q Анализ политик Отслеживание измен	<ul> <li>Создание запроса</li> <li>Описание запроса</li> </ul>	Обработка	Завершение		Проверьте правильность настроек брандмауэра и ACL на обоих устройствах. Призов Д.А. Локальный 5 мая 2024 15:43			
С Центр запросов	Сетевой экран блокирует прилож	кение, потому что оно пытается получить доступ	к определённым ресурсам или порта	ам, которые были заблокированы в настройках безоп	Постройте защищенный туннель для всех			
<ul> <li>Карта сети</li> <li>Уязвимости</li> </ul>	- Анализ от 25.05.24 15:43	Смотреть результаты Обновить анализ			соединении приложения. Исследуйте возможные уязвимости в приложении,			
🖉 Администратор	Действие	Источник	Назначение	Сервис	которые могут привести к блокировкам. Призов Д.А. Локальный 5 мая 2024 15:43			
	Accept	<b>192.168.1.1</b> NAT: 255.255.125.1:888 <b>192.168.1.1/255.255.255.0</b> NAT: 255.255.125.1:888	192.168.1.1	o <sup>©</sup> DNS	Обеспечьте шифрование данных предотвращения перехвата информа Непрочитанные сообщения	к для ации.		
	Комментарий Необходимо разрешить доступ п	о указанным параметрам, чтобы МЭ не блокиро	Проверьте настройки VPN и других средств безопасности, которые могут влиять на доступ к приложению. Призов Д.А. Локальный 5 мая 2024 15:43					
~			Оставить комментарий					

#### ЦЕНТР ЗАПРОСОВ — АРХИВЫ ЗАПРОСОВ

Н   КА⊔ОУ	Центр запросов								¢	Смирнов
Управление П Рабочий стол	<ul> <li>Центр запросов</li> <li>Запросы Рабочие процессы</li> </ul>		В случае инцидентов обратитесь к архиву запросов, которые раннее были завершены, чтобы ознакомиться с историей изменений и обсуждений пользователей							
🔡 Список устройств	Все запросы Мои запросы Черновики Архив = …									<b>≂</b>
🕞 Конфигурации	🗌 Номер	Название	Этап	Приоритет	Комментарии	Рабочий процесс	Последнее изменение	Создатель	Создано 个	
<b>-</b> Анализ политик	136117	Сетевой экран блокирует приложение	И Выполнено	Высокий	Д 3	Общий	1.01.2022 15:43	🔍 Чекунов С.В.	01.01.2022 15:43	
Отслеживание измен	136117	<u>Открыть порты открыть для cSNA</u>	Отклонено	Средний	🟳 1	Работа с трафиком	1.01.2022 15:43	🔍 Чекунов С.В.	📋 01.01.2022 15:43	
<b>С</b> Центр запросов	136117	Новое правило в firewall151	• Отклонено	Низкий	0	Работа с трафиком	1.01.2022 15:43	义 Чекунов С.В.	01.01.2022 15:43	
🖁 Карта сети	136117	<u>Блокировка DMZ</u>	И Выполнено	Низкий	□ 0 ▷	Общий	01.01.2022 15:43	Смирнов А.Д.	01.01.2022 15:43	•••
Ø Уязвимости	136117	Новое правило в firewall151	🗸 Выполнено	Низкий	0	Работа с объектом	01.01.2022 15:43	🔍 Чекунов С.В.	01.01.2022 15:43	
	136117	<u>Открыть порты открыть для cSNA</u>	🗸 Выполнено	Низкий	0	Общий	01.01.2022 15:43	🔍 Чекунов С.В.	01.01.2022 15:43	
🔇 Администратор	136117	Сетевой экран блокирует приложение	И Выполнено	Средний	5	Общий	01.01.2022 15:43	义 Чекунов С.В.	01.01.2022 15:43	
	136117	Новое правило в firewall151	И Выполнено	Низкий	0	Общий	01.01.2022 15:43	义 Чекунов С.В.	01.01.2022 15:43	
	136117	Новое правило в firewall151	🗸 Выполнено	Высокий	0	Общий	01.01.2022 15:43	🝳 Чекунов С.В.	01.01.2022 15:43	
	136117	Сетевой экран блокирует приложение	🗸 Выполнено	Низкий	0	Общий	01.01.2022 15:43	🝳 Чекунов С.В.	01.01.2022 15:43	
	L									
*	Найдено записей:	15						*	< <u>1</u> из 2 > »	10 ~

# 

## СПАСИБО ЗА ВНИМАНИЕ!



Игорь Душа

Директор портфеля решений по информационной безопасности НОТА КУПОЛ idusha@nota.tech ЗАПИСАТЬСЯ На персональную демонстрацию



