

Операционная инструкция Аналитика МСЭ

1. Типовые операции, выполняемые Аналитиком МСЭ

Аналитик МСЭ участвует в следующих сценариях работы Нетхаб:

1. «Управление запросом на изменение сетевого доступа»;
2. «Оптимизация конфигураций МСЭ»;
3. «Контроль легитимности сетевых доступов»;
4. «Контроль SLA».

Аналитик МСЭ управляет конфигурацией МСЭ и выполняет функции:

1. Подтверждение предложенного маршрута прохождения трафика;
2. При выявлении несоответствий реализованных настроек МСЭ с запрошенными проведение анализа несоответствий и информирование Координатора УСД о причинах несоответствий, подтверждает легитимность внесенных изменений;
3. При выявлении изменений настроек МСЭ, несвязанных или некорректно связанных с запросом на управление сетевым доступом, выбор и указание реквизитов корректного запроса или удаление некорректной связи;
4. Принятие решения о необходимости и способе оптимизации правил МСЭ.

При осуществлении указанных функций Аналитик МСЭ выполняет следующие операции:

1. Определение необходимости оптимизации правил МСЭ;
2. Выбор способа оптимизации правил МСЭ и формирование запросов;
3. Передача на реализацию смоделированных настроек МСЭ;
4. Подтверждение выбранного маршрута прохождения трафика;
5. Подтверждение легитимности изменения настроек конфигураций МСЭ;
6. Связывание изменений настроек конфигураций МСЭ с запросом на управление сетевым доступом.

При выполнении указанных операций Аналитик МСЭ руководствуется инструкциями, описанными в следующих разделах настоящего документа.

1.1. Определение необходимости оптимизации правил МСЭ

Данная операция предназначена для выявления необходимости оптимизации правил МСЭ.

Цель – повышение производительности МСЭ за счет оптимизации последовательности правил, а также упрощение эксплуатации комплекса МСЭ за счет удаления неиспользуемых объектов конфигурации.

1.1.1. Условия выполнения операции

Данная операция выполняется если:

- Сформирован отчет о прохождении трафика и конфигурации МСЭ;
- Поступила заявка на выполнение оптимизации либо по расписанию.

1.1.2. Порядок выполнения операции

1.1.2.1. Подготовительные действия

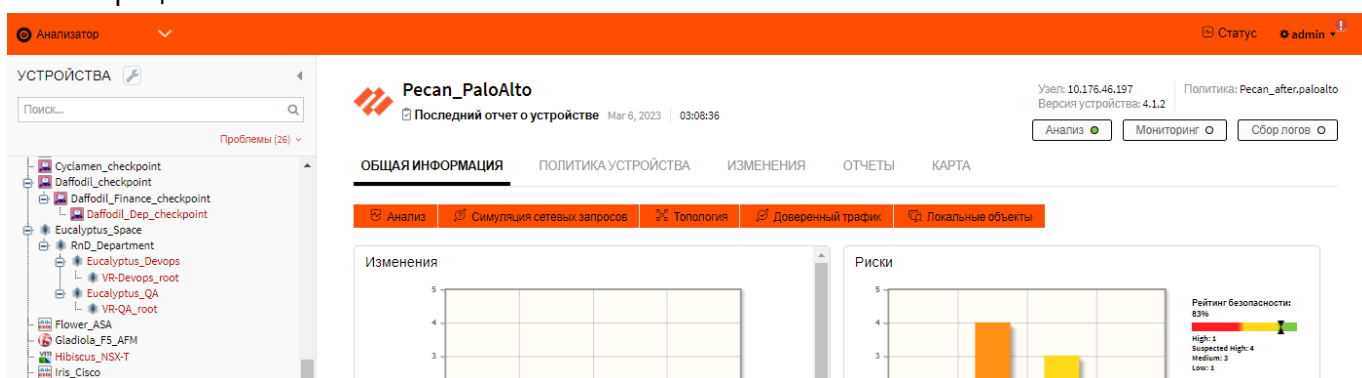
Перед началом данной операции необходимо определить следующие параметры:

- IP Адрес(а) и hostname МСЭ.

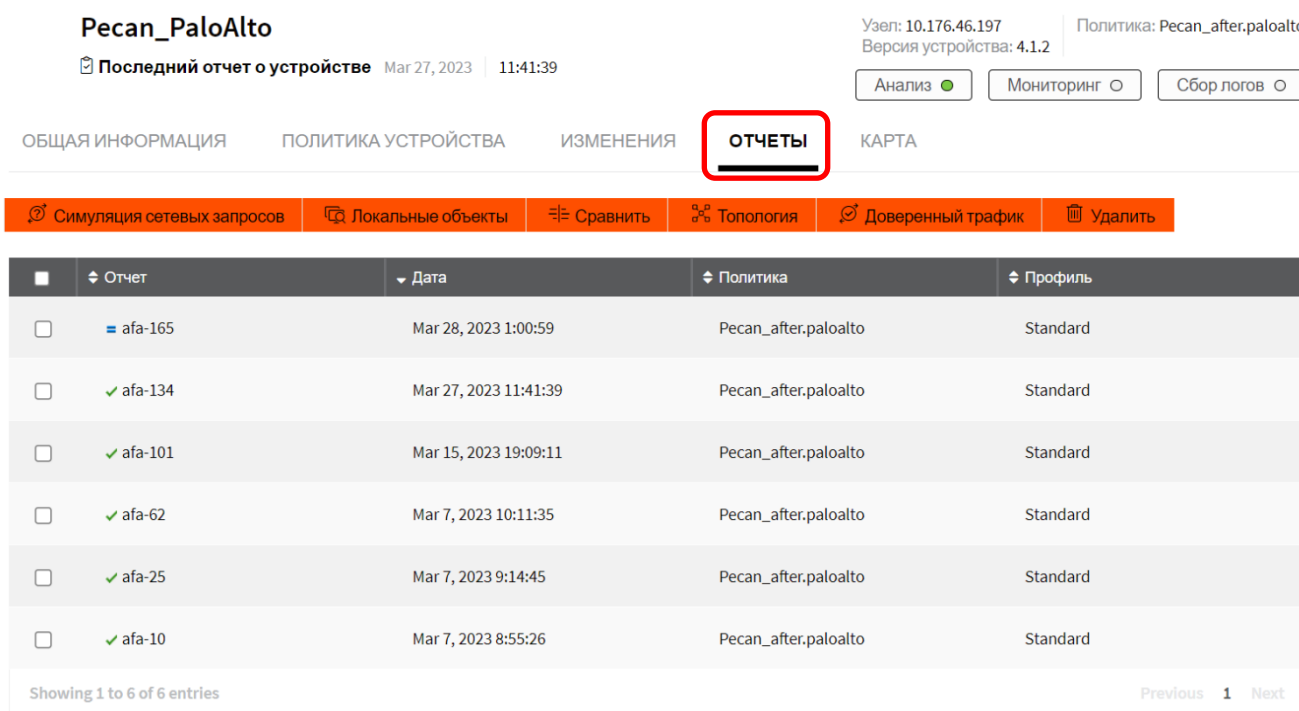
1.1.2.2. Основные действия

С помощью браузера подключиться к Web-интерфейсу системы Нетхаб.

В левом верхнем углу страницы перейти в модуль **Нетхаб Анализатор**, для этого надо нажать символ «V» и в выпадающем списке выбрать **Нетхаб Анализатор**. Перейти в раздел **УСТРОЙСТВА**, выбрать в дереве устройств МСЭ, для которого выполняется операция.

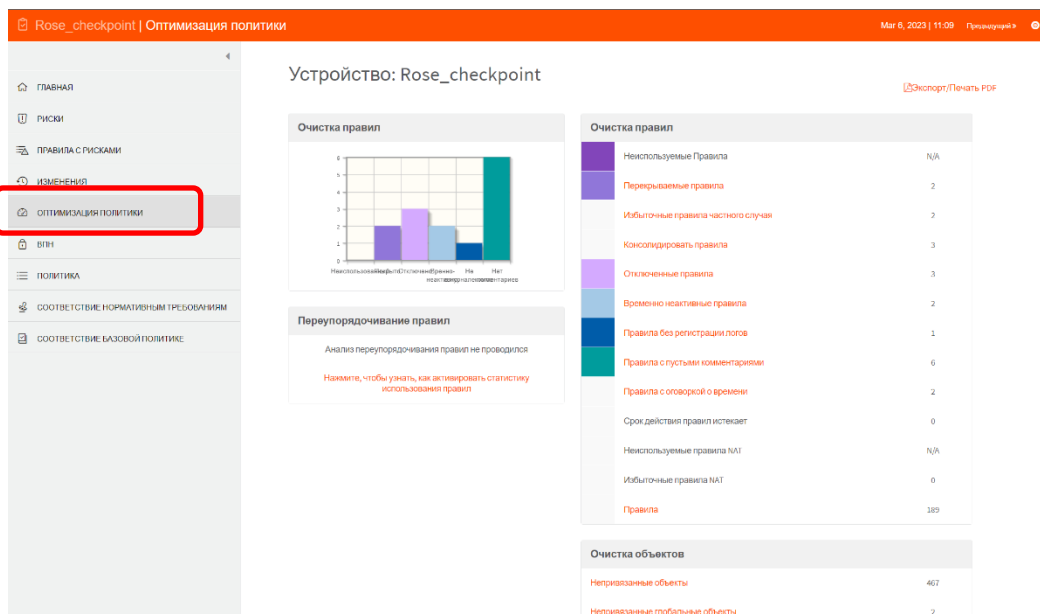


Для просмотра отчета необходимо перейти на вкладку **ОТЧЕТЫ** и выбрать интересующий отчет.



Для анализа отчета по группе МСЭ необходимо выбрать раздел **ГРУППЫ** и выбрать интересующую группу МСЭ. Для просмотра или загрузки отчета необходимо перейти на вкладку **ОТЧЕТЫ** и выбрать интересующий отчет.

Для определения необходимости оптимизации правил требуется проанализировать рекомендации из отчета системы Нетхаб. Для этого необходимо выбрать устройство и открыть отчет, после чего перейти в раздел **ОПТИМИЗАЦИЯ ПОЛИТИКИ**.



Данный раздел отчета содержит следующие блоки рекомендаций:

Очистка правил - рекомендации по оптимизации правил, включая перечень редко или совсем не используемых правил (**Неиспользуемые Правила**), перекрывающихся правил (**Перекрываемые правила**), правил, которые могут быть объединены (**Консолидировать правила** и **Избыточные правила частного случая**), а также правил без журналирования или без комментариев. Переход по соответствующей ссылке отображает более детальную информацию.

Очистка объектов – рекомендации по оптимизации набора объектов на МСЭ, включая неиспользуемые объекты (**Непривязанные объекты** и **Неиспользуемые объекты в рамках правил**), а также объекты-дубликаты. Переход по соответствующей ссылке отображает более детальную информацию.

Интеллектуальный Тюнер Политики – рекомендации на основе детального анализа журналов срабатывания правил (для МСЭ Cisco ASA применяется только если в правиле включено журналирование с помощью ключевого слова **log**). В данном разделе приведены рекомендации по более строгому описанию правил. Переход по соответствующей ссылке отображает более детальную информацию.

Переупорядочивание правил – рекомендации по изменению порядка правил. Данные рекомендации на основе статистики срабатывания правил за период мониторинга. Основная метрика - **RMPP (Rules Matched Per Packet)**, количество правил, проверяемых для каждого пакета. Чем данное значение меньше, тем более оптимальный

порядок правил на МСЭ. Переход по соответствующей ссылке отображает более детальную информацию.

Для выполнения операции необходимо выбрать блок рекомендаций и после проведения детального анализа принять решение о необходимости выполнения оптимизации правил МСЭ.

1.1.2.3. Заключительные действия

В зависимости от принятого решения продолжить обработку заявки либо перейти к выполнению операции Выбор способа оптимизации правил МСЭ и формирование запросов.

1.2. Выбор способа оптимизации правил МСЭ и формирование запросов

Данная операция предназначена для формирования запросов на выполнение работ по оптимизации правил.

Оптимизация осуществляется путем внесения изменений в существующие правила МСЭ, а также удалением объектов.

1.2.1. Условия выполнения операции

Данная операция выполняется если требуется оптимизация правил МСЭ одним из следующих способов:

- модификация существующих правил;
- Модификация объектов правил;
- Дезактивация правил.

1.2.2. Порядок выполнения операции

1.2.2.1. Подготовительные действия

Определить идентификатор МСЭ и правила, требующие модификации.

1.2.2.2. Основные действия

С помощью браузера подключиться к Web-интерфейсу системы Нетхаб. В левом верхнем углу страницы перейти в модуль **Нетхаб Менеджер**, для этого нужно нажать символ «V» и в выпадающем списке выбрать **Нетхаб Менеджер**.

Для создания запроса необходимо выполнить следующие действия.

В левом верхнем углу страницы перейти в модуль **Нетхаб Менеджер**, для этого нужно нажать символ «V» и в выпадающем списке выбрать **Нетхаб Менеджер**. Для перехода в режим создание запроса нужно нажать кнопку **+ Новый запрос**.

Обзор

► 2 Change Requests to Approve

▼ 11 Change Requests to Plan

Идентификатор	Тема	Инициатор	Рабочий процесс	Политика, подлежащая изменению
29	Change Request to Allow Traffic	admin@nethub.localBasic		
17	(Нет заголовка)	admin@nethub.localBasic		
21	Change Request to Allow Traffic	admin@nethub.localBasic		scr-3feb.W garden

Для модификации правил далее необходимо выбрать шаблон запроса **Rule Modification Request** из списка.

Создайте новый запрос на изменение


Загрузить черновик

Выберите шаблон запроса:

Шаблон	Описание
Standard	Создайте запрос на изменение для запроса трафика
110: Запрос на множественное подтверждение	Создайте запрос на изменение трафика, который требует
115: Automatic Traffic Change Request	Create a traffic change request that progresses automatically
120: Generic request	Create a generic change request
130: Object Change Request	Создайте запрос на изменение объекта (добавление/удаление)
140: Rule Removal Request	Create a change request for removing a device rule
145: Rule Modification Request	Create change request for editing a device rule
150: Parallel-Approval Request	Create a traffic change request which requires parallel approvals
160: Web Filter-Change Request (Blue Coat)	Create a web-filter change request
170: Traffic Change Request (IPv6)	Create a request for IPv6 traffic change in Cisco devices
180: Traffic Change Request (Multicast)	Create a request for Multicast traffic change in Cisco devices
190: Verbatim Rule Addition	Create a traffic change request for bulk rules addition exactly as
Basic Change Traffic Request	Create a basic change traffic request

На открывшейся странице карточки запроса необходимо заполнить поля **Тема** и **Владелец**, после чего в поле **Имя устройства** выбрать устройство МСЭ для внесения изменений и в поле **Правило для изменения** нажать кнопку **Выберите правило**.

The screenshot shows the 'Создайте новый запрос на изменение' (Create new request for change) form. The left sidebar contains a 'Менеджер' (Manager) header and a navigation menu with items: '+ Новый запрос' (New request), 'Поиск' (Search), 'Расширенный поиск' (Advanced search), 'ДОМАШНЯЯ СТРАНИЦА' (Home page), 'ИНФОГРАФИКА' (Infographic), 'ПОИСК ПО ПРАВИЛАМ' (Search by rules), 'МЕНЮ: ПОДБОР' (Menu: Selection), 'ШАБЛОНЫ ЗАЯВОК' (Request templates), 'КОНФИГУРАЦИЯ' (Configuration), 'КОНФИГУРАЦИЯ+' (Configuration+), and 'ОПЦИИ' (Options). The main form area has the title 'Создайте новый запрос на изменение' and the subtitle 'Создайте новый запрос на изменение'. The form fields are: 'Владелец:' (Owner) with a dropdown menu showing 'Не Назначенный' (Not assigned); 'Тема:' (Topic) with a text input field; 'Связанный:' (Related) with a text input field and a calendar icon; 'Опишите проблему:' (Describe the problem) with a large text area and a file upload icon; 'Прикрепить файл:' (Attach file) with a 'Choose File' button, 'No file chosen' text, and a 'Добавить Дополнительные Файлы' (Add Additional Files) button; 'Истекает:' (Expires) with a text input field and a calendar icon; 'Инициатор:' (Initiator) with a text input field showing 'admin@nethub.local'; 'Имя устройства:' (Device name) with a text input field and a placeholder 'Нажмите, чтобы выбрать устройства' (Click to select devices); 'Правило для изменения:' (Rule for change) with a 'Выберите правило' (Select rule) button; 'Идентификатор внешнего запроса на изменение:' (External request identifier) with a text input field; 'Рабочий процесс:' (Workflow) with the value 'Rule-Modification'; and 'Из Шаблона:' (From template) with the value '145: Rule Modification Request'. A 'Назад' (Back) button is located at the bottom left of the form area.

В открывшемся представлении правил МСЭ необходимо выбрать правило для внесения изменений, нажав на символ . После чего в поле **Правило для изменения** указать новые значения полей правила, после чего нажать кнопку **Далее**.

Для модификации объектов в конфигурации МСЭ необходимо выбрать шаблон запроса **Object Change Request** из списка.

Далее выбрать устройство для конфигурации в поле **Имя устройства**, после чего выбрать действие с объектами и указать необходимые данные. При необходимости можно добавить дополнительные объекты нажав кнопку **+ Измените Больше Объектов**.

Прикрепить файл: No file chosen

Истекает:

Инициатор:

Имя устройства:

Запрос:

Object Type: NETWORK СЕРВИС

Действие	Имя объекта	New Values	Scope
1. <input checked="" type="radio"/> Add IPs to Network Object	<input type="text" value="Type or doubleclick"/>	<input type="text" value="Type or doubleclick"/>	<input checked="" type="radio"/> Local
<input type="radio"/> Remove IPs from Network Object			<input type="radio"/> Глобальный
<input type="radio"/> New Network Object			
<input type="radio"/> Delete Network Object			

Идентификатор внешнего запроса на изменение:

Рабочий процесс: Change-Object

Из Шаблона: 130: Object Change Request

После внесения всех данных в карточку запроса нажать кнопку **Далее**.

Для дезактивации правил необходимо выполнить следующие действия.

В левом верхнем углу страницы перейти в модуль **Нетхаб Аналитатор**, для этого надо нажать символ «V» и в выпадающем списке выбрать **Нетхаб Аналитатор**. Перейти в раздел **УСТРОЙСТВА**, выбрать в дереве устройств МСЭ, для которого выполняется операция. Для определения правил, для которых требуется дезактивация необходимо выбрать устройство и открыть отчет, после чего перейти в раздел **ОПТИМИЗАЦИЯ ПОЛИТИКИ**. На открывшейся странице необходимо перейти по ссылке **Неиспользуемые Правила** либо **Избыточные правила частного случая**. После внесения всех данных в карточку запроса нажать кнопку Next.

Rose_checkpoint | Оптимизация политики Mar 6, 2023 | 11:09

Устройство: Rose_checkpoint

Очистка правил

Переупорядочивание правил

Анализ переупорядочивания правил не проводился

Нажмите, чтобы узнать, как активировать статистику использования правил

Очистка правил	Количество
Неиспользуемые Правила	N/A
Перекрытые правила	2
Избыточные правила частного случая	2
Консолидировать правила	3
Отключенные правила	3
Временно неактивные правила	2
Правила без регистрации логов	1
Правила с пустыми комментариями	6
Правила с отсрочкой о времени	2
Срок действия правил истекает	0
Неиспользуемые правила NAT	N/A
Избыточные правила NAT	0
Правила	189

Очистка объектов

Непривязанные объекты	467
Непривязанные глобальные объекты	2

Rules Cleanup: Rose_checkpoint

Экспорт/Печать PDF
Скачать CSV

Перекрываемые правила

На этой странице показаны правила, которые покрываются (скрываются) другими правилами. Такие правила фактически отключены и, вероятно, могут быть удалены.



☐ Выбрать все Перекрываемые правила

Отключить выбранные

Правило 36 перекрывается правилами 15, 34.

RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	DOCUMENTATION
15	GP_NW_SU_LAN	GP_NW_Garden_ICN	GP_NW_Garden_ICN	TCP http TCP https TCP ldap	accept	-	
34	GP_NW_BAI_LAN	GP_NW_Garden_ICN	GP_NW_Garden_ICN	Any	accept	-	
<input checked="" type="checkbox"/> 36	GP_NW_BAI_LAN GP_NW_SU_LAN	NW_Garden_ICN_003	NW_Garden_ICN_003	TCP https	accept	FireFlow #322: Added by Sally	

Правило 42 перекрывается правилом 37.

RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	DOCUMENTATION
37	GP_NW_Garden_ICN	Any	Any	Any	accept	-	
<input type="checkbox"/> 42	GP_PC_Garden_Time-ICR	PC_Time-ICR_01_EXT PC_Time-ICR_02_EXT	PC_Time-ICR_01_EXT PC_Time-ICR_02_EXT	TCP telnet TCP tcp-12100-IBM-MQ-Series	accept	FireFlow #338: PSQT Servers at Garden to Time	

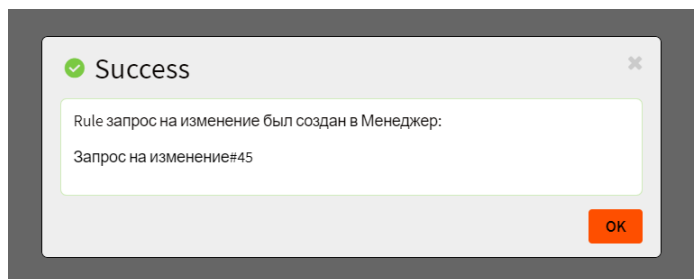
☐ Выберите все Перекрываемые правила

[Назад к списку](#)

Отключить выбранные

На открывшейся странице выбрать правила, которые нужно деактивировать и нажать кнопку **Отключить выбранные**, после чего в **Нетхаб Менеджер** будет создан запрос на отключение / удаление правил(а).

После отображения сообщения об успешном создании запроса перейти в карточку запроса путем перехода по ссылке в сообщении **Запрос на изменение#45**.



1.2.2.3. Заключительные действия

Проинформировать Администратора ГУСД о созданном запросе по электронной почте.

1.3. Подтверждение выбранного маршрута прохождения трафика

Данная операция предназначена для подтверждения маршрута прохождения трафика, выбранного системой Нетхаб.

1.3.1. Условия выполнения операции

Данная операция выполняется если:

- В системе НЕТХАБ создан запрос на управление сетевым доступом и назначен ответственный Аналитик МСЭ для выполнения операции.

1.3.2. Порядок выполнения операции

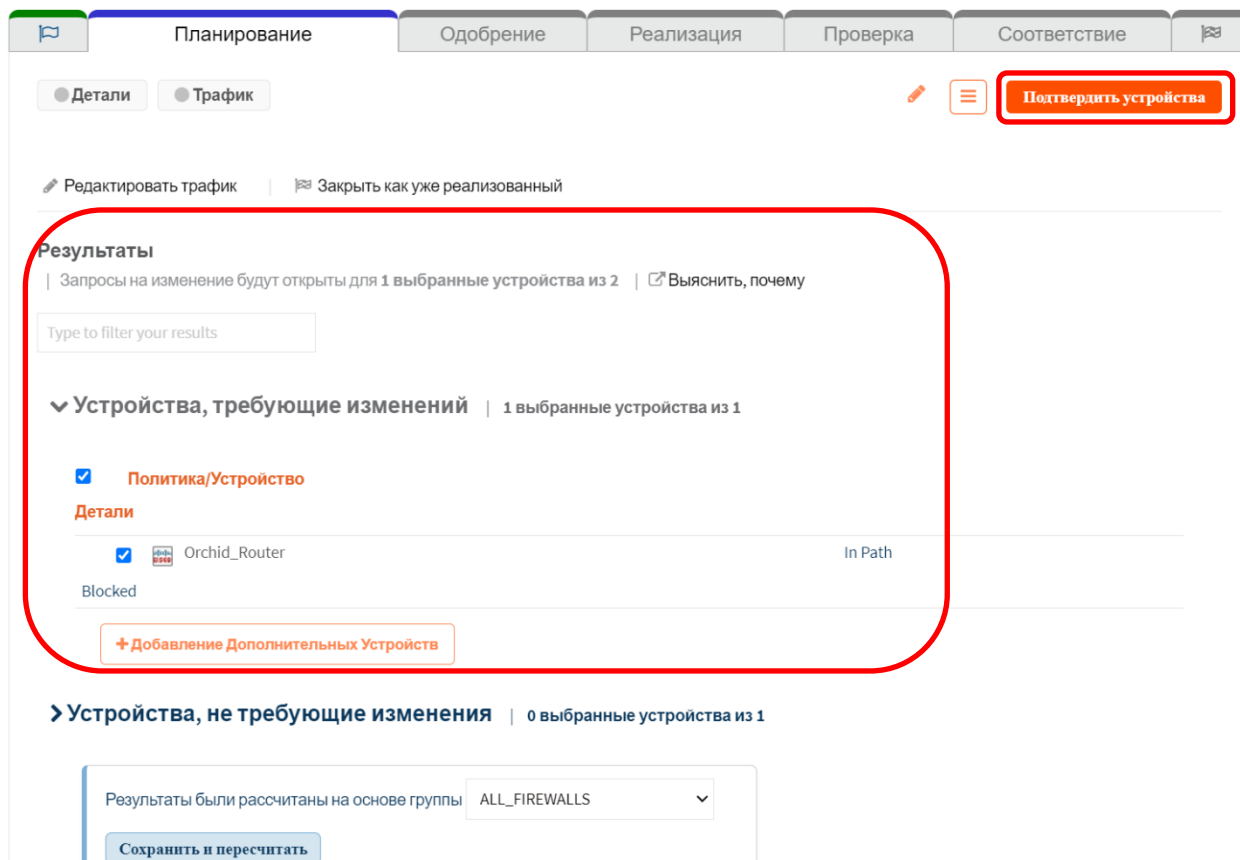
1.3.2.1. Подготовительные действия

Определить идентификатор запроса в НЕТХАБ на основе ранее сохраненных данных или данных из заявки. Определить идентификаторы нарядов(подзапросов) на внесение изменений.

1.3.2.2. Основные действия

С помощью браузера подключиться к Web-интерфейсу системы Нетхаб. В левом верхнем углу страницы перейти в модуль **Нетхаб Менеджер**, для этого нужно нажать символ «V» и в выпадающем списке выбрать **Нетхаб Менеджер**.

Для выполнения операции необходимо перейти по ссылке в карточку запроса или ввести его номер в поле **Поиск**, на открывшейся странице проанализировать перечень устройств, предлагаемых системой Нетхаб для внесения изменений в конфигурацию правил фильтрации. Если набор устройств соответствует ожидаемому, то нажать кнопку **Подтвердить устройства**.



В случае если в списке устройств отсутствует необходимое, то нужно нажать кнопку **+ Добавление Дополнительных Устройств** выбрать его из списка, после чего нажать кнопку **Подтвердить устройства**.

В случае если в списке устройств присутствуют лишние устройства, то нужно удалить их из списка сняв отметку напротив имени таких устройств, после чего нажать кнопку **Подтвердить устройства**.

В случае, если необходимых устройств нет в списке возможных, то необходимо указать это в карточке заявки и оповестить Администратора ГУСД.

1.3.2.3. Заключительные действия

Оповестить Администратора ГУСД о выполнении операции.

1.4. Подтверждение легитимности изменения настроек конфигураций МСЭ

Данная операция предназначена для подтверждения легитимности изменения настроек конфигурации МСЭ.

1.4.1. Условия выполнения операции

Данная операция выполняется если:

- Аудитор ИБ выявил изменения в конфигурации МСЭ, выполненные без создания запроса, и направил оповещение Аналитика МСЭ о необходимости подтверждения их легитимности.

1.4.2. Порядок выполнения операции

1.4.2.1. Подготовительные действия

Проанализировать данные из оповещения от Аудитора ИБ.

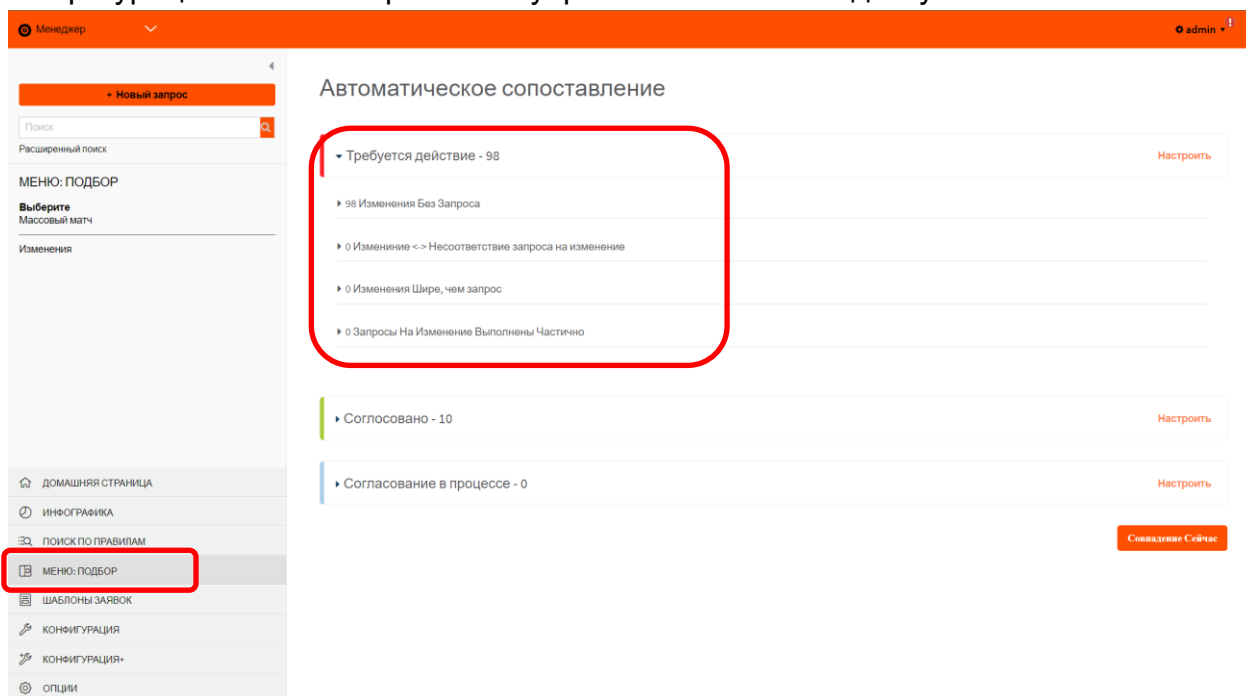
1.4.2.2. Основные действия

С помощью браузера подключиться к Web-интерфейсу системы. В левом верхнем углу страницы перейти в модуль **Нетхаб Менеджер**, для этого нужно нажать символ «V» и в выпадающем списке выбрать **Нетхаб Менеджер**.

Перейти в раздел меню **МЕНЮ: ПОДБОР** и проанализировать список выявленных изменений, которые не удалось сопоставить с запросом в системе Нетхаб. Для этого необходимо развернуть список **Требуется действие**.

Для легитимных изменений необходимо инициировать создание соответствующего им запроса, после чего выполнить операцию «Связывание изменений настроек

конфигураций МСЭ с запросом на управление сетевым доступом».



1.4.2.3. Заключительные действия

Оповестить Аудитора ИБ и Администратора ГУСД о выполнении операции.

1.5. Связывание изменений настроек конфигураций МСЭ с запросом на управление сетевым доступом

Данная операция предназначена для создания связи между легитимными изменениями настроек конфигурации МСЭ и запросами на изменение сетевого доступа в случае, если изменения были выполнены до создания соответствующих запросов. Возможны ситуации оперативного внесения изменений в конфигурацию МСЭ, например, для отражения атаки или в процессе других работ без создания соответствующего запроса на изменение сетевого доступа.

1.5.1. Условия выполнения операции

Данная операция выполняется если:

- Аудитор ИБ выявил изменения в конфигурации МСЭ выполненные без создания запроса и направил оповещение Аналитика МСЭ о необходимости подтверждения их легитимности;
- Для легитимных изменений созданы соответствующие запросы на изменение сетевого доступа.

1.5.2. Порядок выполнения операции

1.5.2.1. Подготовительные действия

Получить идентификаторы запросов, созданных для сопоставления с легитимными изменениями.

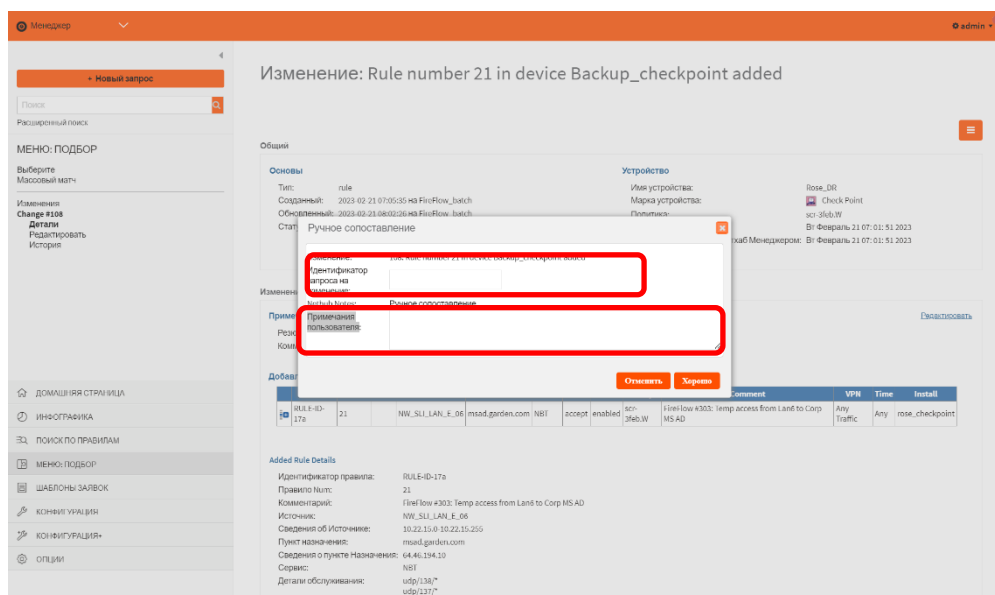
1.5.2.2. Основные действия

С помощью браузера подключиться к Web-интерфейсу системы Нетхаб. В левом верхнем углу страницы перейти в модуль **Нетхаб Менеджер**, для этого нужно нажать символ «V» и в выпадающем списке выбрать **Нетхаб Менеджер**.

Операционная инструкция Аналитика МСЭ

Перейти в раздел меню **МЕНЮ: ПОДБОР** и проанализировать список выявленных изменений, которые не удалось сопоставить с запросом в системе Нетхаб. Для этого необходимо развернуть список **Требуется действие**.

Для легитимных изменений необходимо перейти по ссылке **Соответствие** и на открывшейся странице внести идентификатор соответствующего им запроса в поле **Идентификатор запроса на изменение** и указать необходимые комментарии в поле **Примечания пользователя**, после чего нажать **ОК**.



1.5.2.3. Заключительные действия

Заключительных действий не требуется.

1.6. Удаление связи изменений настроек конфигураций МСЭ с запросом на управление сетевым доступом

Данная операция предназначена для удаления ошибочной связи между изменениями настроек конфигурации МСЭ и запросами на изменение сетевого доступа в случае.

1.6.1. Условия выполнения операции

Данная операция выполняется если:

- Аудитор ИБ выявил изменения в конфигурации МСЭ, выполненные без создания запроса, и направил оповещение Аналитика МСЭ о необходимости подтверждения их легитимности.

1.6.2. Порядок выполнения операции

1.6.2.1. Подготовительные действия

Проанализировать данные из оповещения от Аудитора ИБ.

1.6.2.2. Основные действия

С помощью браузера подключиться к Web-интерфейсу системы Нетхаб. В левом верхнем углу страницы перейти в модуль **Нетхаб Менеджер**, для этого нужно нажать символ «V» и в выпадающем списке выбрать **Нетхаб Менеджер**.

Перейти в раздел меню **МЕНЮ: ПОДБОР** и проанализировать список выявленных изменений, которые не корректно сопоставлены с запросом в системе Нетхаб. Для этого необходимо развернуть список **Требуется действие** и в подсписке **Изменение <-> Несоответствие запроса на изменение** проанализировать записи об изменениях.

Для просмотра детальной информации необходимо перейти на станицу детальной информации с помощью ссылки **Details**. Далее из выпадающего списка выбрать необходимое действие:

- **Совпадение В порядке** – для подтверждения корректной связи между изменениями и запросом;
- **Неправильный запрос на Изменение** – для указания идентификатора корректного соответствующего запроса;
- **Удалить совпадение** – для удаления связи между изменениями и запросом.

1.6.2.3. Заключительные действия

Оповестить Аудитора ИБ и Администратора УСД о выполнении операции.