

Программный комплекс по защите
системно-технической инфраструктуры
«Efros Defence Operations»

Руководство пользователя
Часть 5

Агент «Efros Defence Operations»

Аннотация

Данный документ входит в комплект пользовательской документации для работы с программным комплексом по защите системно-технической инфраструктуры «Efros Defence Operations» (ПК «Efros DO» или комплекс).

Руководство содержит назначение и описание функциональных возможностей агента «Efros Defence Operations» (агент ПК «Efros DO» или агент). Также приведено описание рекомендуемой последовательности работы для настройки возможностей агента ПК «Efros DO» отдельно и совместно с суппликантом ПК «Efros DO» и VPN-решением.

Для работы с возможностями агента ПК «Efros DO» необходимо убедиться в установке лицензии модуля «Efros Network Access Control» (модуль «Efros NAC»).

Руководство состоит из следующих частей:

- часть 1 – содержит сведения, необходимые для настройки доступа пользователей ПК «Efros DO» к сетевым ресурсам и функциям, а также описание выполнения функций контроля работы объектов сети с использованием веб-интерфейса;
- часть 2 – содержит сведения, необходимые для настройки и конфигурирования функций контроля устройств;
- часть 3 – содержит сведения, необходимые для настройки и конфигурирования функций контроля доступа;
- часть 4 – содержит сведения, необходимые для настройки возможностей контроля целостности функционального модуля «Efros Integrity Check Compliance» («Efros ICC»);
- часть 5 (данный документ) – содержит сведения, необходимые для настройки агента «Efros Defence Operations».

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:



Важная информация
Указания, требующие особого внимания.



Дополнительная информация
Информация, позволяющая упростить работу с комплексом.

Представленные в документе снимки экрана могут отличаться для различных версий поставляемого комплекса и предназначены для демонстрации работы комплекса.

Содержание

1	Назначение.....	5
1.1	Назначение агента	5
1.2	Назначение дополнительных компонентов	5
2	Варианты подключения устройств и устанавливаемые компоненты	7
3	Алгоритмы настройки разграничения доступа.....	8
3.1	Разграничение доступа к сети с использованием агента и суппликанта ПК «Efros DO»	8
3.2	Настройка запроса по протоколу TEAP с использованием агента и встроенного суппликанта	10
3.3	Разграничение доступа к сети с использованием агента и VPN-клиента	11
3.4	Разграничение доступа к сети с использованием политики профилирования..	12
4	Функциональные возможности	13
4.1	Функциональные возможности агента	13
4.1.1	Инвентаризация данных конечных точек.....	13
4.1.2	Запрос данных для проверки конечной точки	14
4.2	Работа с агентами и политиками в ПК «Efros DO»	16
4.2.1	Список подключенных агентов	16
4.2.2	Политика безопасности	17
4.2.3	Политика контроля целостности до загрузки ОС	19
4.2.4	Политика доступа в сеть	19
4.2.5	Политика профилирования.....	20
4.2.6	Изменение авторизации.....	21
4.3	Схемы разграничения доступа к корпоративным ресурсам.....	21
4.3.1	Решение с суппликантом	21
4.3.2	Решение с VPN	22
	Приложение А Рекомендуемая последовательность действий для настройки подключения к сети с помощью агента и суппликанта	27
	Приложение Б Рекомендуемая последовательность действий для настройки разграничения доступа к сети с использованием агента и встроенного суппликанта....	61
	Приложение В Рекомендуемая последовательность действий для настройки разграничения доступа к сети с использованием агента через VPN	74

Приложение Г Рекомендуемая последовательность действий для настройки разграничения доступа к сети с использованием политики профилирования.....	83
Перечень сокращений	91

1 Назначение

1.1 Назначение агента

Агент ПК «Efros DO» совместно с ПК «Efros DO» позволяет управлять доступом пользователей к корпоративным ресурсам при проводном и беспроводном подключении с учетом состояния защищенности рабочих мест и соответствия принятым в организации требованиям по информационной безопасности.

Агент ПК «Efros DO», установленный устройстве (конечной точке), выполняет сбор сведений об устройстве. На основе полученных данных определяется статус соответствия требованиям политики безопасности:

- «Соответствует»;
- «Не соответствует»;
- «Не определено».

Статус соответствия требованиям безопасности может быть использован в политиках доступа в сеть в правилах авторизации, чтобы предоставлять различный уровень доступа, в зависимости от состояния устройства, с которого подключается пользователь. Например, полный доступ, если устройство полностью соответствует всем требованиям, или ограниченный доступ, если состояние устройства не определено или не соответствует требованиям политики безопасности.

При работе агент ПК «Efros DO» взаимодействует с суппликантом 802.1X, встроенным в операционную систему (встроенный суппликант). Для изменения методов подключения устройства можно изменить параметры встроенного суппликанта.

1.2 Назначение дополнительных компонентов

Для реализации дополнительных возможностей использования агента ПК «Efros DO» на устройство могут быть установлены следующие компоненты:

- суппликант ПК «Efros DO» (суппликант) – предназначен для выполнения проверки устройства на соответствие требованиям политики безопасности на этапе подключения к корпоративной сети;



При установке суппликанта ПК «Efros DO» агент перестает взаимодействовать с встроенным суппликантом.

- модуль «Контроль целостности до загрузки ОС» – предназначен для проверки политики контроля целостности объектов до загрузки операционной системы (ОС);
- VPN-клиент – предназначен для удаленного подключения к корпоративной сети через VPN (VPN-решение).



В данной версии агент ПК «Efros DO» поддерживает интеграцию с VPN-решением КриптоПро NGate.

2 Варианты подключения устройств и устанавливаемые компоненты

Основные варианты подключения устройства к корпоративной сети и соответствующий перечень устанавливаемых компонентов приведены в таблице 1.

Таблица 1 – Устанавливаемые компоненты в зависимости от варианта подключения



Вариант подключения	Устанавливаемые компоненты
Прямое подключение к корпоративной сети	Агент ПК «Efros DO»
Проверка требований безопасности на этапе подключения к корпоративной сети	<ul style="list-style-type: none">• Агент ПК «Efros DO»;• Суппликант ПК «Efros DO»
Удаленное подключение к корпоративной сети	<ul style="list-style-type: none">• Агент ПК «Efros DO»;• VPN-клиент
Профилирование конечной точки на основе данных источника «Edo-Agent»	–

Допустимо одновременно устанавливать агент, суппликант и VPN-клиент на контролируемом устройстве.

В этом случае при подключении к сети через суппликант проверка требований безопасности будет производиться на этапе подключения к корпоративной сети.

При удаленном подключении к сети через VPN-клиент проверка требований безопасности будет производиться после подключения к корпоративной сети.

Модуль «Контроль целостности до загрузки ОС» не влияет на вариант подключения.

-  Настроить расписание для автоматического обновления агента можно в подразделе «Установка и обновление». Также можно настроить установку или обновление модуля «Контроль целостности до загрузки ОС».
-  Описание установки агента и суппликанта на устройство приведены в документе «Руководство администратора».

3 Алгоритмы настройки разграничения доступа


3.1 Разграничение доступа к сети с использованием агента и суппликанта ПК «Efros DO»

Краткая последовательность действий для настройки разграничения доступа к сети с использованием агента и суппликанта ПК «Efros DO» представлена в таблице 2.

При использовании только агента (без суппликанта) последовательность действий будет такой же.

Пример настройки разграничения доступа к сети в веб-интерфейсе ПК «Efros DO» приведен в Приложении А.

Таблица 2 – Краткая последовательность действий для настройки подключения к сети с помощью агента и суппликанта ПК «Efros DO»

№ п/п	Действие	Описано в разделе документа	Пример настройки
На устройстве			
1	Установить агент	–	–
2	*Установить суппликант ПК «Efros DO»	–	–
3	*Настроить суппликант ПК «Efros DO»	–	–
На аутентификаторе			
4	Произвести необходимые настройки аутентификатора. Для работы в комплексе потребуются следующие данные: <ul style="list-style-type: none"> • IP-адрес подключения к аутентификатору; • секретный ключ подключения аутентификатора к серверу RADIUS; • VLAN или ACL для требуемых уровней доступа в сеть 	–	–
В веб-интерфейсе ПК «Efros DO»			
5	Настроить подключенный агент	4.2.1	Приложение А.1
6	Настроить расписание обновления компонентов инсталляционного пакета	–	Приложение А.2
7	Создать политику безопасности	4.2.2	Приложение А.3
8	Создать политику контроля целостности до загрузки ОС	4.2.3	Приложение А.4
9	*Настроить разрешенные протоколы <div style="margin-top: 10px;">  При использовании суппликанта ПК «Efros DO» необходимо включить метод проверки подлинности EAP-TNC для выполнения проверки устройства на соответствие требованиям политики безопасности на этапе подключения к корпоративной сети </div>	–	Приложение А.5

№ п/п	Действие	Описано в разделе документа	Пример настройки
10	Создать профиль сетевого оборудования для аутентификатора	–	Приложение А.6, п. 1
11	Создать сетевое оборудование – аутентификатор	–	Приложение А.6, п. 2
12	Создать профиль авторизации доступа в сеть для устройства со статусом несоответствия требованиям политики безопасности «Не соответствует» (Non-Compliant) и «Не определено» (Indeterminate)	–	Приложение А.7, п. 1
13	Создать профиль авторизации доступа в сеть, назначаемый после успешной авторизации устройства со статусом соответствия требованиям политики безопасности «Соответствует» (Compliant)	–	Приложение А.7, п. 2
14	**Создать шаблоны условий	–	Приложение А.7, п. 3
15	**Настроить источник данных Active Directory	–	Приложение А.7, п. 4
16	Создать политику доступа в сеть. Настроить правила аутентификации и авторизации	4.2.4	Приложение А.7, п.п. 5 - 7
<p>Примечания:</p> <p>* При работе только с агентом (без суппликанта ПК «Efros DO») шаги можно пропустить.</p> <p>** Дополнительные настройки, шаги можно пропустить.</p>			

3.2 Настройка запроса по протоколу TEAP с использованием агента и встроенного суппликанта

Краткая последовательность действий для настройки запроса на одновременную аутентификацию устройства и пользователя по протоколу TEAP с использованием агента и суппликанта, встроенного в ОС, представлена в таблице 3.

Пример настройки встроенного суппликанта и пример настройки разграничения доступа к сети в веб-интерфейсе ПК «Efros DO» приведены в Приложениях А и Б.

Таблица 3 – Краткая последовательность действий для настройки запроса по протоколу TEAP с помощью агента и встроенного суппликанта

№ п/п	Действие	Описано в разделе документа	Пример настройки
На устройстве			
1	Установить агент ПК «Efros DO»	–	–
2	Настроить суппликант, встроенный в ОС	–	Приложение Б.1
На аутентификаторе			
3	Произвести необходимые настройки аутентификатора. Для работы в комплексе потребуются следующие данные: <ul style="list-style-type: none"> • IP-адрес подключения к аутентификатору; • секретный ключ подключения аутентификатора к серверу RADIUS 	–	–
В веб-интерфейсе ПК «Efros DO»			
4	Настроить разрешенные протоколы (TEAP)	–	Приложение Б.2
5	Создать профиль сетевого оборудования для аутентификатора	–	Приложение А.6, п. 1
6	Создать сетевое оборудование – аутентификатор	–	Приложение А.6, п. 2
7	Создать профиль авторизации доступа в сеть для пользователя	–	Приложение Б.3, п. 1
8	Создать профиль авторизации доступа в сеть для устройства	–	Приложение Б.3, п. 2
9	Настроить источник данных Active Directory	–	Приложение Б.3, п. 3
10	Настроить источник данных профилей сертификатов	–	Приложение Б.3, п. 4
11	Создать политику доступа в сеть. Настроить правила аутентификации и авторизации	–	Приложение Б.3, п.п. 5 - 7

3.3 Разграничение доступа к сети с использованием агента и VPN-клиента

Краткая последовательность действий для настройки разграничения доступа к сети с использованием агента и VPN-клиента представлена в таблице 4.

Пример настройки разграничения доступа к сети в веб-интерфейсе ПК «Efros DO» приведен в приложениях А и В.

Таблица 4 – Краткая последовательность действий для настройки разграничения доступа к сети с использованием агента и VPN-клиента

№ п/п	Действие	Описано в разделе документа	Пример настройки
На устройстве			
1	Установить агент ПК «Efros DO»	–	–
2	Установить VPN-клиент	–	–
На VPN-шлюзе			
3	Произвести необходимые настройки VPN-шлюза. Для работы в комплексе потребуются следующие данные: <ul style="list-style-type: none"> • IP-адрес подключения к VPN-шлюзу; • секретный ключ подключения VPN-шлюза к серверу RADIUS; • ACL или VLAN для требуемых уровней доступа в сеть 	–	–
В веб-интерфейсе ПК «Efros DO»			
4	Настроить подключенный агент	4.2.1	Приложение А.1
5	Создать политику безопасности	4.2.2	Приложение А.3
6	Создать профиль сетевого оборудования для VPN-шлюза	–	Приложение В, п. 2
7	Создать сетевое оборудование – VPN-шлюз	–	Приложение В, п. 3
8	Создать профиль авторизации доступа в сеть для устройства со статусом несоответствия требованиям политики безопасности «Не соответствует» (Non-Compliant) и «Не определено» (Indeterminate)	–	Приложение В, п. 4
9	Создать профиль авторизации доступа в сеть, назначаемый после успешной авторизации устройства со статусом соответствия требованиям политики безопасности «Соответствует» (Compliant)	–	Приложение В, п. 5
10	Создать политику доступа в сеть. Настроить правила аутентификации и авторизации	4.2.4	Приложение В, п.п. 6 - 8

3.4 Разграничение доступа к сети с использованием политики профилирования

Краткая последовательность действий для настройки разграничения доступа к сети с использованием политики профилирования представлена в таблице 5.

Пример настройки разграничения доступа к сети в веб-интерфейсе ПК «Efros DO» приведен в приложениях А и Г.

Таблица 5 – Краткая последовательность действий для настройки разграничения доступа к сети с использованием политики профилирования

№ п/п	Действие	Описано в разделе документа	Пример настройки
На аутентификаторе			
1	Произвести необходимые настройки аутентификатора. Для работы в комплексе потребуются следующие данные: <ul style="list-style-type: none"> • IP-адрес подключения к аутентификатору; • секретный ключ подключения аутентификатора к серверу RADIUS; • VLAN или ACL для требуемых уровней доступа в сеть 	–	–
В веб-интерфейсе ПК «Efros DO»			
2	Создать политику безопасности	4.2.1	Приложение А.3
3	Создать профиль сетевого оборудования для аутентификатора	4.2.2	Приложение А.6, п. 1
4	Создать сетевое оборудование – аутентификатор	–	Приложение А.6, п. 2
5	Создать профиль авторизации доступа в сеть для устройства со статусом несоответствия требованиям политики безопасности «Не соответствует» (Non-Compliant) и «Не определено» (Indeterminate)	–	Приложение А.7, п. 1
6	Создать профиль авторизации доступа в сеть, назначаемый после успешной авторизации устройства со статусом соответствия требованиям политики безопасности «Соответствует» (Compliant)	–	Приложение А.7, п. 2
7	Создать политику профилирования	4.2.5	Приложение Г.1
8	Создать политику доступа в сеть. Настроить правила аутентификации и авторизации	4.2.4	Приложение Г.2

4 Функциональные возможности

Агент ПК «Efros DO» совместно с ПК «Efros DO» реализует следующие функциональные возможности:

- получение сведений об ОС и составе программного обеспечения (ПО);
- проверка устройств на соответствие требованиям политик безопасности, сконфигурированных в ПК «Efros DO»;
- реагирование на нарушения.

4.1 Функциональные возможности агента

4.1.1 Инвентаризация данных конечных точек

Данные, запрашиваемые агентом ПК «Efros DO» у конечных точек:

- Имя устройства (конечной точки).
- ОС:
 - название;
 - версия;
 - сборка;
 - платформа;
 - архитектура;
 - дата установки;
 - статус службы обновлений.
- Антивирусное ПО:
 - название;
 - версия;
 - статус защиты;
 - дата обновления антивирусных баз;
 - статус обновления антивирусных баз.



В данной версии агент ПК «Efros DO» поддерживает опрос антивирусного ПО компаний «Лаборатория Касперского» и «Доктор Веб».

- Сетевые интерфейсы:
 - имя;
 - служебное имя;
 - производитель;
 - тип;
 - состояние;
 - MAC-адрес.

4.1.2 Запрос данных для проверки конечной точки

Перечень запрашиваемых данных агентом у конечной точки настраивается в политике безопасности.

Перечень данных конечных точек, доступных для запроса агентом, приведен в таблице 6.

Таблица 6 – Перечень данных конечных точек, доступных для запроса

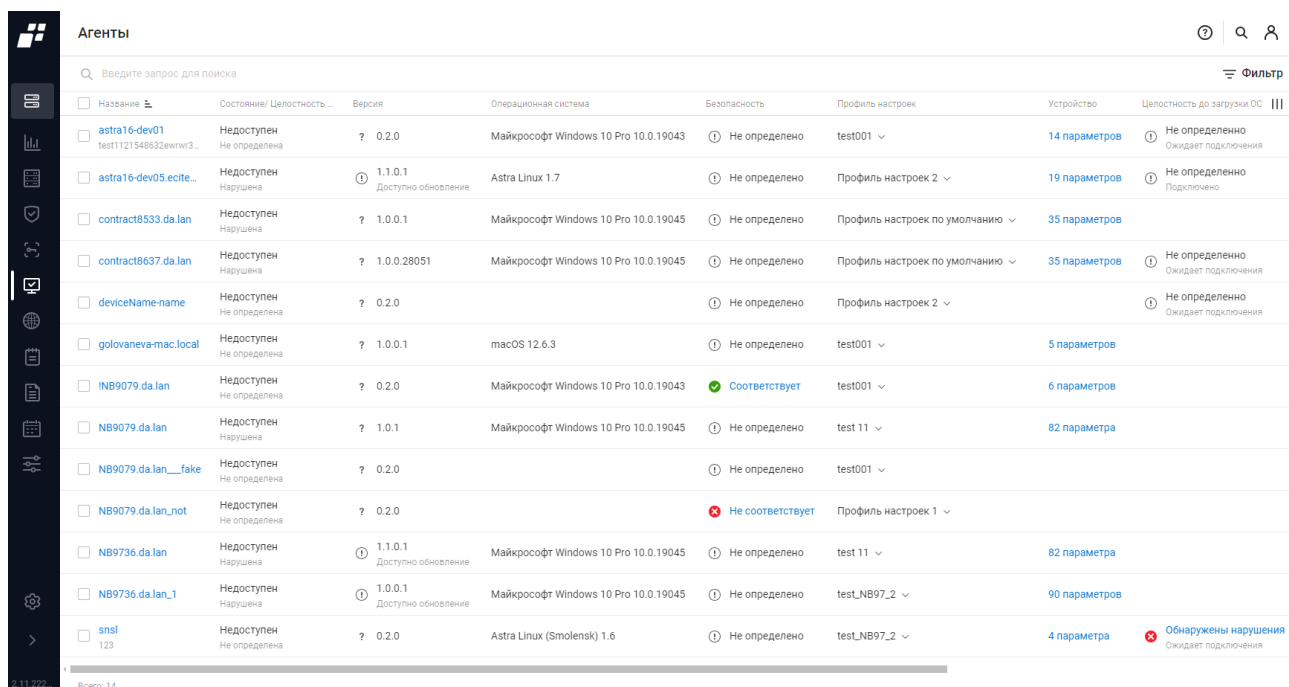
Объект	Название	ОС
Программы	Название	Windows
	Состояние	
	Версия	
	Дата установки	
	Источник установки	
	Расположение	
	Издатель	
Антивирусные приложения	Название	Windows, Linux, macOS
	Состояние	Windows, Linux, macOS
	Версия	Linux, macOS
	Состояние защиты	Windows, Linux, macOS
	Дата обновления антивирусных баз	Windows, Linux, macOS
	Статус обновления антивирусных баз	Windows
Пакеты	Название	Linux, macOS
	Состояние	
	Версия	
	Издатель	
	Архитектура	
Процессы	Название процесса	Windows, Linux, macOS
	Команда	
	Состояние	
	Имя пользователя	
	Путь	
Файлы	Абсолютный путь	Windows, Linux, macOS
	Существование	Windows, Linux, macOS
	Дата создания	Windows, Linux, macOS
	Дата изменения	Windows, Linux, macOS
	Версия	Windows, Linux, macOS
	Права	Linux, macOS
	Размер (в байтах)	Windows, Linux, macOS
Операционная система	Семейство	Windows, Linux, macOS
	Название	Windows, Linux, macOS
	Версия	Windows, Linux, macOS
	Платформа	Windows, Linux, macOS
	Сборка	Windows, Linux, macOS
	Архитектура	Windows, Linux, macOS
	Дата установки	Windows, Linux, macOS

Объект	Название	ОС
	Сервис обновлений	Windows
Обновления системы	Идентификатор	Windows
	Код обновления	
	Описание	
	Дата установки	
	Статус	
USB устройства	Серийный номер	Windows, Linux, macOS
	Состояние	
	Производитель	
	Модель	
Разделы реестра	Раздел	Windows
	Существование	
	Содержимое	
Параметры реестра	Раздел	Windows
	Параметр	
	Существование	
	Значение (строка)	
	Значение (числовое)	
Сетевые интерфейсы	Имя	Windows, Linux, macOS
	Служебное имя	Windows
	Тип	Windows, Linux, macOS
	Производитель	Windows, Linux, macOS
	Состояние	Windows, Linux, macOS
	Общее количество	Windows, Linux, macOS
Службы	Имя службы	Windows
	Отображаемое имя	
	Описание	
	Состояние	
	Тип запуска	
	Исполняемый файл	
Доверенная загрузка	Статус проверки	Windows, Linux
	Контроль целостности	
	Дата проверки	

4.2 Работа с агентами и политиками в ПК «Efros DO»

4.2.1 Список подключенных агентов

Управление списком агентов, установленных на устройствах и подключенных к комплексу, осуществляется в веб-интерфейсе ПК «Efros DO» в разделе «Агенты». Формирование списка производится автоматически при подключении агента к комплексу (рис. 1).




Название	Состояние/ Целостность ...	Версия	Операционная система	Безопасность	Профиль настроек	Устройство	Целостность до загрузки ОС
astra16-dev01 test1121548632ewrwr3...	Недоступен Не определена	? 0.2.0	Майкрософт Windows 10 Pro 10.0.19043	ⓘ Не определено	test001	14 параметров	ⓘ Не определено Ожидает подключения
astra16-dev05.ecite...	Недоступен Нарушена	ⓘ 1.1.0.1 Доступно обновление	Astra Linux 1.7	ⓘ Не определено	Профиль настроек 2	19 параметров	ⓘ Не определено Подключено
contract8533.da.lan	Недоступен Нарушена	? 1.0.0.1	Майкрософт Windows 10 Pro 10.0.19045	ⓘ Не определено	Профиль настроек по умолчанию	35 параметров	
contract8637.da.lan	Недоступен Нарушена	? 1.0.0.28051	Майкрософт Windows 10 Pro 10.0.19045	ⓘ Не определено	Профиль настроек по умолчанию	35 параметров	ⓘ Не определено Ожидает подключения
deviceName-name	Недоступен Не определена	? 0.2.0		ⓘ Не определено	Профиль настроек 2		ⓘ Не определено Ожидает подключения
golovaneva-mac.local	Недоступен Не определена	? 1.0.0.1	macOS 12.6.3	ⓘ Не определено	test001	5 параметров	
INB9079.da.lan	Недоступен Не определена	? 0.2.0	Майкрософт Windows 10 Pro 10.0.19043	✔ Соответствует	test001	6 параметров	
NB9079.da.lan	Недоступен Нарушена	? 1.0.1	Майкрософт Windows 10 Pro 10.0.19045	ⓘ Не определено	test 11	82 параметра	
NB9079.da.lan__fake	Недоступен Не определена	? 0.2.0		ⓘ Не определено	test001		
NB9079.da.lan_not	Недоступен Не определена	? 0.2.0		✖ Не соответствует	Профиль настроек 1		
NB9736.da.lan	Недоступен Нарушена	ⓘ 1.1.0.1 Доступно обновление	Майкрософт Windows 10 Pro 10.0.19045	ⓘ Не определено	test 11	82 параметра	
NB9736.da.lan_1	Недоступен Нарушена	ⓘ 1.0.0.1 Доступно обновление	Майкрософт Windows 10 Pro 10.0.19045	ⓘ Не определено	test_NB97_2	90 параметров	
snsf 123	Недоступен Не определена	? 0.2.0	Astra Linux (Smolensk) 1.6	ⓘ Не определено	test_NB97_2	4 параметра	✖ Обнаружены нарушения Ожидает подключения

Рисунок 1 – Раздел «Агенты»

Список агентов реализован в виде таблицы. Для каждой записи списка отображаются данные:

- название и описание агента. Является ссылкой, при переходе по которой открывается окно для просмотра и редактирования;
- состояние (активен/ недоступен) и целостность агента (подтверждена/ нарушена/ не определена)
- версия агента и состояние версии (актуальная версия/ доступно обновление/ нет данных);
- операционная система, на которой установлен агент;
- безопасность – статус соответствия подключенного устройства требованиям политики безопасности (соответствует/ не соответствует/ не определено). Значения «Соответствуют» и «Не соответствуют» являются ссылкой, при переходе по которой открывается окно просмотра результата проверки подключенного устройства (см. п. 4.2.2);
- профиль настроек, который применяются к агенту. При нажатии на профиль в выпадающем окне выводятся настройки, заданные в выбранном профиле

- настроек;
- устройство. Является ссылкой, при переходе по которой открывается окно просмотра списка параметров устройства полученные при инвентаризации данных устройства (см. п. 4.1.1);
 - целостность до загрузки ОС – статус соответствия подключенного устройства требованиям политики контроля целостности до загрузки ОС (нарушения отсутствуют/ обнаружены нарушения/ не определено). Значение «Обнаружены нарушения» является ссылкой, при переходе по которой открывается окно просмотра списка нарушений обнаруженные при проверке подключенного устройства (см. п. 4.2.3). Также для модуля контроля целостности отображается состояние подключения (подключено/ ожидает подключения/ ошибка подключения);
 - политика контроля целостности, который применяется к устройству. При нажатии на политику в выпадающем окне выводятся количество объектов для ОС, заданные в выбранной политике;
 - тип подключения к сети с устройства, на котором установлен агент, пользователь и дата выполнения последнего подключения;
 - последнее изменение – дата внесения последних изменений для агента и имя пользователя ПК «Efros DO», внесившего последние изменения.

 Подробное описание веб-интерфейса раздела «Агенты» приведено в документе «Руководство пользователя. Часть 3. Контроль доступа».

4.2.2 Политика безопасности

Политика безопасности содержит набор требований, которым должно соответствовать устройство, чтобы считаться надежным и безопасным для получения доступа к сетевым ресурсам организации.

Проверка требований политики безопасности устройства, подключенного к корпоративной сети, производится с заданным интервалом.

Для настройки политики безопасности в веб-интерфейсе ПК «Efros DO» необходимо перейти в раздел «Агенты» → «Наборы политик» → вкладка «Безопасность».

В случае обнаружения нарушений требований политики безопасности:

- 1) Для агента будет изменен статус соответствия требованиям политики безопасности.
- 2) В комплексе будет зафиксировано соответствующее событие («События» → «Объекты сети» → «Агенты»).
- 3) Для устройства будет запрещен доступ к ресурсам при наличии соответствующих настроек в политике доступа в сеть (см. п. 4.2.4).
- 4) Если для агента включена настройка изменения авторизации Change of Authorization «Изменение авторизации (CoA)», то будет отправлен запрос аутентификатору на повторную авторизацию конечной точки в сети. Для

пользователя будет применено изменение уровня доступа к корпоративным ресурсам в зависимости от настроенных правил авторизации в политиках доступа в сеть.

При создании требований политики безопасности доступна проверка следующих атрибутов для различных операционных систем:

— Атрибуты ОС Linux:

- USB устройства;
- антивирусные приложения;
- операционная система;
- пакеты;
- процессы;
- сетевые интерфейсы;
- файлы;
- целостность до загрузки ОС.

— Атрибуты ОС Windows:

- USB устройства;
- антивирусные приложения;
- обновления системы;
- операционная система;
- параметры реестра;
- программы;
- процессы;
- разделы реестра;
- сетевые интерфейсы;
- службы;
- файлы;
- целостность до загрузки ОС.

— Атрибуты ОС MacOS:

- USB устройства;
- антивирусные приложения;
- операционная система;
- пакеты;
- процессы;
- сетевые интерфейсы;
- файлы.

Результат проверки приведен в колонке «Безопасность» подраздела «Агенты» или на странице редактирования агента. Возможные значения:

- «Соответствует» – является ссылкой, при переходе по которой открывается окно просмотра результата проверки требований безопасности;
- «Не соответствует» – является ссылкой, при переходе по которой открывается окно просмотра результата проверки требований безопасности;
- «Не определено».

Проверка требований политики безопасности производится при наличии подключения агента ПК «Efros DO» к комплексу и предварительно настроенной политики безопасности.

4.2.3 Политика контроля целостности до загрузки ОС

Политика контроля целостности до загрузки ОС содержит набор требований к объектам ОС, которым должно соответствовать устройство, чтобы считаться надежным и безопасным для получения доступа к сетевым ресурсам организации.

Для настройки политики контроля целостности до загрузки ОС в веб-интерфейсе ПК «Efros DO» необходимо перейти в раздел «Агенты» → «Наборы политик» → вкладка «Контроль целостности».

В случае обнаружения нарушений требований политики будет изменен результат проверки требованиям политики контроля целостности.

Результат проверки приведен в колонке «Целостность до загрузки ОС» подраздела «Агенты» или на странице редактирования агента. Возможные значения:

- «Нарушения отсутствуют»;
- «Обнаружены нарушения» – является ссылкой, при переходе по которой открывается окно просмотра списка нарушений, обнаруженные при проверке подключенного устройства;
- «Не определено».

Проверка требований политики контроля целостности до загрузки ОС производится при наличии подключения агента с модулем «Контроль целостности до загрузки ОС» к комплексу и предварительно настроенной политики контроля целостности.



Для применения созданных/обновленных политик контроля целостности необходимо перезагрузить конечное устройство.

4.2.4 Политика доступа в сеть

ПК «Efros DO» позволяет задавать настройки для управления доступом в сеть на основе списка наборов политик сетевого доступа. Наборы политик позволяют логически группировать политики аутентификации и авторизации в одном наборе.

Статус соответствия устройства требованиям политики безопасности, сформированный на основе данных от агента, может быть использован при настройке правил авторизации.

Для разграничения доступа на основе статуса соответствия требованиям безопасности, необходимо настроить правила авторизации с использованием атрибута «Gazinformservice/ EDO-Compliance-Status». Атрибут может принимать следующие значения:

- «Compliant» – статус «Соответствует»;
- «Non-Compliant» – статус «Не соответствует»;
- «Indeterminate» – статус «Не определено» или отсутствие статуса (если агент был удален с устройства или отключен).

Для настройки политики доступа в сеть в веб-интерфейсе ПК «Efros DO» необходимо перейти в раздел «Контроль доступа» → «Наборы политик» → вкладка «Доступ в сеть».

4.2.5 Политика профилирования

В ПК «Efros DO» поддерживается источник профилирования «Edo-Agent».

Для профилирования конечных точек используются данные инвентаризации конечных точек (см. пункт 4.1.1).

В результате профилирования конечным точкам присваивается профиль (один или несколько) или метки, которые можно использовать при настройке политик доступа в сеть.

При получении или обновлении параметров от источников профилирования конечной точки, осуществляется проверка на соответствие данных условиям политик, заданным в политиках профилирования. В случае совпадения с условиями одной или нескольких политик – конечной точке назначается один или несколько профилей, которые соответствуют названию сработавших активных политик.

Если в политике профилирования задана метка, то она автоматически будет добавлена к конечной точке при срабатывании политики. Если была изменена сама политика профилирования, то происходит автоматическая проверка всех конечных точек на соответствие новым условиям согласно заданным атрибутам.


При использовании настройки «Изменение авторизации (CoA)» в политике профилирования будет отправляться запрос аутентификатору на повторную авторизацию конечной точки в сети при назначении профиля.


Атрибут «EdoAgent / compliance» может быть использован в политиках профилирования в комбинации с настройкой «Изменение авторизации (CoA)», что позволит настроить повторную авторизацию конечной точки в сети при назначении того или иного профиля в случае изменения значения атрибута.

Для настройки политики профилирования в веб-интерфейсе ПК «Efros DO»

необходимо перейти в раздел «Контроль доступа» → «Наборы политик» → вкладка «Профилирование».

4.2.6 Изменение авторизации

 Некоторые устройства не поддерживают возможность изменения авторизации (CoA).

 Для включения возможности изменения авторизации устройства переключатель «Изменение авторизации (CoA)» в настройке агента должен быть установлен в положение «Активен».

Изменение авторизации происходит при изменении статуса соответствия устройства требованиям политики безопасности.

Изменение авторизации устройства может быть настроено двумя способами:

- 1) Настройка политики безопасности. Изменение авторизации произойдет при изменении статуса соответствия требованиям политики безопасности. Включение возможности производится в настройках агента.
- 2) Настройка политики профилирования. Изменение авторизации произойдет при назначении конечной точке соответствующего профиля. Включение возможности производится в настройках политики профилирования («Контроль доступа» → «Наборы политик» → вкладка «Профилирование»).

В случае нарушения требований политики безопасности, статус соответствия требованиям изменится на «Не соответствует». Для пользователя будет применено изменение уровня доступа в зависимости от настроенных правил авторизации в политиках доступа в сеть.

4.3 Схемы разграничения доступа к корпоративным ресурсам

4.3.1 Решение с суппликантом

Схема разграничения доступа к корпоративным ресурсам с использованием агента ПК «Efros DO» со встроенным в ОС суппликантом 802.1X и с суппликантом ПК «Efros DO» приведена на рис. 2.

Агент позволяет произвести инвентаризацию данных конечных точек и выполнить проверку устройства на соответствие требованиям безопасности.

Суппликант ПК «Efros DO» предназначен для реализации возможности проверки устройства на соответствие требованиям безопасности на этапе подключения к корпоративной сети.

Уровень доступа определяется с учетом статуса соответствия устройства требованиям

политики безопасности, настроенной в комплексе.

Предоставление пользователю полного доступа, ограниченного доступа или запрета доступа зависит от настройки соответствующих VLAN или ACL на аутентификаторе и политики доступа в ПК «Efros DO».

После того, как устройство получило доступ к корпоративным ресурсам, агент повторяет проверку устройства с заданным интервалом. В случае изменения статуса соответствия требованиям безопасности, выполняется повторная авторизация с целью изменения уровня доступа.

4.3.2 Решение с VPN

Схема разграничения доступа к корпоративным ресурсам в рамках решения с VPN приведена на рис. 3.

При установке агента ПК «Efros DO» и VPN-клиента на конечной точке выполняются те же функции, что и в решении с суппликантом, но имеются следующие отличия:

- 1) наличие возможности удаленного подключения устройства к корпоративной сети;
- 2) выполнение проверки устройства на соответствие требованиям безопасности происходит после подключения к корпоративной сети;
- 3) требуемые VLAN или ACL настраиваются на VPN-шлюзе.

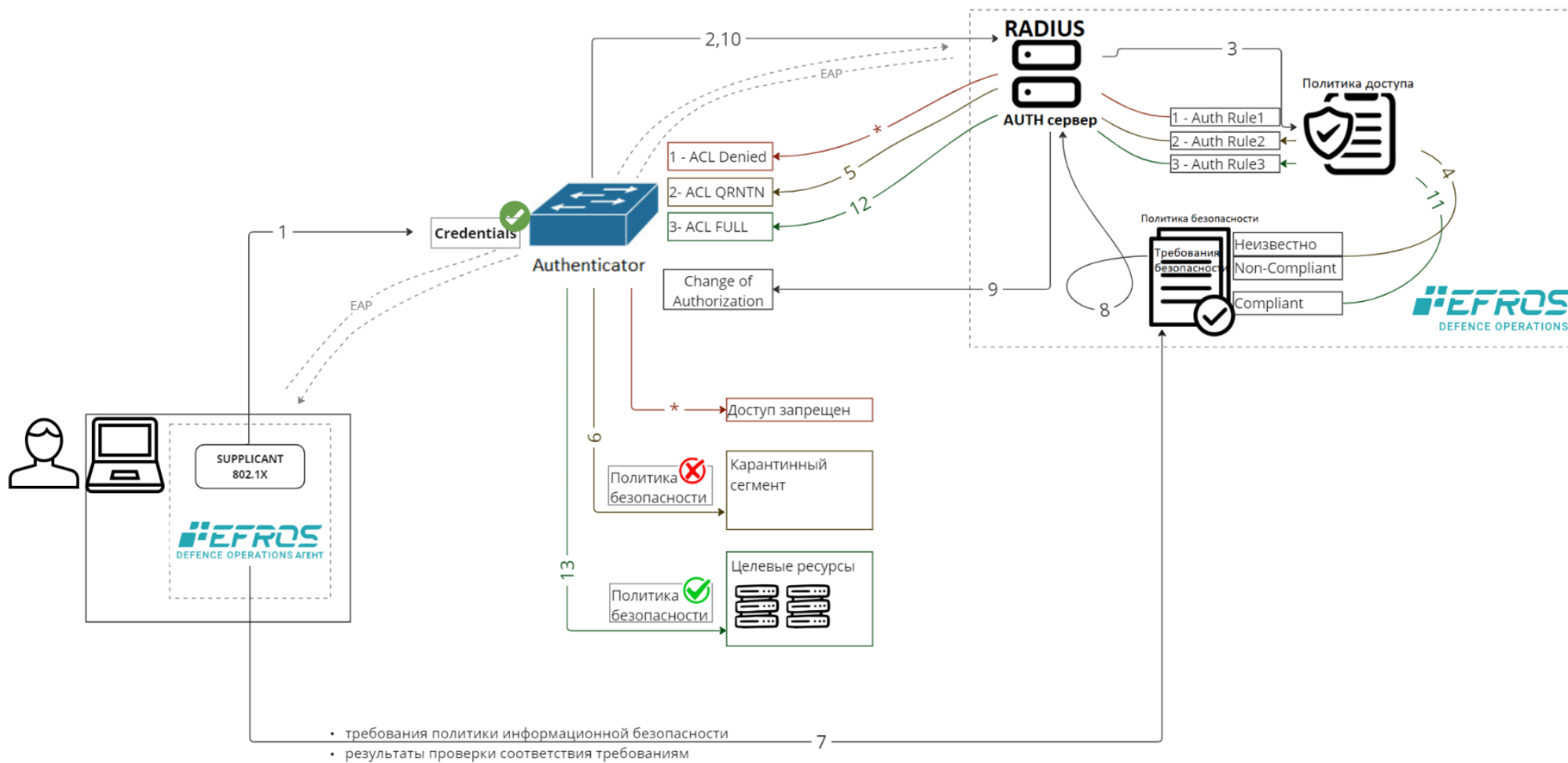


Рисунок 2 – Схема разграничения доступа к корпоративным ресурсам с использованием агента и суппликанта

Последовательность взаимодействия элементов схемы разграничения доступа к корпоративным ресурсам с использованием агента с суппликантом 802.1X, встроенным в ОС, или с суппликантом ПК «Efros DO»:

1 – Пользователь со своего рабочего места выполняет проводное или беспроводное подключение к сети. Агент с помощью одного из суппликанта передает запрос на доступ аутентификатору.

2 – Аутентификатор отправляет запрос доступа на сервер аутентификации RADIUS.

3 – Сервер аутентификации инициирует определение политики доступа в сеть.

4 – Политика доступа определяется с учетом статуса соответствия требованиям политики безопасности. При отсутствии суппликанта ПК «Efros DO» при первом подключении устройства статус неизвестен. При наличии суппликанта ПК «Efros DO» происходит определение статуса соответствия требованиям политики безопасности.

5 – Сервер аутентификации отправляет аутентификатору данные соответствующего VLAN или ACL, в котором содержится направление в ограниченный/карантинный сегмент сети. При наличии суппликанта ПК «Efros DO» возможно получение направления на полный доступ к целевым ресурсам.

6 – Аутентификатор предоставляет доступ устройству к ограниченному/карантинному сегменту сети. При наличии суппликанта ПК «Efros DO» возможно предоставление полного доступа к целевым ресурсам.

7 – Запущенный на рабочем месте пользователя агент получает от ПК «Efros DO» последнюю версию требований политики безопасности, выполняет проверку устройства на соответствие требованиям и передает результаты проверки в ПК «Efros DO».

8 – ПК «Efros DO» обрабатывает данные, поступившие от агента, формирует статус соответствия требованиям политикам безопасности и назначает его устройству. Если устройство соответствует требованиям безопасности, то инициируется отправка запроса на изменение авторизации (CoA).

9 – Сервер аутентификации отправляет запрос на изменение авторизации (CoA) аутентификатору.

10-12 – Аутентификатор повторно запрашивает у сервера аутентификации правило авторизации для безопасного устройства и, получив ответ, выполняет переподключение.

13 – Аутентификатор предоставляет безопасному устройству полный доступ к целевым ресурсам.

* – На схеме обозначено, что в случае необходимости доступ к любым ресурсам в сети организации можно полностью запретить, настроив соответствующий VLAN или ACL на аутентификаторе и политику доступа в ПК «Efros DO».

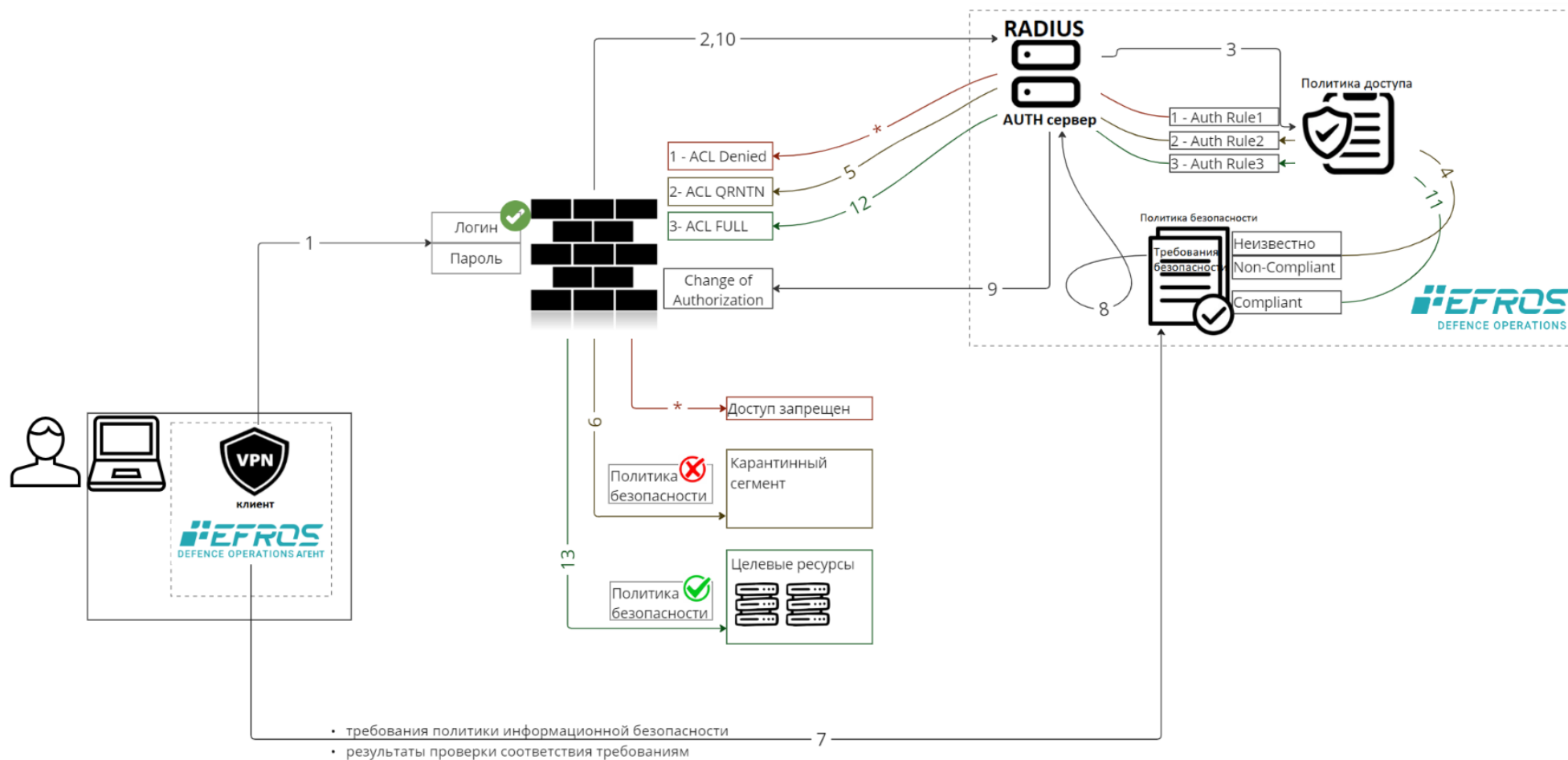


Рисунок 3 – Схема разграничения доступа к корпоративным ресурсам в рамках решения с VPN

Последовательность взаимодействия элементов схемы разграничения доступа к корпоративным ресурсам в рамках решения с VPN:

- 1 – Пользователь на рабочем месте запускает VPN клиента, проходит процесс аутентификации. Запрос на доступ передается VPN-шлюзу.
 - 2 – VPN-шлюз отправляет запрос доступа на сервер аутентификации RADIUS.
 - 3 – Сервер аутентификации инициирует определение политики доступа в сеть.
 - 4 – Политика доступа определяется с учетом статуса соответствия требованиям политики безопасности. При первом подключении устройства статус неизвестен.
 - 5 – Сервер аутентификации отправляет VPN-шлюзу данные соответствующего VLAN или ACL, в котором содержится направление в ограниченный/карантинный сегмент сети.
 - 6 – VPN-шлюз предоставляет доступ устройству к ограниченному/карантинному сегменту сети.
 - 7 – Запущенный на рабочем месте пользователя агент получает от ПК «Efros DO» последнюю версию требований политики безопасности, выполняет проверку устройства на соответствие требованиям и передает результаты проверки в ПК «Efros DO».
 - 8 – ПК «Efros DO» обрабатывает данные, поступившие от агента, формирует статус соответствие требованиям политикам безопасности и назначает его устройству. Если устройство соответствует требованиям безопасности, то инициируется отправка запроса на изменение авторизации (CoA).
 - 9 – Сервер аутентификации отправляет запрос на изменение авторизации (CoA) VPN-шлюзу.
 - 10-12 – VPN-шлюз повторно запрашивает у сервера аутентификации правило авторизации для безопасного устройства и, получив ответ, выполняет переподключение.
 - 13 – VPN-шлюз предоставляет безопасному устройству полный доступ к целевым ресурсам.
- * – На схеме обозначено, что в случае необходимости доступ к любым ресурсам в сети организации можно полностью запретить, настроив соответствующий VLAN или ACL на VPN-шлюзе и политику доступа в ПК «Efros DO».

Приложение А

Рекомендуемая последовательность действий для настройки подключения к сети с помощью агента и суппликанта

- ❗ В начале необходимо убедиться, что все предварительные действия выполнены:
 - на устройстве пользователя установлен агент ПК «Efros DO»;
 - на устройстве пользователя установлен суппликант ПК «Efros DO», при необходимости;
 - настроен аутентификатор, в том числе VLAN или ACL, для требуемых вариантов доступа к корпоративной сети.

- ❗ В приложении А приведен пример заполнения минимально необходимых полей для подключения устройства к корпоративной сети с помощью агента или агента с суппликантом ПК «Efros DO».

А.1 Настройка подключенного агента

Последовательность действий для настройки подключенного агента:

- 1) Перейти в раздел «Агенты» → «Профили настроек».
- 2) Нажать кнопку «+ Профиль» (рис. 4).

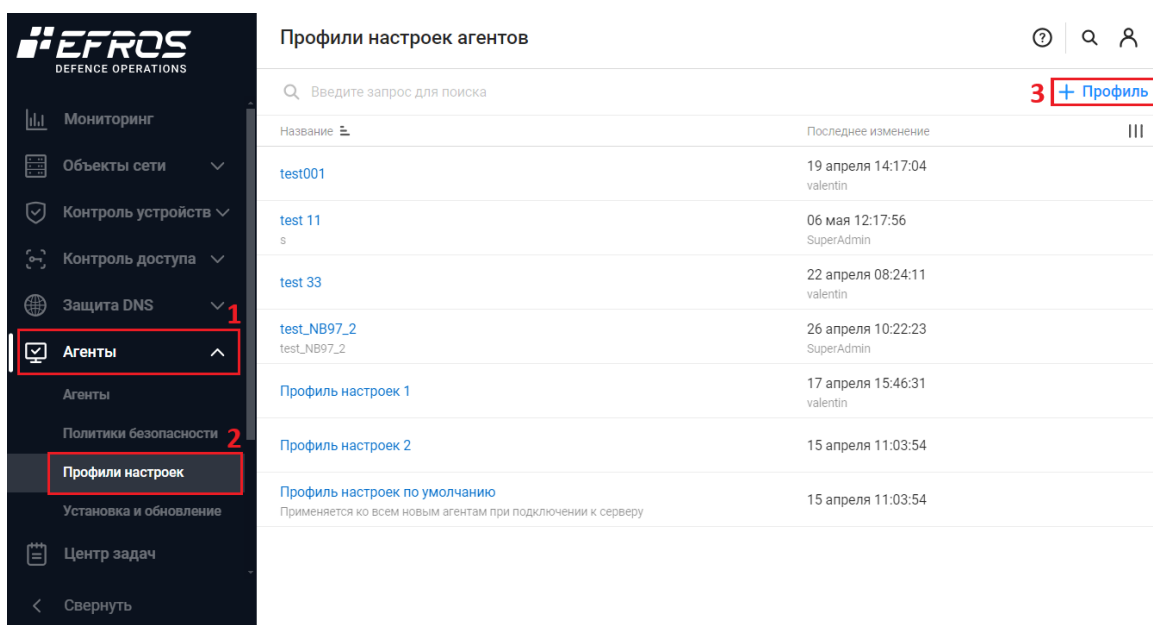


Рисунок 4 – Подраздел «Профили настроек агентов»

- 3) Откроется страница «Создание профиля» (рис. 5). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать».

< Создание профиля

Название

Описание

Проверка требований политики ⓘ секунд

Изменение авторизации (CoA) ⓘ

Время переподключения ⓘ секунд

Контроль целостности агента

Проверка целостности ⓘ секунд

Рисунок 5 – Страница «Создание профиля»

Особенности заполнения полей описаны ниже:

- поле «Проверка требований политики»: 30 секунд;
- поле «Изменение авторизации (CoA)»: активен;
- поле «Время переподключения»: 5 секунд;
- поле «Контроль целостности»: активен;
- поле «Проверка целостности»: 60 секунд.

Переключатель «Изменение авторизации (CoA)» предназначен для включения отправки запроса на оборудование на изменение параметров сессии (Change of Authorization) при изменении статуса соответствия подключенного к сети устройства требованиям политики безопасности.

Поле «Время переподключения» предназначено для ввода значения допустимого времени ожидания возобновления связи с агентом после изменения авторизации (CoA). По истечении времени состояние агента будет изменено на «Недоступен».

- ⓘ Параметры запроса изменения авторизации (CoA) настраиваются в профиле оборудования в блоке «Change of Authorization».

Переключатель «Контроль целостности агента» предназначен для включения проверки целостности агента по контрольным суммам основных компонентов агента.

i Аналогично можно отредактировать «Профиль настроек по умолчанию».

- 4) Перейти в раздел «Агенты» (см. рис. 1) и нажать на название требуемого агента.
- 5) На вкладке «Настройки» изменить профиль настроек и настроить применение политики контроля целостности (рис. 6).

i Создание политики контроля целостности до загрузки ОС приведено в Приложении А.4.

< !NB9079.da.lan

Настройки Дополнительно


Название

Описание


Состояние агента Недоступен

Безопасность Соответствует

Целостность агента Не определена

Профиль настроек 

Модуль контроля целостности **i**

Политика контроля целостности 

Статус подключения модуля Ожидание выполнения

Целостность до загрузки ОС **i** Не определено

Рисунок 6 – Вкладка «Настройки» выбранного агента

- 6) На вкладке «Настройки» при нажатии в поле «Безопасность» на значение «Соответствует» или «Не соответствует» откроется окно результата проверки подключенного устройства на соответствие заданным требованиям политики безопасности (рис. 7). Данные значения также приведены в колонке «Безопасность» подраздела «Агенты».

- ❗ Проверка требований политики безопасности производится при наличии подключения агента ПК «Efros DO» к комплексу и предварительно настроенной политики безопасности.

✕ !NB9079.da.lan

Результат проверки	✔ Соответствует
Дата проверки	31 января 11:39:05
Политика безопасности	test2132

Требования политики безопасности

🔍 Введите запрос для поиска

▼ ✔ test

И	И	Обновления системы ▶ Категория обновлений Равно Доступные
	И	Описание Содержит HP Development Company
Полученные значения: Available ▼		
И	И	Обновления системы ▶ Категория обновлений Равно Установленные
	И	Код обновления Равно KB4464538
Полученные значения: Installed ▼		

Рисунок 7 – Окно результата проверки требований политики безопасности

Для агента в заголовке указано наименование и приведены следующие данные:

- результат проверки: «Соответствует», «Не соответствует»;
- дата и время проверки;
- наименование политики безопасности.

Область «Требования политики безопасности» содержит поле поиска по названию требования и список проверок с раскрывающимися строками блоков условий. Блоки условий состоят из наименования, описания требований политики безопасности и объединены логическими операторами «И», «ИЛИ».

В зависимости от результата проверки требований, для блока условий применены следующие цветовые обозначения:

- зеленый – проверка пройдена успешно;
- красный – проверка не пройдена;

— серый – проверка не производилась.

Количество полученных значений, сформированных в ходе проверки условий блока, приводится под блоком условия. Для просмотра значений необходимо нажать на кнопку «Полученные значения».

- 7) На вкладке «Настройки» при нажатии в поле «Целостность до загрузки ОС» на значение «Обнаружены нарушения» откроется окно просмотра списка нарушений (рис. 8). Данные значения также приведены в колонке «Целостность до загрузки ОС» подраздела «Агенты»

i Проверка требований политики контроля целостности до загрузки ОС производится при наличии подключения агента с модулем «Контроль целостности до загрузки ОС» к комплексу и предварительно настроенной политики контроля целостности.

× snsl

Результат проверки ✖ Обнаружены нарушения

Дата проверки 24 апреля 2024 12:56:15

Политика контроля целостности new_policy

Список нарушений

🔍 Введите запрос для поиска

Объект	Тип нарушения
NVMe S/N: c00c01700c0000e01000000000000000 64.04GB NTFS\5100\5100.txt	Нарушена целостность файлового объекта
NVMe S/N: c00c01700c0000e01000000000000000 64.04GB NTFS\test\	Файловый объект не найден
NVMe S/N: c00c01700c0000e01000000000000000 64.04GB NTFS\test\test – копия (...)	Файловый объект не найден

Рисунок 8 – Окно просмотра списка нарушений

Для устройства, у которого обнаружены нарушения до загрузки ОС, приведены следующие данные:

- результат проверки: «Обнаружены нарушения»;
- дата и время проверки;
- наименование политики контроля целостности.

Список нарушений реализован в виде таблицы. Для каждой записи списка отображаются данные:

- объект – путь к проверяемому объекту;
- тип нарушения.

- 8) На вкладке «Дополнительно» доступен просмотр параметров устройства, на котором установлен выбранный агент (рис. 9).

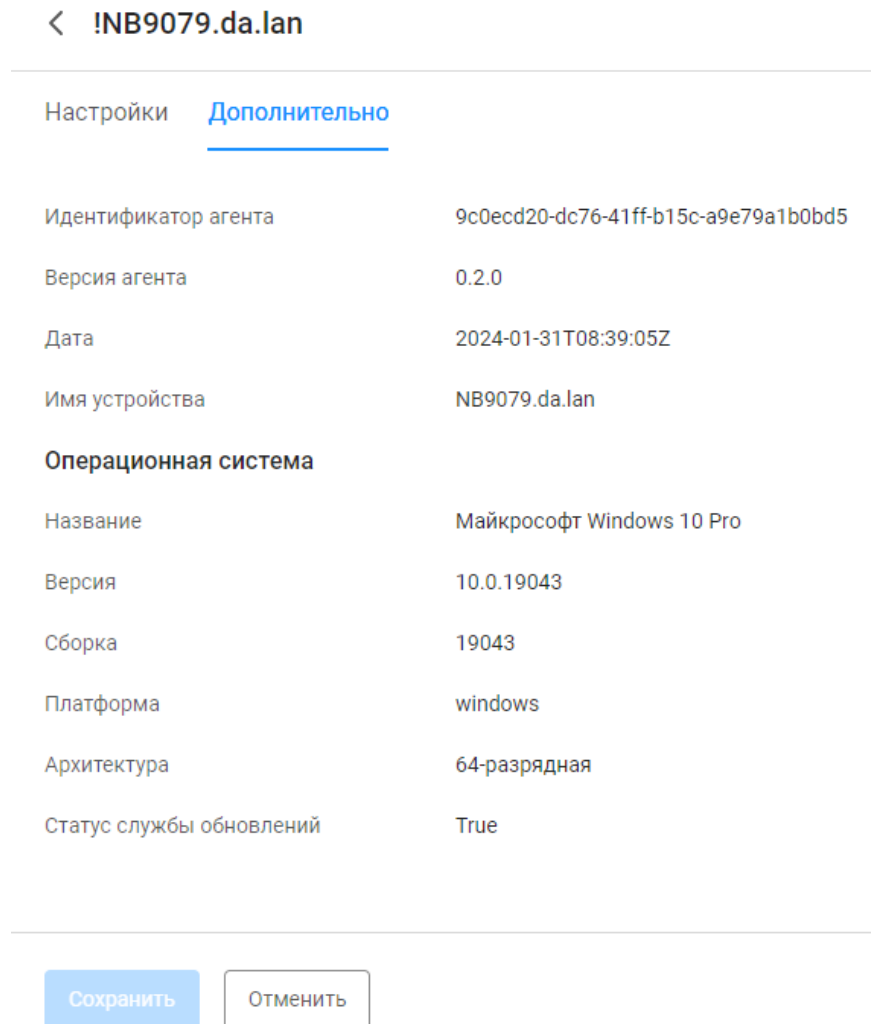


Рисунок 9 – Вкладка «Дополнительно» выбранного агента

A.2 Настройка расписания обновления

Последовательность действий для настройки расписания обновления агента, а также установки и (или) обновления дополнительных модулей инсталляционного пакета:

- 1) Перейти в раздел «Агенты» → «Установка и обновление» → вкладка «Обновление».
- 2) Нажать кнопку «**+** **Расписание**» (рис. 10).

The screenshot displays the 'Установка и обновление' (Installation and update) section of the Efros DO software. The left sidebar contains navigation options, with 'Агенты' (Agents) marked with a red box and the number 1, and 'Установка и обновление' (Installation and update) marked with a red box and the number 2. The main content area shows a table of updates. A red box with the number 3 highlights the 'Обновление' (Update) tab, and a red box with the number 4 highlights the '+ Расписание' (Schedule) button. The table lists various updates with columns for Name, Target version, Updatable agents, Start time, Status, and Last change.

Название	Целевая версия	Обновляемые агенты	Время запуска	Статус	Последнее изменение
asd12312asdadasdas	Linux x86_64 0.2.0	11	31 мая 18:42:31	Завершено с ошибками	31 мая 18:52:00 reshetnikov-d
Test #1 Test #1	Linux x86_64 0.2.0	2	31 мая 14:45:53	Завершено с ошибками	31 мая 14:55:00 SuperAdmin
Test_ Test_	Linux x86_64 0.2.0	11	31 мая 14:44:26	Завершено с ошибками	31 мая 14:54:00 reshetnikov-d
test2105 ttttt	2	Все	31 мая 10:58:39	Выполняется	22 мая 14:20:51 SuperAdmin
qwewqwewe	Windows x86_64 1.0.1	Все	30 мая 15:39:38	Завершено с ошибками	30 мая 15:49:53 DA\Iv.Ivanova
qwewe	Windows x86_64 1.0.0.17...	Все	30 мая 15:33:22	Завершено с ошибками	30 мая 15:43:43 DA\Iv.Ivanova
Артём	Windows x86_64 1.1.0.1	NB9736.da.lan	30 мая 15:25:36	Завершено с ошибками	30 мая 15:36:01 DA\myagkov-aa
Еще один тест создания из т...	Windows x64 0.2.0	6	30 мая 14:50:50	Завершено с ошибками	30 мая 15:00:00 reshetnikov-d
test00885	Windows x86_64	Все	28 мая 16:13:48	Завершено с ошибками	28 мая 16:23:00 valentin
test00	Linux x86_64	Все	28 мая 16:11:59	Завершено с ошибками	28 мая 16:21:00 valentin
Тестовое расписание из таб... Тестовое расписание из таблицы...	Linux x86_64 1.0.0.1	10	27 мая 23:38:50	Завершено с ошибками	27 мая 23:48:00 reshetnikov-d

Рисунок 10 – Подраздел «Установка и обновление», вкладка «Обновление»

3) Откроется страница создания расписания. Необходимо заполнить поля требуемыми параметрами (рис. 11).

< Создание расписания

Название	<input type="text" value="new"/>
Описание	<input type="text" value="Описание"/>

Обновляемые агенты ⓘ	<input type="button" value="Все"/> <input type="button" value="Выбранные"/>										
Агенты	2 агента										
Целевая версия ⓘ	<table><tr><td><input type="text" value="Windows x86_64"/></td><td>▼</td><td><input type="text" value="1.2.0"/></td><td>▼</td><td>+ <input type="button" value="Удалить"/></td></tr><tr><td><input type="text" value="Astra 1.7 x86_64"/></td><td>▼</td><td><input type="text" value="1.1.0"/></td><td>▼</td><td>+ <input type="button" value="Удалить"/></td></tr></table>	<input type="text" value="Windows x86_64"/>	▼	<input type="text" value="1.2.0"/>	▼	+ <input type="button" value="Удалить"/>	<input type="text" value="Astra 1.7 x86_64"/>	▼	<input type="text" value="1.1.0"/>	▼	+ <input type="button" value="Удалить"/>
<input type="text" value="Windows x86_64"/>	▼	<input type="text" value="1.2.0"/>	▼	+ <input type="button" value="Удалить"/>							
<input type="text" value="Astra 1.7 x86_64"/>	▼	<input type="text" value="1.1.0"/>	▼	+ <input type="button" value="Удалить"/>							
Дополнительные модули агента ⓘ	<input checked="" type="checkbox"/> Контроль целостности до загрузки ОС										
Запуск расписания ⓘ	<input type="button" value="Значение"/> <input type="button" value="Немедленно"/>										
Время запуска	<input type="text" value="05.07.2024 20:00:00"/> <input type="button" value="Календар"/>										

<input type="button" value="Создать"/>	<input type="button" value="Отменить"/>
--	---

Рисунок 11 – Создание расписания

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Обновляемые агенты»: выбранные;
- поле «Агенты»: выбрать требуемые агенты (рис. 12);
- поле «Целевая версия»: выбрать ОС и версию инсталляционного пакета;

ⓘ Если версия агента и/или дополнительных модулей ниже целевой версии, то они будут обновлены до целевой версии.

Если версия агента выше целевой версии, то обновление выполняться не будет.

Если версия дополнительных модулей не соответствует версии агента, то они будут переустановлены.

- поле «Дополнительные модули агента»: выбрать модуль;

ⓘ Дополнительные модули, устанавливаются из инсталляционного пакета в случае их отсутствия на устройстве.

Если модули уже установлены, то они будут автоматически обновлены при запуске задачи, выбирать их в настройках расписания не требуется.

- поле «Запуск расписания»: значение;
- поле «Время запуска»: любое.

× **Агенты**

<input type="checkbox"/> Название	Версия	Операционная система	III
<input type="checkbox"/> astra16-dev05.ecitest.dom1	? 1.1.0.1	Linux x86_64	
<input type="checkbox"/> deviceName-name	? 0.2.0		
<input checked="" type="checkbox"/> NB9736.da.lan	✓ 1.1.0.1 Актуальная	Windows x86_64	
<input type="checkbox"/> NB9079.da.lan	? 1.0.1		
<input type="checkbox"/> contract8637.da.lan	? 1.0.0.28051		
<input type="checkbox"/> NB9079.da.lan__fake	? 0.2.0		
<input checked="" type="checkbox"/> u11pve-as17-devAM	? 1.0.0.1	Linux x86_64	
<input type="checkbox"/> golovaneva-mac.local	? 1.0.0.1		

Всего: 14

Рисунок 12 – Выбор агентов для обновления

A.3 Создание политики безопасности

Последовательность действий для настройки политики безопасности:

- 1) Перейти в раздел «Агенты» → «Наборы политик» → вкладка «Безопасность».
- 2) Нажать кнопку «+ Политика» (рис. 13).

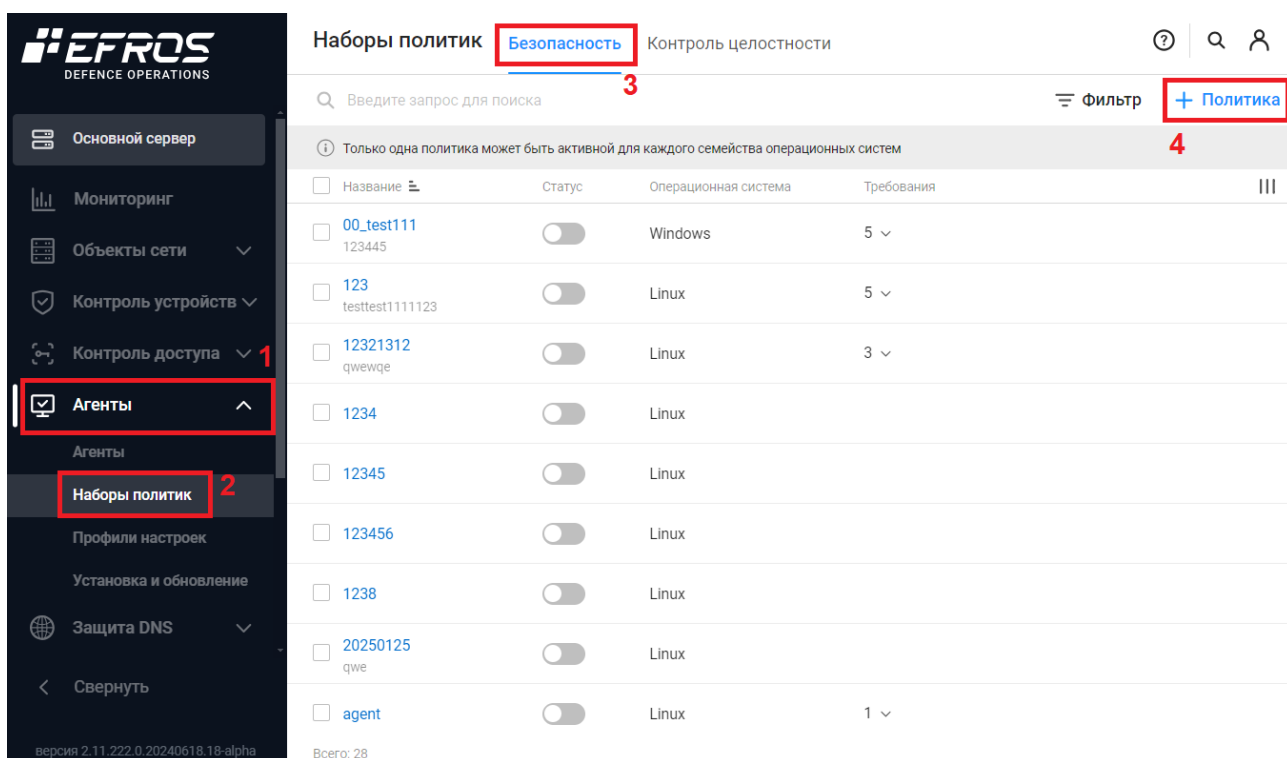


Рисунок 13 – Подраздел «Наборы политик», вкладка «Безопасность»

- 3) Откроется страница создания политики безопасности. Требуется ввести название политики, выбрать семейство операционных систем и нажать кнопку «Создать» (рис. 14).

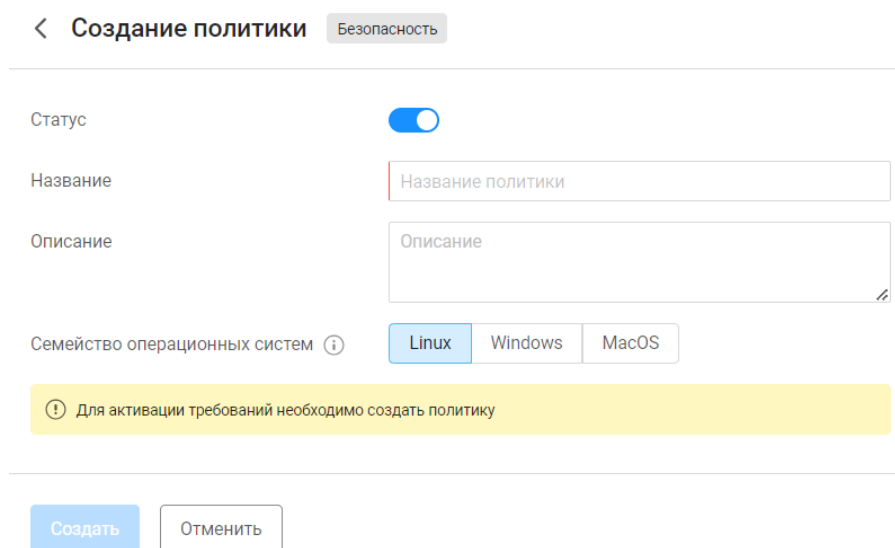


Рисунок 14 – Создание политики безопасности

- 4) После создания политики необходимо перейти на вкладку «Требования» и нажать кнопку «+ Требование» (рис. 15).

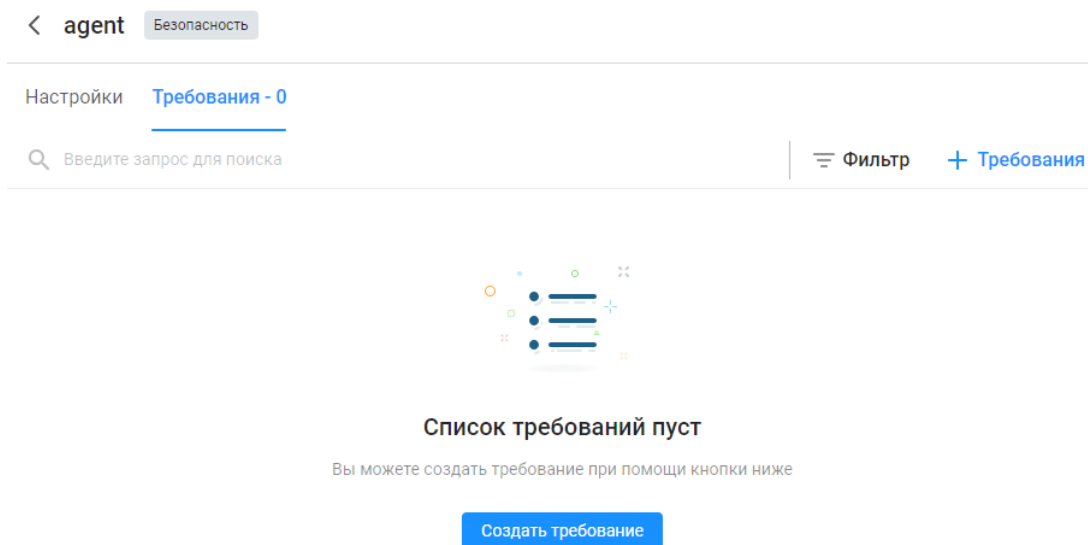


Рисунок 15 – Вкладка «Требования»

- 5) На странице создания требования политики необходимо ввести название, объект и условия проверки с учетом логических операторов «И»/«ИЛИ» (рис. 16).

< Создание требования Безопасность

Статус

Название requirements_agent

Описание Описание

Условия

И ИЛИ Объект

Объект Операционная система

Семейство Семейство Равно Равно Linux

Условия

И ИЛИ Условие

Версия Версия Начинается с 1.9

Дата установки Дата установки Больше Больше 09.01.2024 09:00:00

Сохранить Отменить

Рисунок 16 – Создание требования политики безопасности

Созданные требования политики безопасности приведены на рис. 17.

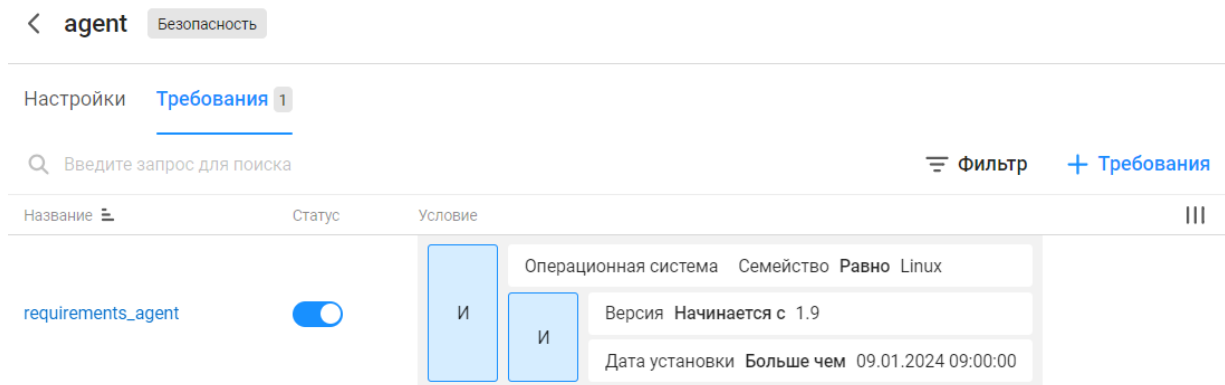


Рисунок 17 – Созданные требования политики безопасности

В результате настроенных требований политик безопасности для устройства будет определяться статус соответствия.

Для разграничения доступа в сеть на основе статуса соответствия требованиям политики безопасности, необходимо настроить в политике «Доступ в сеть» правила авторизации с использованием атрибута «Gazinformservice/ EDO-Compliance-Status» (пример приведен в Приложении А).



Если разграничение доступа в сеть не настроено, то статус соответствия требованиям политики безопасности устройства не будет влиять на доступ к корпоративной сети.

А.4 Создание политики контроля целостности до загрузки ОС

Последовательность действий для настройки политики контроля целостности до загрузки ОС:

- 1) Перейти в раздел «Агенты» → «Наборы политик» → вкладка «Контроль целостности».
- 2) Нажать кнопку «+ Политика» (рис. 18).

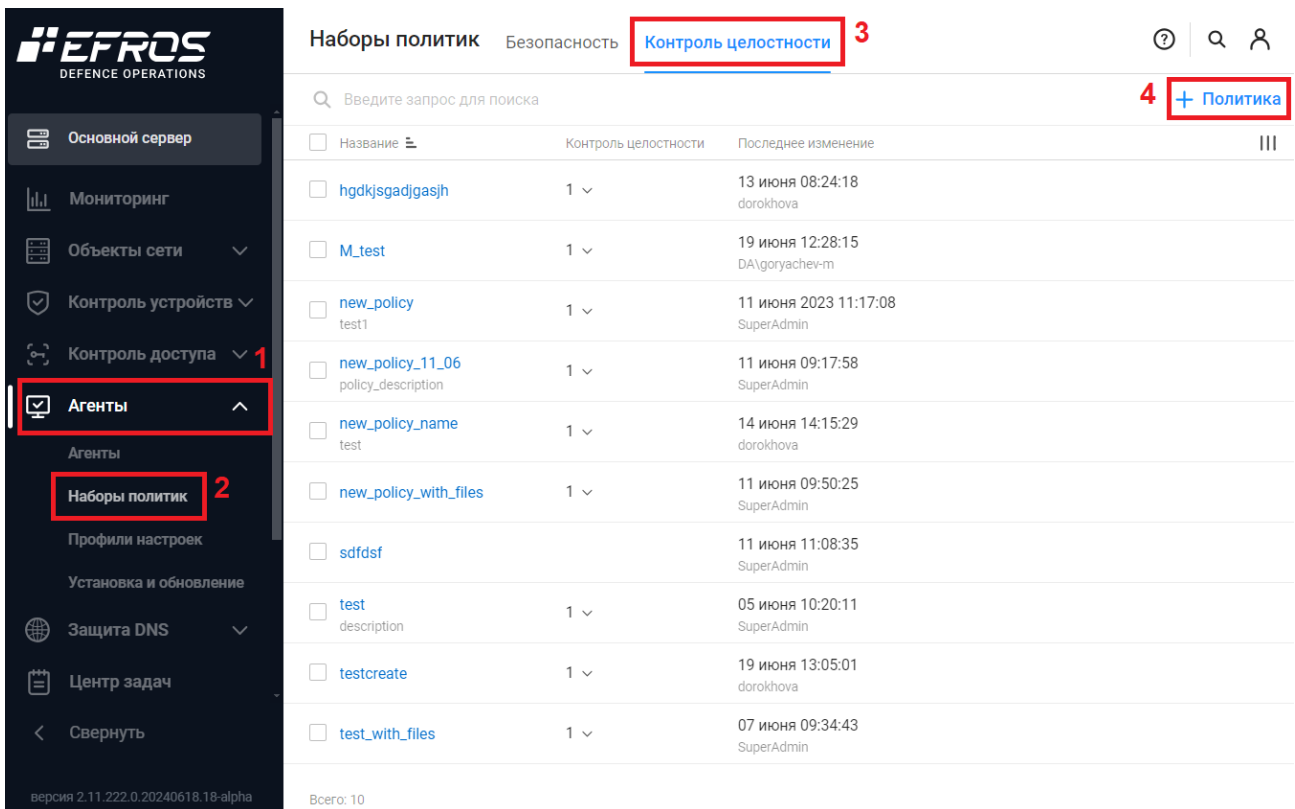


Рисунок 18 – Вкладка «Контроль целостности»

- 3) Откроется страница создания политики контроля целостности. Необходимо заполнить поля требуемыми значениями и нажать кнопку «Создать» (рис. 19).

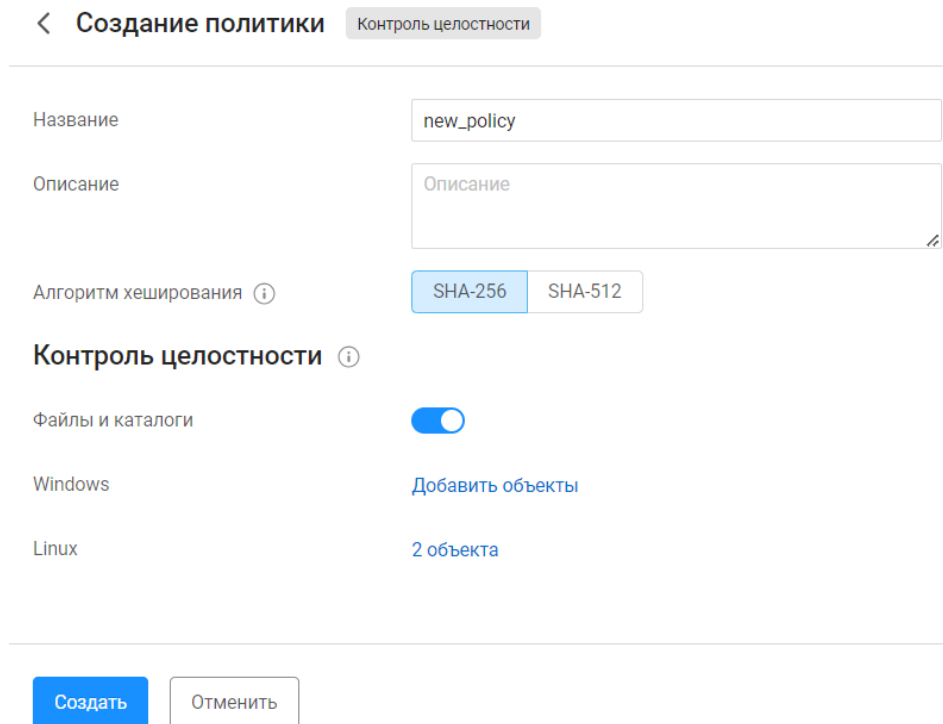
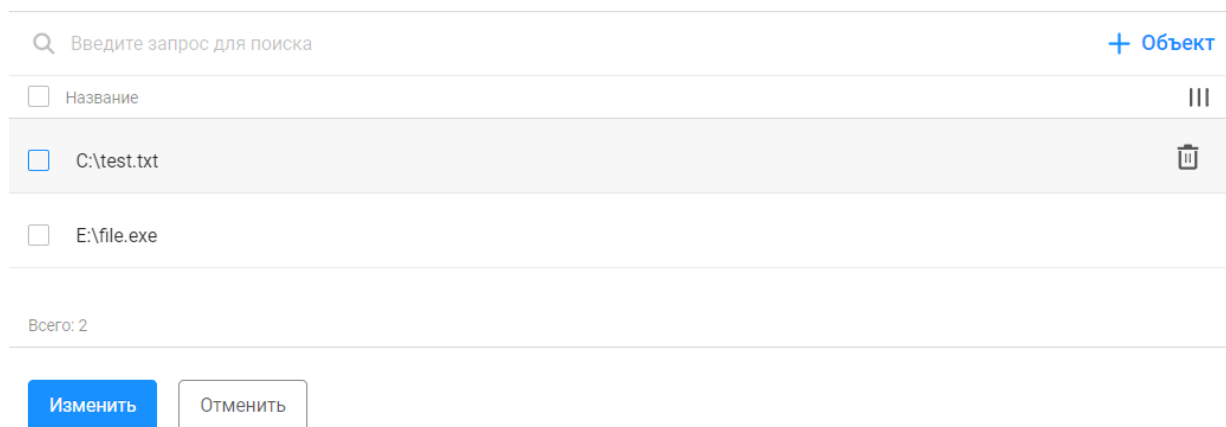


Рисунок 19 – Создание политики контроля целостности

Особенности заполнения полей страницы описаны ниже:

- поле «Название»: любое;
- поле «Алгоритм хеширования»: SHA-256;
- поле «Файлы и каталоги»: активен;
- поле «Windows»: добавить требуемые объекты (рис. 20);
- поле «Linux»: добавить требуемые объекты (рис. 21).

× Файлы и каталоги Windows



Введите запрос для поиска + Объект

Название ☰

C:\test.txt 🗑️

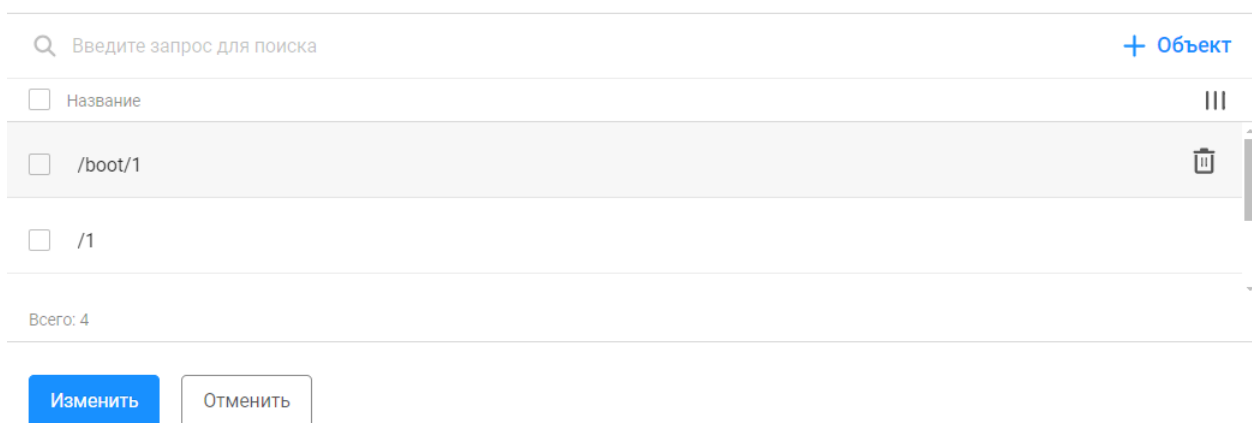
E:\file.exe

Всего: 2

Изменить Отменить

Рисунок 20 – Добавление объектов Windows

× Файлы и каталоги Linux



Введите запрос для поиска + Объект

Название ☰

/boot/1 🗑️

/1

Всего: 4

Изменить Отменить

Рисунок 21 – Добавление объектов Linux



Для применения созданных/обновленных политик контроля целостности необходимо перезагрузить конечное устройство.

A.5 Настройка разрешенных протоколов

! При работе только с агентом (без суппликанта ПК «Efros DO») список разрешенных протоколов можно не настраивать. Достаточно использовать список протоколов по умолчанию.

Последовательность действий для настройки разрешенных протоколов:

1) Создать настройки TLS:

- перейти в раздел «Контроль доступа» → «Разрешенные протоколы» → вкладка «Настройки TLS» → кнопка «+ Настройки TLS» (рис. 22);
- откроется страница создания настройки TLS. Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать» (рис. 23).

Название	Системный сертификат	Доверенный сертифи...	Кэширование	Время жизни кэша	Проверять список отзыва сертификатов	OCSP	Последнее изменение
098	Efros DefOps Server Certif...	6	Отключен	10 часов	Отключен	Отключен	04 июня 00:14:02 System
0981	Efros DefOps Server Certif...	10	Отключен	10 часов	Отключен	Отключен	04 июня 00:14:03 System
0982	Efros DefOps Server Certif...	7	Отключен	10 часов	Отключен	Отключен	31 мая 12:47:49 System
a-test-tls2f	Efros DefOps Server Certif...	Efros DefOps Node ...	Включен	24 часа	Отключен	Отключен	23 апреля 09:32:43 System
b-test	ServerCertTest	Efros DefOps Node ...	Отключен	1 час	Отключен	Включен	04 июня 00:14:05 System
fgfdgfdgdfg	Efros DefOps Server Certif...	Efros DefOps Node ...	Включен	1 час	Включен	Включен	01 января 02:30:17
Golovaneva	Efros DefOps Server Certif...	Efros DefOps Node ...	Отключен	1 час	Отключен	Отключен	01 января 02:30:17
qqq	ServerCertTest	3	Включен	1 час	Отключен	Отключен	23 апреля 09:32:43 System
test	Efros DefOps Server Certif...	Efros DefOps Node ...	Отключен	1 час	Отключен	Отключен	01 января 02:30:17
test	ServerCertTest	Efros DefOps Node ...	Включен	1 час	Отключен	Отключен	23 апреля 09:32:42 System
test123	Efros DefOps Server Certif...	3	Отключен	1 час	Включен	Отключен	10 июня 15:11:54 System

Рисунок 22 – Подраздел «Разрешенные протоколы», вкладка «Настройки TLS»

< Создание настройки TLS

Название	<input type="text" value="tls-common"/>
Системный сертификат	<input type="text" value="Efros ACS Server Certificate"/>
Доверенный сертификат	<input type="text" value="Efros ACS Node CA"/>
Минимальная версия TLS	<input type="text" value="TLS 1.0"/>
Максимальная версия TLS	<input type="text" value="TLS 1.2"/>
Кэширование	<input type="checkbox"/>
Проверять список отзыва сертификатов	<input checked="" type="checkbox"/>
OCSP	<input checked="" type="checkbox"/>

Рисунок 23 – Создание настройки TLS

Особенности заполнения полей страницы создания настроек TLS описаны ниже:

- поле «Название»: любое;
- поле «Системный сертификат»: выбрать сертификат из списка;
- поле «Доверенный сертификат»: выбрать сертификат из списка;
- поле «Минимальная версия TLS»: TLS 1.0;
- поле «Максимальная версия TLS»: TLS 1.2;
- поле «Проверять список отзыва сертификатов»: активен;
- поле «OCSP»: активен.

2) Включить метод проверки подлинности EAP-TNC:

- перейти в раздел «Контроль доступа» → «Разрешенные протоколы» → вкладка «Доступ в сеть» → кнопка «[+ Список протоколов](#)» (рис. 24);
- откроется страница создания списка разрешенных протоколов. Заполнить поля требуемыми параметрами для активации возможности использования необходимых протоколов и включить метод проверки подлинности EAP-TNC в блоке протоколов EAP-TTLS и PEAP (рис. 25).

! Метод проверки подлинности EAP-TNC необходимо включать при использовании суппликанта ПК «Efros DO» для выполнения проверки устройства на соответствие требованиям политики безопасности на этапе подключения к корпоративной сети.

The screenshot displays the 'Allowed protocols' section of the Efros DO interface. The 'Access to network' tab is selected and highlighted with a red box (3). A search bar is present with the text 'Введите запрос для поиска' and a red box (4) around the '+ Список протоколов' button. The table below lists various protocols, including EAP-MD5 and several ACS_Imported_Network_Access entries.

Название	Протоколы	Последнее изменение
0001234	EAP-MD5	17 апреля 14:32:43 test-s
123 Description121	2	21 мая 15:18:43 SuperAdmin
ACS_Imported_Network_Access Импортированный набор разрешенных протоколов		21 марта 16:34:18 SuperAdmin
ACS_Imported_Network_Access1 Импортированный набор разрешенных протоколов	4	21 марта 16:52:12 SuperAdmin
ACS_Imported_Network_Access10 Импортированный набор разрешенных протоколов		24 мая 10:50:41 geer
ACS_Imported_Network_Access11 Импортированный набор разрешенных протоколов		24 мая 14:48:30 geer
ACS_Imported_Network_Access12 Импортированный набор разрешенных протоколов		28 мая 17:23:59 Shulepova
ACS_Imported_Network_Access13 Импортированный набор разрешенных протоколов		28 мая 17:39:13 Shulepova
ACS_Imported_Network_Access14 Импортированный набор разрешенных протоколов		28 мая 18:10:18 Shulepova
ACS_Imported_Network_Access2 Импортированный набор разрешенных протоколов		25 марта 12:46:40 SuperAdmin
ACS_Imported_Network_Access3 Импортированный набор разрешенных протоколов		25 марта 14:15:10 SuperAdmin

Рисунок 24 – Подраздел «Разрешенные протоколы», вкладка «Доступ в сеть»

← **Создание списка разрешенных протоколов** Доступ в сеть

Название	<input type="text" value="Authenticity-protocol"/>
Описание	<input type="text" value="Описание"/>
Тип EAP по умолчанию ⓘ	<input type="text" value="TEAP"/> ▼
Время ответа на EAP пакет	<input type="text" value="60"/> секунд
Максимально открытых сессий	<input type="text" value="16 384"/>

EAP-MD5

EAP-FAST

Настройки TLS	<input type="text" value="tls-common"/> ▼
Метод по умолчанию	<input type="text" value="EAP-MSCHAPv2"/> ▼
Идентификатор сервера ⓘ	<input type="text" value="Efros Defence Operation"/>
Срок действия PAC	<input type="text" value="1"/> <input type="text" value="неделя"/> ▼

EAP-MSCHAPv2

EAP-TLS

Настройки TLS	<input type="text" value="tls-common"/> ▼
---------------	---

EAP-TTLS

Рисунок 25 – Создание списка разрешенных протоколов доступа в сеть

Список доступных для активации протоколов:

- «EAP-MD5»;
- «EAP-FAST»;
- «EAP-TLS»;
- «EAP-TTLS» с методом проверки подлинности «EAP-TNC»;
- «PEAP» с методом проверки подлинности «EAP-TNC»;
- «TEAP».

А.6 Настройка профиля сетевого оборудования и самого сетевого оборудования

Последовательность действий для настройки сетевого оборудования:

- 1) Создать профиль сетевого оборудования для аутентификатора:
 - перейти в раздел «Контроль доступа» → «Профили оборудования» → кнопка «+ Профиль» (рис. 26);
 - откроется страница создания профиля сетевого оборудования. Заполнить поля необходимыми параметрами (рис. 27-28).

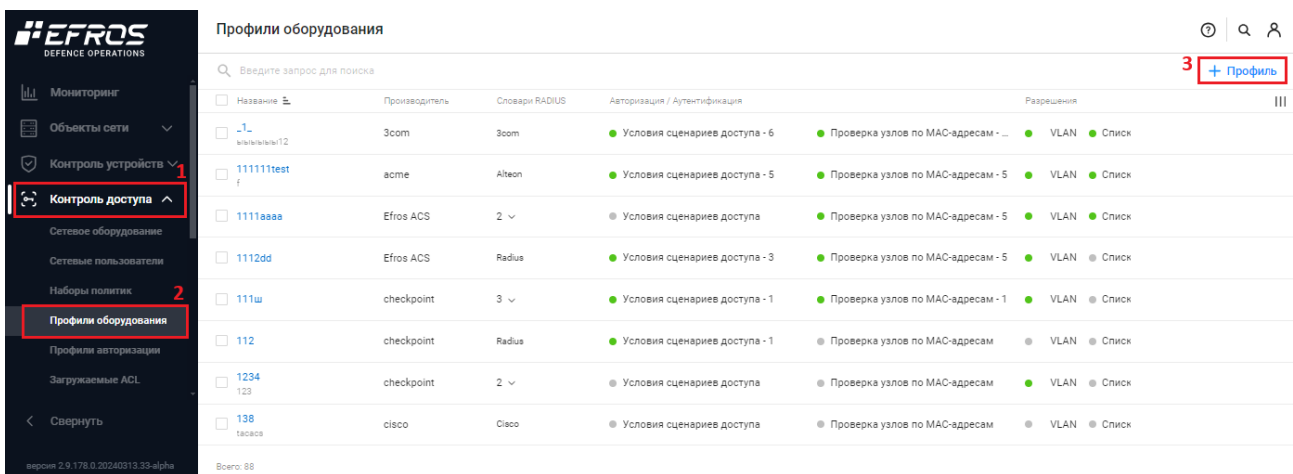


Рисунок 26 – Подраздел «Профили оборудования»

< Создание профиля сетевого оборудования

Название	<input type="text" value="_1_"/>
Описание	<input type="text" value="Описание"/>
Производитель	<input type="text" value="cisco"/>
Словари RADIUS	<input type="text" value="Выбрано: 2"/>

Аутентификация / Авторизация

Условия сценариев доступа

- Проводная аутентификация по MAC-адресам (Wired MAB)
- | | | | | |
|------------------------|---|------------|---|---|
| Radius / NAS-Port-Type | = | Ethernet | + | 🗑 |
| Radius / Service-Type | = | Call-Check | + | 🗑 |
- Беспроводная аутентификация по MAC-адресам (Wireless MAB)
- Проводная аутентификация по стандарту 802.1X (Wired 802.1X)
- | | | | | |
|------------------------|---|-------------|---|---|
| Radius / NAS-Port-Type | = | Ethernet | + | 🗑 |
| Radius / Service-Type | = | Framed-User | + | 🗑 |
- Беспроводная аутентификация по стандарту 802.1X (Wireless 802.1X)
- | | | | | |
|----------------------------|---|---------------------------|---|---|
| Radius / NAS-Port-Type | = | Virtual | + | 🗑 |
| Cisco-ASA / ASA-ClientType | = | AnyConnect-Client-SSL-VPN | + | 🗑 |
- Управление сетевыми устройствами (Device Administration)
- Удаленный доступ (VPN)

Проверка узлов по MAC-адресам (MAB)


- Метод проверки узлов
- С использованием PAP/ASCII
- Проверить пароль
- Проверить атрибут Calling-Station-Id на соответствие MAC-адресу
- С использованием CHAP
- С использованием EAP-MD5

Рисунок 27 – Создание профиля сетевого оборудования. Блок полей «Аутентификация / авторизация»

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Производитель»: cisco;

— поле «Словари RADIUS»: Radius, Cisco, Cisco-ASA;

-  Параметры, которые необходимо указать в полях раскрывающегося списка «Условия сценариев доступа», зависят от выбранных словарей в поле «Словари RADIUS» и от типа аутентификации/авторизации.

— блок полей «Аутентификация/авторизация»:

1. Блок полей «Условия сценариев доступа»

- Проводная аутентификация по MAC-адресам (Wired MAB), перевести переключатель в положение «Активен»:
 1. *Radius / NAS-Port-Type = Ethernet*
 2. *Radius / Service-Type = Call-Check*
- Проводная аутентификация по стандарту 802.1X (Wired 802.1X), перевести переключатель в положение «Активен»:
 1. *Radius / NAS-Port-Type = Ethernet*
 2. *Radius / Service-Type = Framed-User*
- Беспроводная аутентификация по стандарту 802.1X (Wireless 802.1X), перевести переключатель в положение «Активен»:
 1. *Radius / NAS-Port-Type = Virtual*
 2. *Cisco-ASA / ASA-ClientType = AnyConnect-Client-SSH-VPN*

2. Блок полей «Проверка узлов по MAC-адресам (MAB)», перевести переключатель в положение «Активен»:

- перевести переключатель «Метод проверки узлов» в положение «Активен» с использованием PAP/ASCII:
 1. *Проверить атрибут Calling-Station-Id на соответствие MAC-адресу.*

< Создание профиля сетевого оборудования

Разрешения

Назначение VLAN

Атрибуты IETF 802.1X Пользовательские атрибуты

Назначение списков доступа (ACL)

Change of Authorization

CoA

Порт CoA

Отправлять Message-Authenticator

ⓘ Хотя бы один из параметров для Отключения или Повторной аутентификации должен быть активен

> Отключение

▼ Повторная аутентификация

Basic ⓘ

Cisco / Cisco-AVPair = subscriber:command=reauthenticate +

Rerun ⓘ

Last ⓘ

Cisco / Cisco-AVPair = subscriber:command=reauthenticate +

Cisco / Cisco-AVPair = subscriber:reauthenticate-type=last +

Перенаправление

Тип

Рисунок 28 – Создание профиля сетевого оборудования. Блоки полей «Разрешения» и «Change of Authorization»

Особенности заполнения полей описаны ниже:

— блок полей «Разрешения»:

- переключатель «Назначение VLAN» перевести в положение «Активен»:
выбрать значение «Атрибут IETF 802.1X».

— блок полей «Change of Authorization»:

- CoA: RADIUS;
- Порт CoA: 1700.

— блок полей «Повторная аутентификация»:

- Basic: Cisco / Cisco-AVPair = subscriber:command=reauthenticate;
- Last:
Cisco / Cisco-AVPair = subscriber:command=reauthenticate
Cisco / Cisco-AVPair = subscriber:reauthenticate-type=last

— поле «Перенаправление»:

- Тип: значение «Не перенаправлять».

2) Создать сетевое оборудование – аутентификатор:

— перейти в раздел «Контроль доступа» → «Сетевое оборудование» → кнопка «**+** Устройство» (рис. 29);

— откроется страница создания сетевого оборудования. Заполнить поля страницы необходимыми параметрами (рис. 30).

Сетевое оборудование **Устройства** Группы

Введите запрос для поиска

Фильтр **+ Устройство**

Название	IP-адрес	Аутентификация	Группы устройств	Профиль оборудования	Последнее изменение
00testcryptopro Описание	10.10.10.13	RADIUS	1	CryptoProProfile	31 мая 2024 13:58:27
20240520_123	5.5.5.50	RADIUS	1	20240520	30 мая 2024 15:02:38
20240520_1 test	5.5.5.51	RADIUS	0	20240520	28 мая 2024 13:42:11
20240520_10 test12345	5.5.5.151	RADIUS	0	20240520	31 мая 2024 13:26:42
AZ_1	4.5.6.8	RADIUS	0	111111test	21 марта 2024 10:33:22
AZ_33	2.2.3.232	RADIUS	0	111111test	21 марта 2024 11:25:53
aztest111	12.12.12.44	RADIUS	0	1	11 июня 2024 10:50:59

Всего: 44

Рисунок 29 – Подраздел «Сетевое оборудование»

< Создание устройства

Свойства Группы

Название

Описание

IP-адрес

Профиль сетевого оборудования

Аутентификация

ⓘ Должен быть выбран хотя бы один протокол

RADIUS

Секретный ключ

Изменение авторизации (CoA) ⓘ

TACACS+

Рисунок 30 – Создание сетевого оборудования

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «IP-адрес»: IP-адрес аутентификатора;
- поле «Профиль сетевого оборудования»: созданный ранее;
- поле «RADIUS»: активен;
- поле «Секретный ключ»: секретный ключ, указанный в настройках подключения аутентификатора к серверу RADIUS.

А.7 Настройка профилей авторизации и политики доступа в сеть

Последовательность действий для настройки профилей авторизации и политики доступа в сеть:

- 1) Создать профиль авторизации доступа в сеть для устройства со статусом соответствия требованиям политики безопасности «Не соответствует» (Non-Compliant):
 - перейти в раздел «Контроль доступа» → «Профили авторизации» → вкладка «Доступ в сеть» → кнопка «**+** Профиль» (рис. 31);
 - откроется страница создания профиля авторизации. Заполнить поля требуемыми параметрами для авторизации устройства со статусом «Не соответствует» (Non-Compliant) (рис. 32).

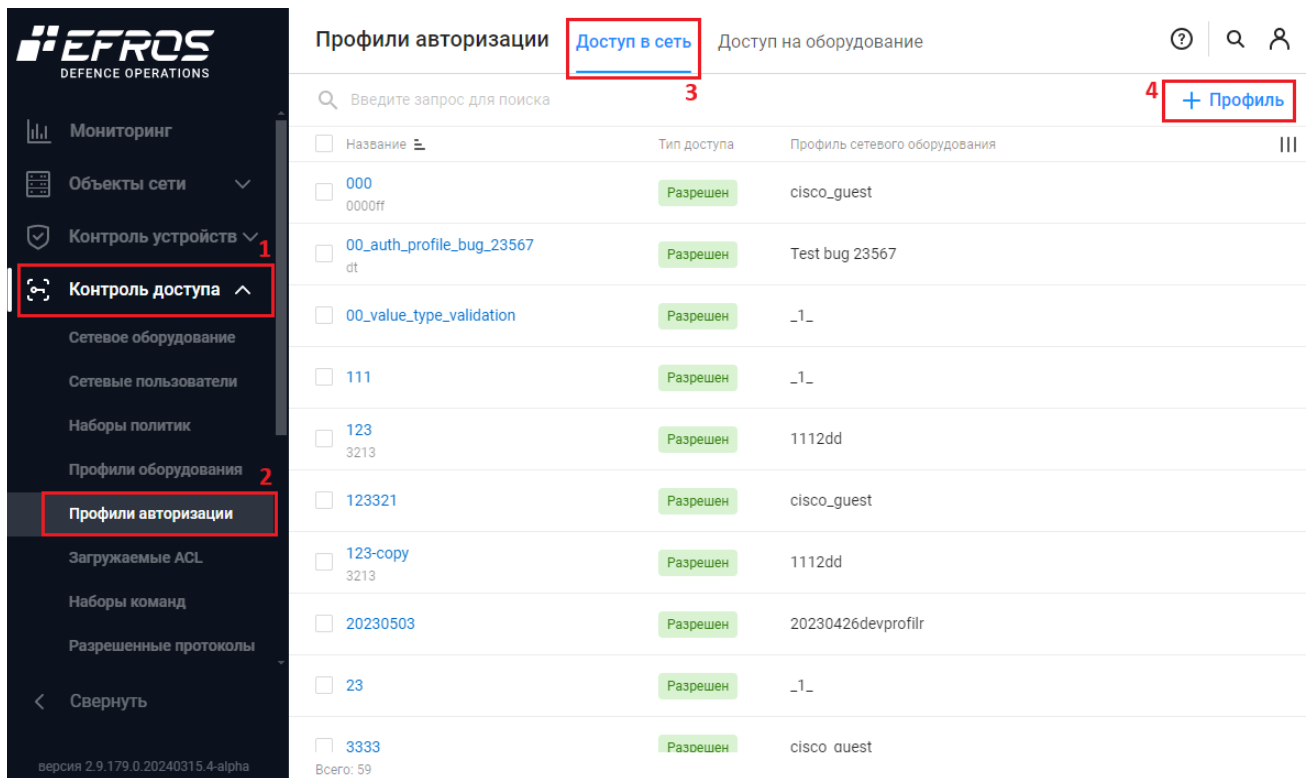


Рисунок 31 – Подраздел «Профили авторизации»

← **Создание профиля авторизации доступа в сеть**

Название: NonCompliantDevicesAuthorisation

Описание: Описание

Тип доступа: **Разрешен** | Запрещен

Профиль сетевого оборудования: _1_

Основные настройки

ACL:

Веб-переадресация:

VLAN:

Название VLAN: 414

Создать | Отменить

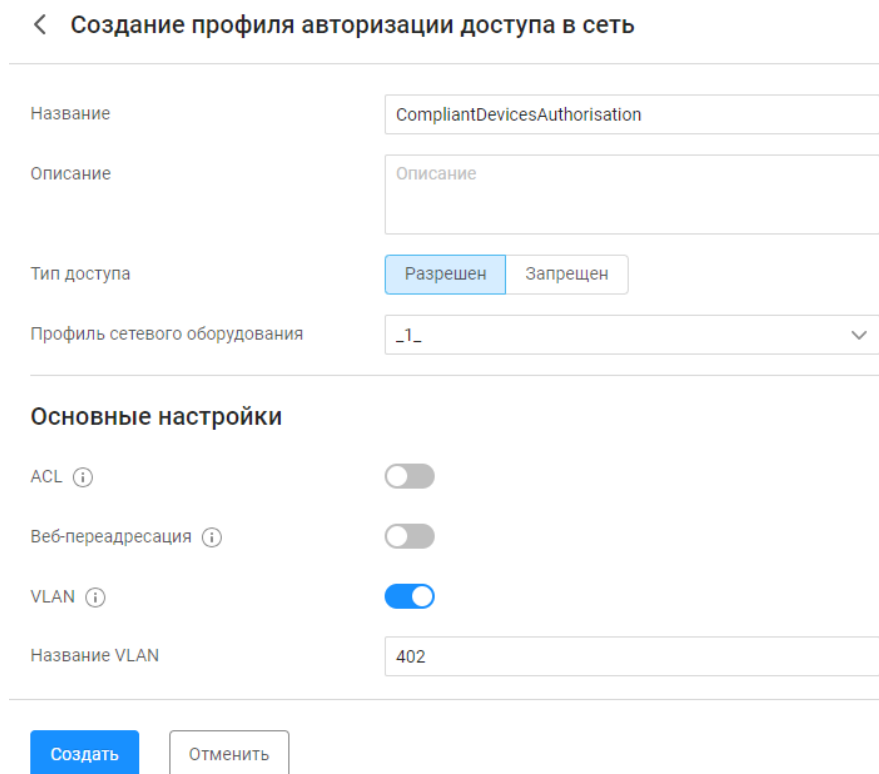
Рисунок 32 – Создание профиля авторизации доступа в сеть устройства со статусом «Не соответствует»

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Тип доступа»: разрешен;
- поле «Профиль сетевого оборудования»: созданный ранее;
- поле «VLAN», перевести переключатель в положение «Активен»:
 - поле «Название VLAN»: указать название VLAN для доступа к сети пользователя со статусом «Не соответствует».

2) Создать профиль авторизации доступа в сеть, назначаемый после успешной авторизации пользователя, назначаемый после успешной авторизации устройства со статусом соответствия требованиям политики безопасности «Соответствует» (Compliant):

- перейти в раздел «Контроль доступа» → «Профили авторизации» → вкладка «Доступ в сеть» → кнопка «+ Профиль» (см. рис. 31);
- откроется страница создания профиля авторизации. Заполнить поля требуемыми параметрами для авторизации устройства со статусом «Соответствует» (Compliant) (рис. 33).



Создание профиля авторизации доступа в сеть

Название: CompliantDevicesAuthorisation

Описание: Описание

Тип доступа: Разрешен / Запрещен

Профиль сетевого оборудования: _1_

Основные настройки

ACL:

Веб-перенадресация:

VLAN:

Название VLAN: 402

Создать / Отменить

Рисунок 33 – Создание профиля авторизации доступа в сеть устройства со статусом «Соответствует»

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Тип доступа»: разрешен;

- поле «Профиль сетевого оборудования»: созданный ранее;
- поле «VLAN», перевести переключатель в положение «Активен»:
 - поле «Название VLAN»: указать название VLAN для доступа к сети пользователя со статусом «Соответствует».

3) Создать шаблоны условий:

- перейти в раздел «Контроль доступа» → «Наборы политик» → вкладка «Шаблоны условий» → кнопка «+ Шаблон» → «Доступ в сеть» (рис. 34);
- откроется страница создания шаблона условий. Заполнить поля необходимыми параметрами для последующего применения как часть правил создаваемых политик (рис. 35).

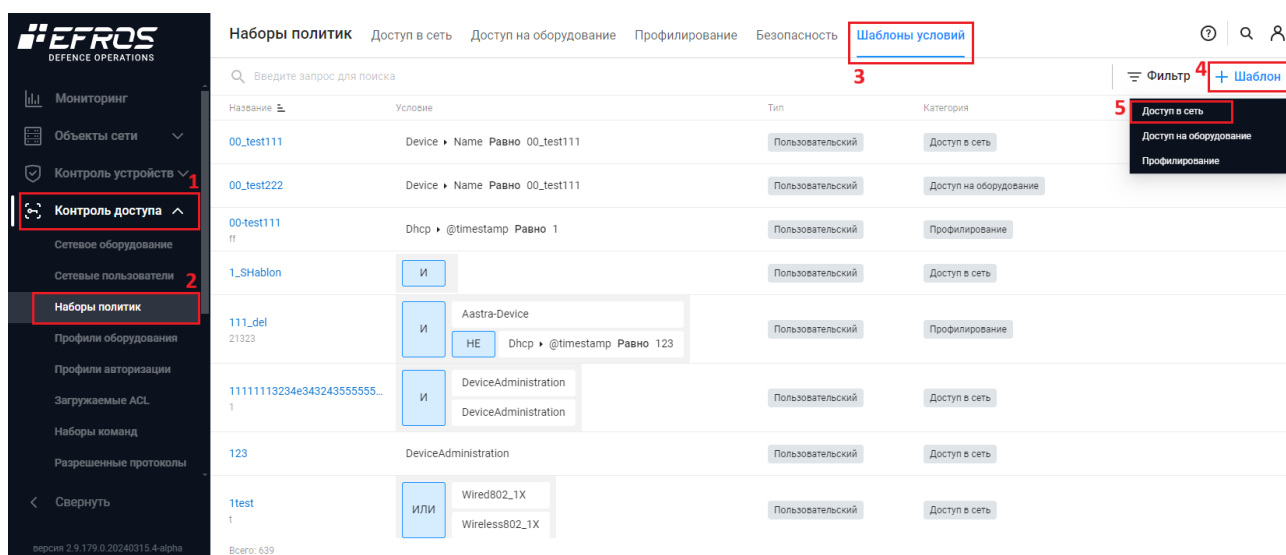


Рисунок 34 – Подраздел «Наборы политик», вкладка «Шаблоны условий»

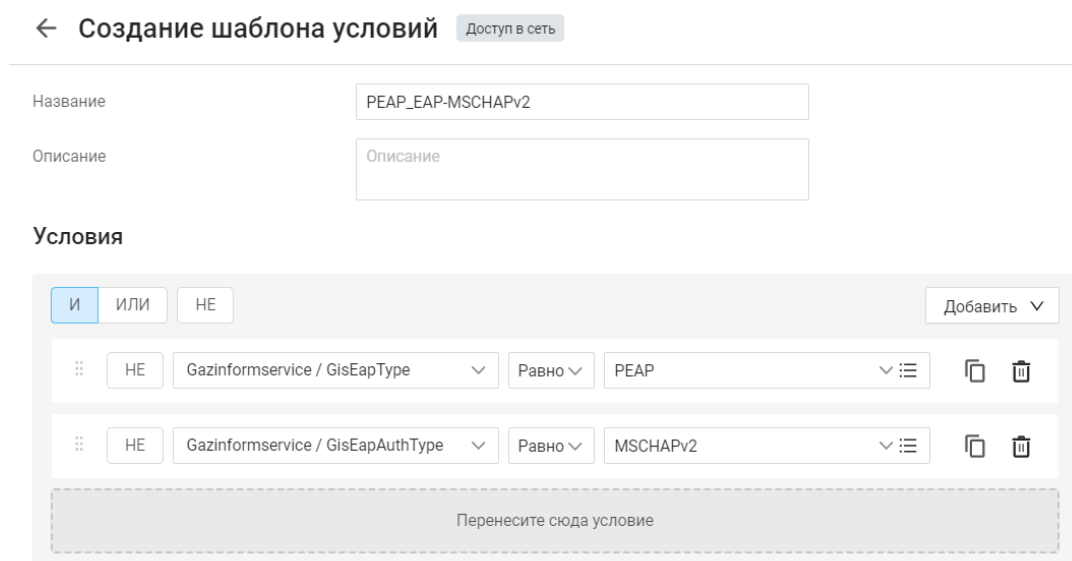


Рисунок 35 – Создание шаблона условий

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- блок полей «Условия»:
 - Gazinformservice / GisEapType Равно PEAP;
 - Gazinformservice / GisEapAuthType Равно MSCHAPv2.

i Значения в поле «Атрибут» зависят от набора словарей в разделе «Словари». Gazinformservice – вспомогательный словарь. Содержит перечень атрибутов, которые можно использовать для настройки правил доступа. Атрибуты, используемые в примере:

- GisEapType – тип EAP (протокол PEAP);
- GisEapAuthType – тип аутентификации EAP (протокол MSCHAPv2).

i Созданный шаблон будет добавлен в набор условий, и его можно использовать как при настройке правил аутентификации

4) Настроить источник данных Active Directory:

- перейти в раздел «Настройки» → «Источники данных» → «Active Directory» → кнопка «**+ Соединение**» (рис. 36);
- откроется страница создания AD соединения. Заполнить поля необходимыми параметрами для настройки параметров работы функционального модуля «Efros NAC» с контроллером домена, в котором хранятся учетные записи сетевых устройств (рис. 37).

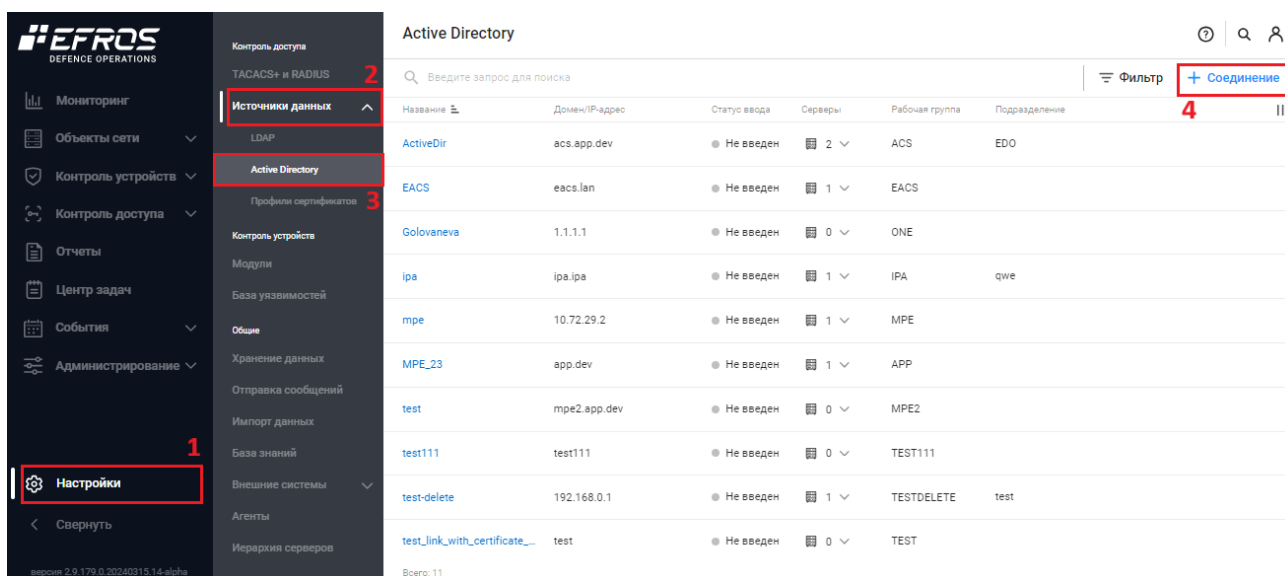





Рисунок 36 – Вкладка «Active Directory»


< Создание Active Directory соединения

Название	<input type="text" value="AD_name"/>
Домен / IP-адрес	<input type="text" value="10.72.29.36"/>
Подразделение (OU)	<input type="text" value="Название подразделения"/>
Серверы аутентификации	<input type="text" value="IP-адрес или DNS имя сервера"/> 
Альтернативное имя группы Имя рабочей группы (NetBIOS)	<input type="checkbox"/>

Ввод в домен

 Для активации ввода в домен необходимо заполнить «Название» и «Домен / IP-адрес», а после нажать кнопку «Создать»

Логин	<input type="text"/>
Пароль	<input type="password"/> 
<input type="button" value="Ввести в домен"/>	


 Для активации выбора "Группы домена" необходимо ввести в домен

Группы домена	<input type="text"/>
---------------	----------------------


Рисунок 37 – Создание AD соединения

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Домен / IP-адрес»: имя или IP-адреса домена, к которому подключается сервер ПК «Efros DO».

 Созданное соединение AD можно использовать как источник данных при настройке правил аутентификации.

5) Создать политику доступа в сеть:

- перейти в раздел «Контроль доступа» → «Наборы политик» → вкладка «Доступ в сеть» → кнопка « Политика» (рис. 38);
- откроется страница создания политики доступа в сеть. Заполнить поля необходимыми параметрами для настройки условий срабатывания политики (рис. 39).

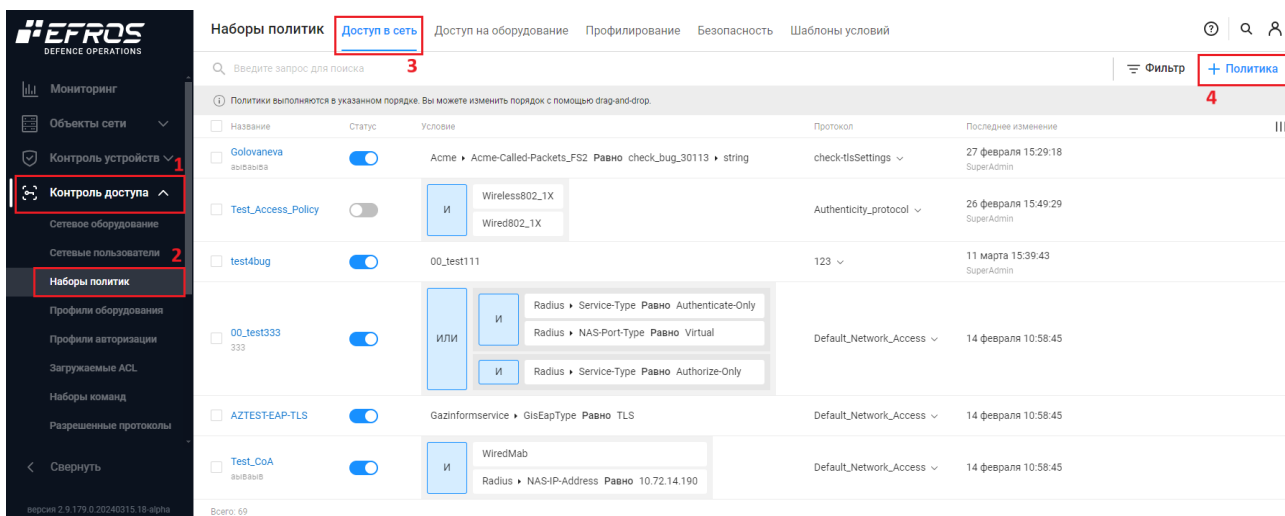


Рисунок 38 – Подраздел «Наборы политик», вкладка «Доступ в сеть»

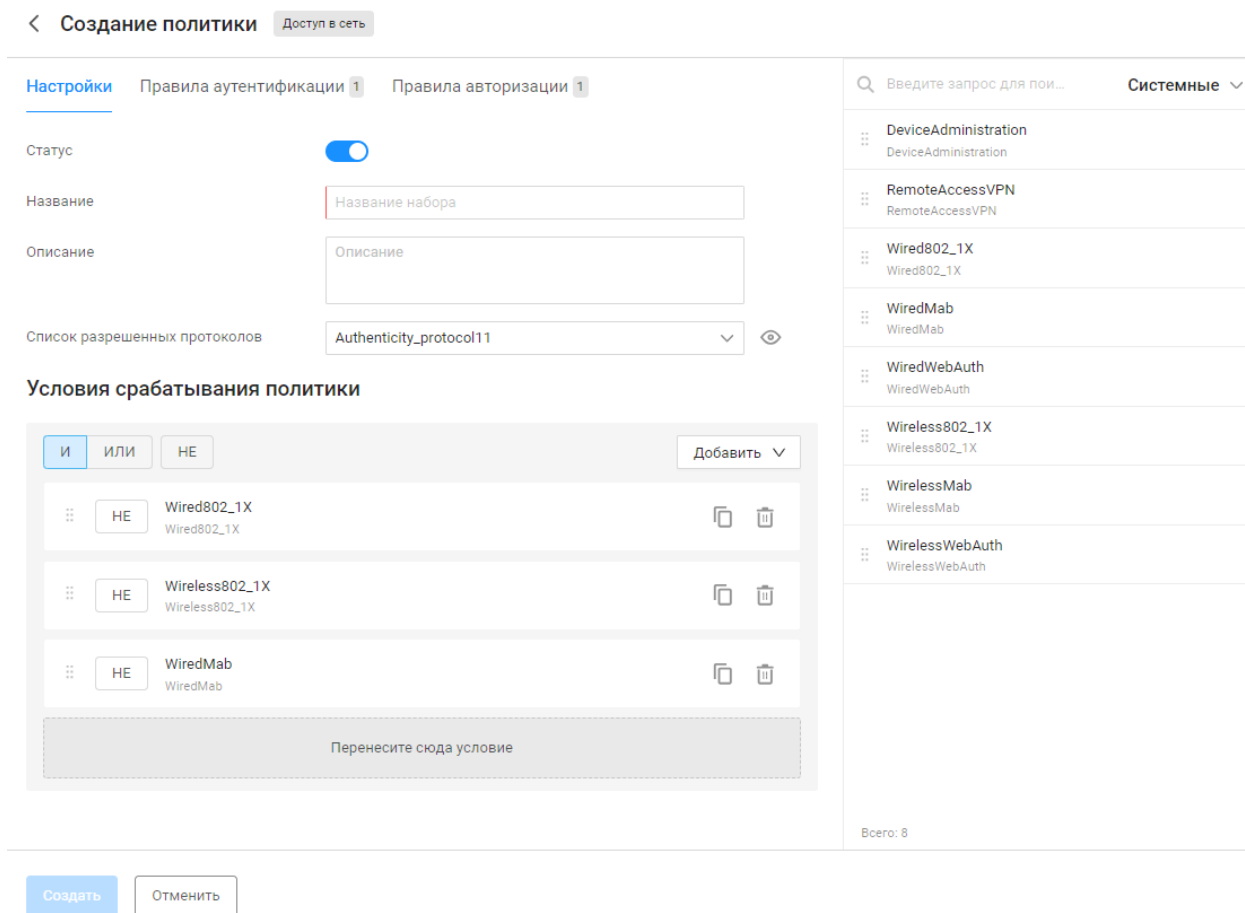


Рисунок 39 – Создание политики доступа в сеть

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Список разрешенных протоколов»: созданный ранее;

— поле «Условия срабатывания политик»: Wired 802.1X; Wireless 802.1X; Wired MAB (из шаблонов условий).

i Шаблон условий «Wired 802.1X» – это набор условий для аутентификации устройств, подключенных к проводной сети по стандарту 802.1X.

Шаблон условий «Wireless 802.1X» – это набор условий для аутентификации устройств, подключенных к беспроводной сети по стандарту 802.1X.

Шаблон условий «Wired MAB» – это набор условий для аутентификации устройств, подключенных к проводной сети по MAC-адресам.

В наборе правил «Условия срабатывания политики» используются атрибуты и значения, заданные в профиле оборудования. В зависимости от того, какое сетевое оборудование будет запрашивать доступ, для подключаемого устройства – могут быть использованы разные значения из профиля оборудования.

В данном случае применены условия, заданные в профиле сетевого оборудования → «Аутентификация / Авторизация» → «Условия сценариев доступа» (см. п. 1).

6) Настроить правила аутентификации:

- на странице созданной политики доступа в сеть перейти на вкладку «Правила аутентификации» (см. рис. 39);
- нажать кнопку «**+** [Правило аутентификации](#)». Создаваемое правило аутентификации предназначено для настройки способов аутентификации устройства;
- откроется страница создания правила аутентификации. Заполнить поля необходимыми параметрами (рис. 40).

← Создание правила аутентификации Доступ в сеть

Статус

Название

Проверка учетных данных

Источник данных

При ошибке аутентификации

Пользователь не найден

Условия срабатывания правила

И ИЛИ НЕ

- НЕ PEAP_EAP-MSCHAPv2
- НЕ TTLS_EAP-MSCHAPv2
- НЕ TTLS_MSCHAPv2

Перенесите сюда условие

Создать

Введите запрос для поиска Все шаблоны условий

- _suppl_fiction2
- test123
- testcond1
- TTLS_EAP-MSCHAPv2
- TTLS_MSCHAPv2
- Wired802_1X
- WiredMab
- WiredWebAuth
- Wireless802_1X
- WirelessMab
- WirelessWebAuth

Всего: 29

Рисунок 40 – Создание правила аутентификации

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Источник данных»: (DOMAIN)_{источник данных AD}, созданный ранее;
- поле «При ошибке аутентификации»: отклонить;
- поле «Пользователь не найден»: отклонить;
- блок полей «Условия срабатывания правила»:
 - логический оператор: «ИЛИ»;
 - PEAP_EAP-MSCHAPv2 (из шаблонов условий);
 - TTLS_EAP-MSCHAPv2 (из шаблонов условий);
 - TTLS_MSCHAPv2 (из шаблонов условий).

i Пользовательские шаблоны условий для использования требуемых протоколов созданы в п. 3.

Для запрета доступа в сеть пользователей, не соответствующих ранее созданным правилам аутентификации, необходимо в строке правила по умолчанию «Default» указать источник данных «DenyAccess» (рис. 41).

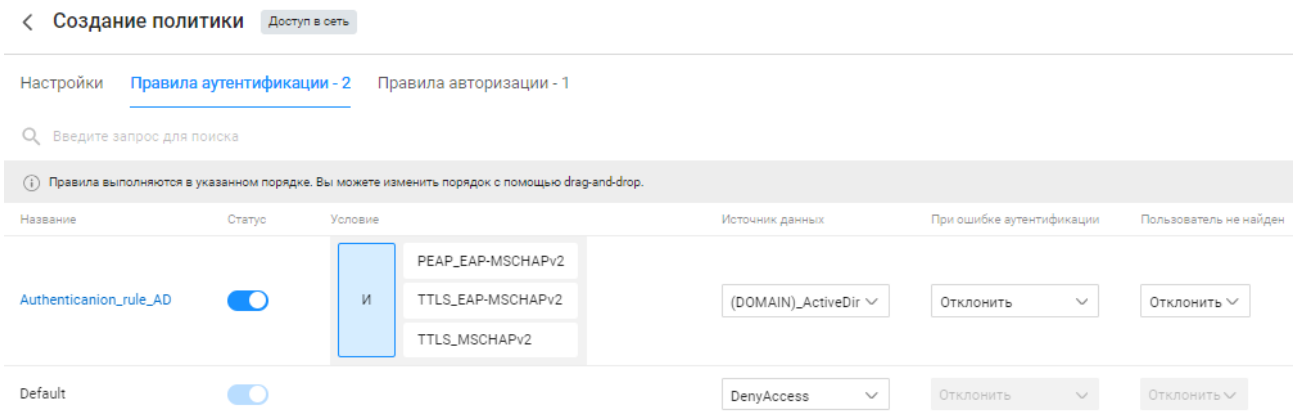


Рисунок 41 – Редактирование правила аутентификации «Default»

7) Настроить правила авторизации:

- на странице созданной политики доступа в сеть перейти на вкладку «Правила авторизации» (см. рис. 39);
- нажать кнопку «**+ Правило авторизации**». Создаваемое правило авторизации предназначено для настройки доступа к сети устройств с разными статусами соответствия требованиям политики безопасности. Заполнить поля необходимыми параметрами для статуса «Не соответствует» (Non-Compliant) и «Не определено» (Interminate) (рис. 42);
- аналогично создать правило авторизации для статуса «Соответствует».

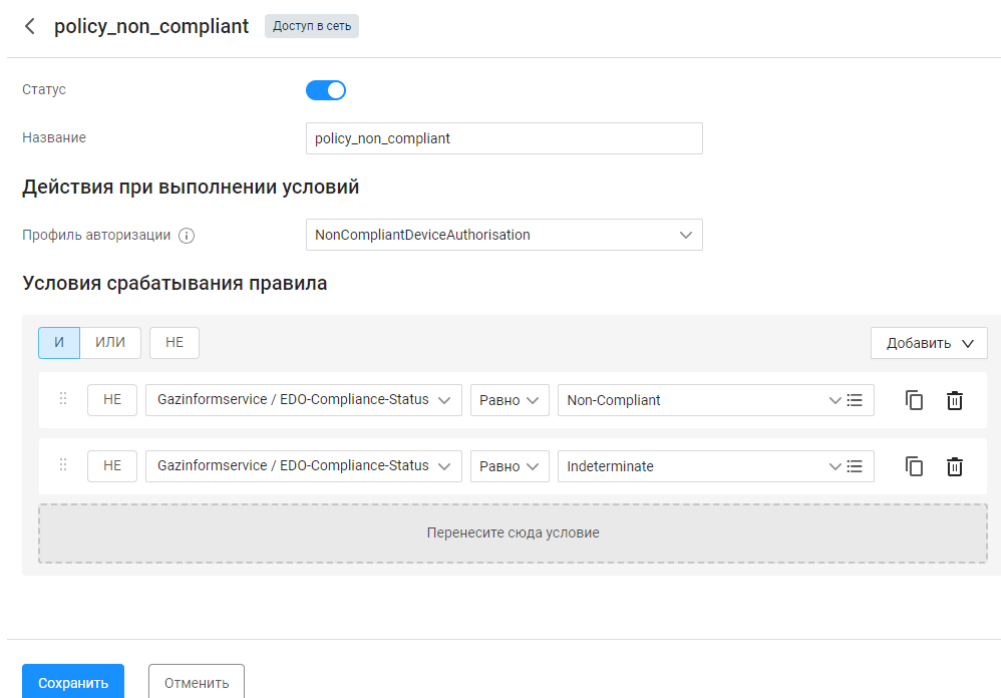


Рисунок 42 – Создание правила авторизации

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Профиль авторизации»: созданный ранее;
- варианты заполнения поля «Условия срабатывания правила»:
 - Gazinformservice / EDO-Compliance-Status Равно Non-Compliant;
 - Gazinformservice / EDO-Compliance-Status Равно Indeterminate;
 - Gazinformservice / EDO-Compliance-Status Равно Compliant.

Устройства, не соответствующие ранее созданным правилам авторизации, должны переадресовываться для аутентификации. Для этого необходимо в строке правила по умолчанию «Default» указать профиль авторизации «DefaultAuthorizationProfile» (рис. 43).

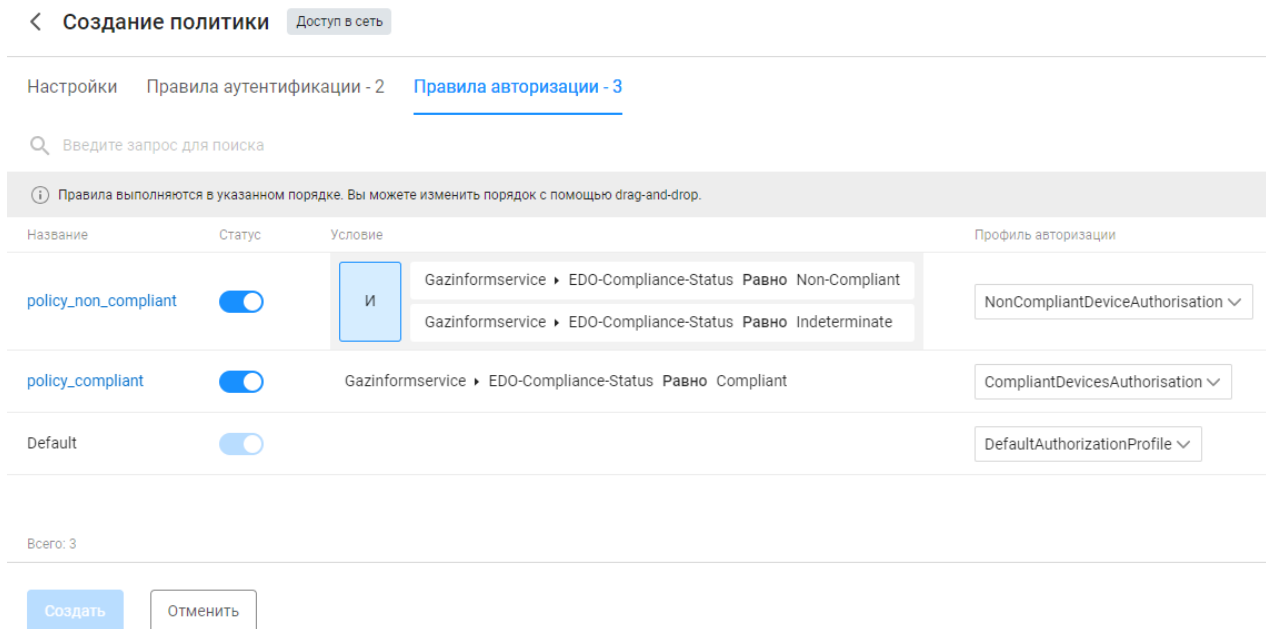


Рисунок 43 – Редактирование правила авторизации «Default» для переадресации пользователей для аутентификации

! Если создано несколько политик доступа, а внутри несколько правил аутентификации/авторизации, то при запросе подключения проверка по условиям срабатывания будет осуществляться по списку политик в указанном порядке (сверху вниз).

Приложение Б

Рекомендуемая последовательность действий для настройки разграничения доступа к сети с использованием агента и встроенного суппликанта

- ❗ В начале необходимо убедиться, что на устройстве пользователя установлен агент ПК «Efros DO».
- ❗ В приложении Б приведен пример заполнения минимально необходимых полей для подключения устройства к корпоративной сети с помощью агента и встроенного суппликанта с использованием протокола TEAP для настройки запроса одновременной аутентификации устройства и пользователя.

Б.1 Настройка суппликанта, встроенного в ОС Windows

- ❗ Настройки встроенного суппликанта необходимо производить с правами администратора.

Последовательность действий для настройки на встроенном суппликанте запроса одновременной аутентификации устройства и пользователя с использованием протокола TEAP:

- 1) На конечном устройстве с ОС Windows зайти в папку «Control Panel» → «All Control Panel Items» → «Network Connections» (рис. 44).

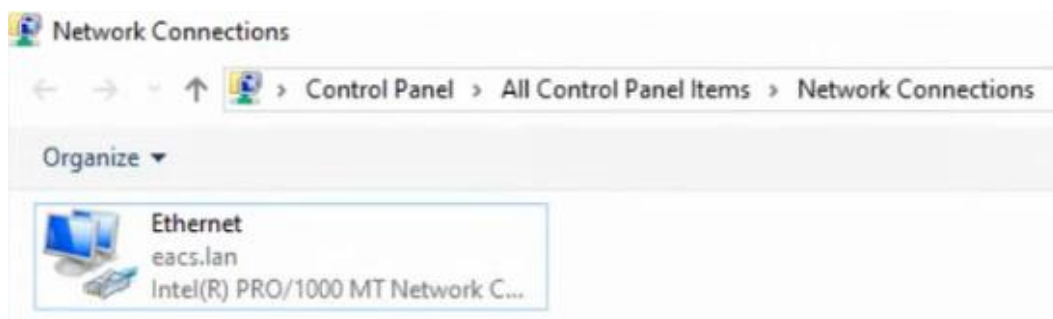


Рисунок 44 – Папка «Network Connections»

- 2) Нажать правой кнопкой на ярлык «Ethernet» и выбрать «Properties». Откроется окно «Ethernet Properties», в котором необходимо перейти на вкладку «Authentication». Далее заполнить поля требуемыми параметрами и нажать кнопку «ОК» (рис. 45).



Рисунок 45 – Окно «Ethernet Properties»

Заполнение полей описаны ниже:

- поле «Enable IEEE 802.X authentication»: установить флаг;
- поле «Choose a network authentication method»: Microsoft: EAP-TEAP.

- 3) В окне «Ethernet Properties» нажать на кнопку «Additional settings». Откроется соответствующее окно. Далее заполнить поля требуемыми параметрами и нажать кнопку «ОК» (рис. 46).

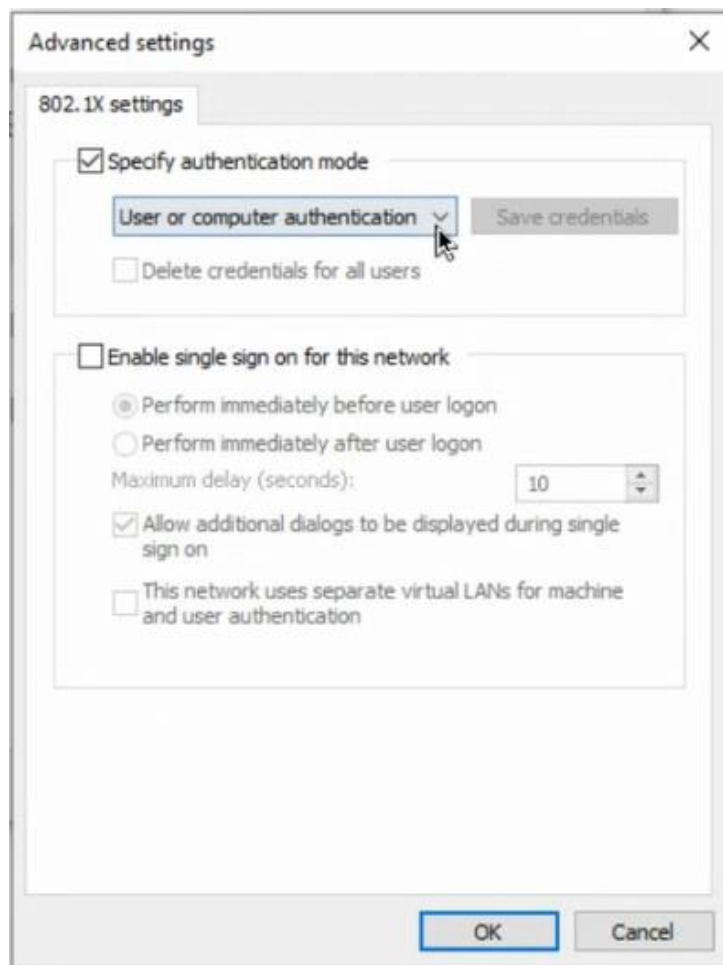


Рисунок 46 – Окно «Advanced settings»

Заполнение полей вкладки «802.X1 settings» описаны ниже:

- поле «Specify authentication mode»: установить флаг;
- раскрывающийся список: User or computer authentication.

- 4) В окне «Ethernet Properties» на вкладке «Authentication» нажать кнопку «Settings». Откроется окно «TEAP Properties». Необходимо заполнить поля требуемыми параметрами и нажать кнопку «ОК» (рис. 47).

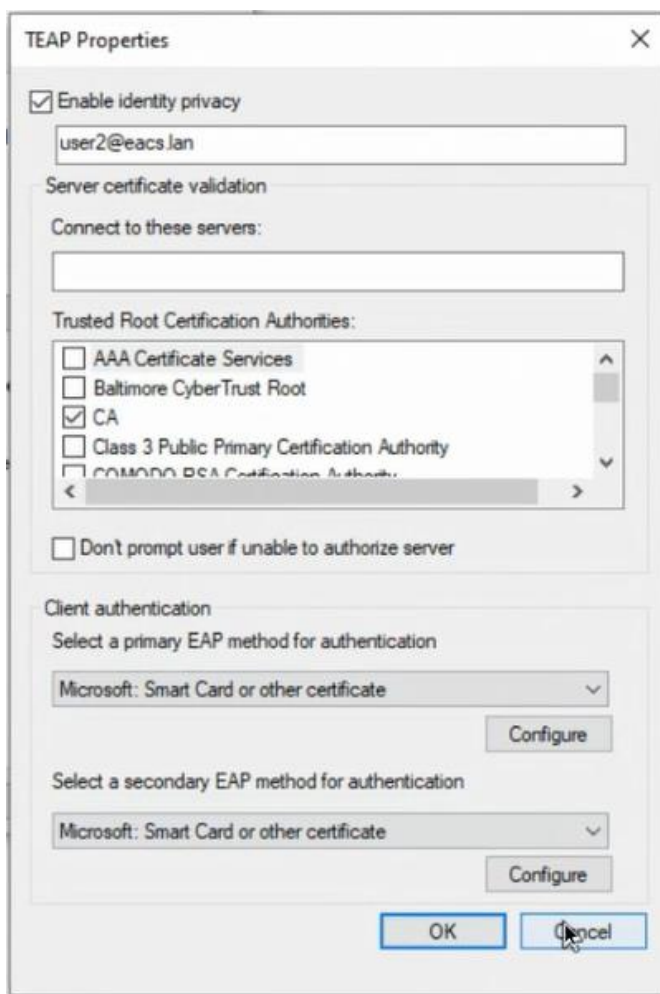


Рисунок 47 – Окно «Ethernet Properties»

Заполнение полей в области «Client authentication» описаны ниже:

- поле «Select a primary EAP method for authentication»: Microsoft: Smart Card or other certificate;
- поле «Select a secondary EAP method for authentication»: Microsoft: Smart Card or other certificate.

5) Для подключения к сети необходимо в папке «Network Connections» нажать правой кнопкой на ярлык «Ethernet» и выбрать «Enable» (см. рис. 44). Для отключения от сети необходимо использовать значение «Disable».



При первом подключении к сети (после включения конечного устройства) производится запрос аутентификации только устройства. Аутентификация пользователя не выполняется. При появлении ошибки подключения необходимо переподключиться к сети. После будет производиться одновременная аутентификация устройства и пользователя.

События аутентификации можно посмотреть в веб-интерфейсе ПК «Efros DO», раздел «События» → «Доступ в сеть» → вкладка «Аутентификация».

Б.2 Настройка разрешенных протоколов (TEAP)

Последовательность действий для настройки разрешенных протоколов:

1) Создать настройки TLS:

- перейти в раздел «Контроль доступа» → «Разрешенные протоколы» → вкладка «Настройки TLS» → кнопка «+ Настройки TLS»;
- откроется страница создания настройки TLS. Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Пример созданной настройки TLS приведен на рис. 48.

< Efros_MIKROT

Название	<input type="text" value="Efros_MIKROT"/>
Системный сертификат	<input type="text" value="Efros"/> ▾
Доверенный сертификат	<input type="text" value="Выбрано: 2"/> × ▾
Минимальная версия TLS	<input type="text" value="TLS 1.0"/> ▾
Максимальная версия TLS	<input type="text" value="TLS 1.2"/> ▾
Кэширование	<input type="checkbox"/>
Проверять список отзыва сертификатов	<input type="checkbox"/>
OCSP	<input type="checkbox"/>

Рисунок 48 – Создание настройки TLS

Особенности заполнения полей страницы создания настроек TLS описаны ниже:

- поле «Название»: любое;
- поле «Системный сертификат»: выбрать предустановленный сертификат из списка;
- поле «Доверенный сертификат»: выбрать сертификат из списка;
- поле «Минимальная версия TLS»: TLS 1.0;
- поле «Максимальная версия TLS»: TLS 1.2.

i Доверенный сертификат можно использовать предустановленный, либо добавить свой в разделе «Администрирование» → «Сертификаты» → вкладка «Доверенные».

2) Включить и настроить протокол «TEAP»:

- перейти в раздел «Контроль доступа» → «Разрешенные протоколы» → вкладка «Доступ в сеть» → кнопка «[+ Список протоколов](#)»;
- откроется страница создания списка разрешенных протоколов. Заполнить поля требуемыми параметрами для активации возможности использования протокола TEAP. Пример заполненных полей приведен на рис. 49.

< My_Protocols Доступ в сеть

Название	My_Protocols
Описание	Описание
Тип EAP по умолчанию i	TEAP ▼
Время ответа на EAP пакет	60 секунд
Максимально открытых сессий	16 384

EAP-MD5

EAP-FAST

EAP-TLS

EAP-TTLS

PEAP

TEAP **i**

Настройки TLS	Efros_MIKROT ▼ 👁
Метод по умолчанию	EAP-MSCHAPv2 ▼
Идентификатор сервера i	Efros Defence Operation
Срок действия PAC	1 неделя ▼

EAP-MSCHAPv2

EAP-TLS

Настройки TLS	Efros_MIKROT ▼ 👁
---------------	--

Сохранить Отменить

Рисунок 49 – Создание списка разрешенных протоколов доступа в сеть

Б.3 Настройка профилей авторизации и политики доступа в сеть

1) Создать профиль авторизации для пользователя:

- перейти в раздел «Контроль доступа» → «Профили авторизации» → вкладка «Доступ в сеть» → кнопка «**+ Профиль**»;
- откроется страница создания профиля авторизации. Заполнить поля страницы необходимыми параметрами. Пример созданного профиля авторизации для пользователя приведен на рис. 50.

< USER_ACCESS

Название	<input type="text" value="USER_ACCESS"/>
Описание	<input type="text" value="Описание"/>
Тип доступа	<input checked="" type="radio"/> Разрешен <input type="radio"/> Запрещен
Профиль сетевого оборудования	<input type="text" value="Cisco_dot1x_MAB"/>

Основные настройки

Загружаемый ACL ⓘ	<input type="checkbox"/>
ACL ⓘ	<input type="checkbox"/>
ACL контроллера точек доступа ⓘ	<input type="checkbox"/>
Веб-переадресация ⓘ	<input type="checkbox"/>
VLAN ⓘ	<input type="checkbox"/>

Настройка дополнительных атрибутов

<input type="text" value="Атрибут"/>	=	<input type="text" value="Значение"/>	+
--------------------------------------	---	---------------------------------------	---

Передаваемые параметры

Рисунок 50 – Пример созданного профиля авторизации для пользователя

2) Создать профиль авторизации для устройства:

- перейти в раздел «Контроль доступа» → «Профили авторизации» → вкладка «Доступ в сеть» → кнопка «**+ Профиль**»;

- откроется страница создания профиля авторизации. Заполнить поля страницы необходимыми параметрами. Пример созданного профиля авторизации для устройства приведен на рис. 51.

< MACHINE_ACCESS

Название

Описание

Тип доступа Разрешен Запрещен

Профиль сетевого оборудования

Основные настройки

Загружаемый ACL

ACL

ACL контроллера точек доступа

Веб-переадресация

VLAN

Настройка дополнительных атрибутов

= +

Передаваемые параметры

Рисунок 51 – Пример созданного профиля авторизации для устройства

- 3) Настроить источник данных Active Directory:
 - перейти в раздел «Настройки» → «Источники данных» → «Active Directory» → кнопка «**+ Соединение**»;
 - откроется страница создания AD соединения. Заполнить поля необходимыми параметрами для настройки параметров работы функционального модуля «Efros NAC» с контроллером домена, в котором хранятся учетные записи. Пример созданного AD соединения приведен на рис. 52.

< eacs

Название	<input type="text" value="eacs"/>
Домен / IP-адрес	<input type="text" value="eacs.lan"/>
Подразделение (OU)	<input type="text"/>
Серверы аутентификации	<input type="text" value="10.72.29.131"/> +
Альтернативное имя группы Имя рабочей группы (NetBIOS)	<input type="checkbox"/>

Ввод в домен ● Введен

Логин	<input type="text" value="eacs\Администратор"/>
Пароль	<input type="password" value="Пароль"/>
	<input type="button" value="Вывести из домена"/>

Группы домена **6 групп**

Рисунок 52 – Созданное AD соединение

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Домен / IP-адрес»: имя или IP-адреса домена, к которому подключается сервер ПК «Efros DO»;
- поле «Группы домена»: выбрать группы пользователей домена.

Соединенное AD можно использовать как источник данных при настройке правил аутентификации.

Соединенное AD соединение можно использовать как источник данных при настройке правил аутентификации.

Выбранную группу домена можно использовать при настройке правил авторизации.

4) Настроить источник данных «Профили сертификатов»:

- перейти в раздел «Настройки» → «Источники данных» → «Профили сертификатов» → кнопка «**+** Профиль сертификатов »;
- откроется страница создания профиля сертификата. Заполнить поля

необходимыми параметрами для настройки параметров профиля сертификата. Пример созданного профиля сертификата приведен на рис. 53.

< UPN

Название

Описание

Основные настройки

Источник данных ⓘ

▼

Атрибут сертификата ⓘ ▼

Рисунок 53 – Созданный профиль сертификата

ⓘ Созданный профиль сертификатов можно использовать как источник данных при настройке правил аутентификации.

- 5) Создать политику доступа в сеть:
- перейти в раздел «Контроль доступа» → «Наборы политик» → вкладка «Доступ в сеть» → кнопка « + Политика »;
 - откроется страница создания политики доступа в сеть. Заполнить поля страницы необходимыми параметрами. Пример созданных основных правил политики доступа в сеть приведены на рис. 54.

< TEAP Доступ в сеть

Настройки Правила аутентификации 2 Правила авторизации 3

Статус

Название TEAP

Описание

Список разрешенных протоколов My_Protocols

Условия срабатывания политики

И ИЛИ НЕ Добавить

НЕ Radius / NAS-IP-Address Равно 10.72.29.155

НЕ Wired802_1X

Перенесите сюда условие

Введите запрос ... Все шаблоны условий

123

Condition_227668

DeviceAdministration

RemoteAccessVPN

test_NetworkTemplateCondition

Wired802_1X

WiredMab

WiredWebAuth

Wireless802_1X

WirelessMab

WirelessWebAuth

Всего: 11

Сохранить Отменить

Рисунок 54 – Пример созданного основного правила политики

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Список разрешенных протоколов»: созданный ранее;
- в поле «Условия срабатывания политики», установить логический оператор «ИЛИ»:
 - Radius / NAS-IP-address Равно {IP-адрес аутентификатора};
 - Wired 802.1X (из шаблонов условий).

i Шаблон условий «Wired 802.1X» – это набор условий для аутентификации устройств, подключенных к проводной сети по стандарту 802.1X.

В наборе правил «Условия срабатывания политики» используются атрибуты и значения, заданные в профиле оборудования. В зависимости от того, какое сетевое оборудование будет запрашивать доступ, для подключаемого устройства – могут быть использованы разные значения из профиля оборудования.

6) Настроить правила аутентификации:

- на странице созданной политики доступа в сеть перейти на вкладку «Правила аутентификации»;

- нажать кнопку « [+ Правило аутентификации](#) ». Откроется страница создания правила аутентификации. Заполнить поля страницы необходимыми параметрами. Пример созданных правил аутентификации приведен на рис. 55.

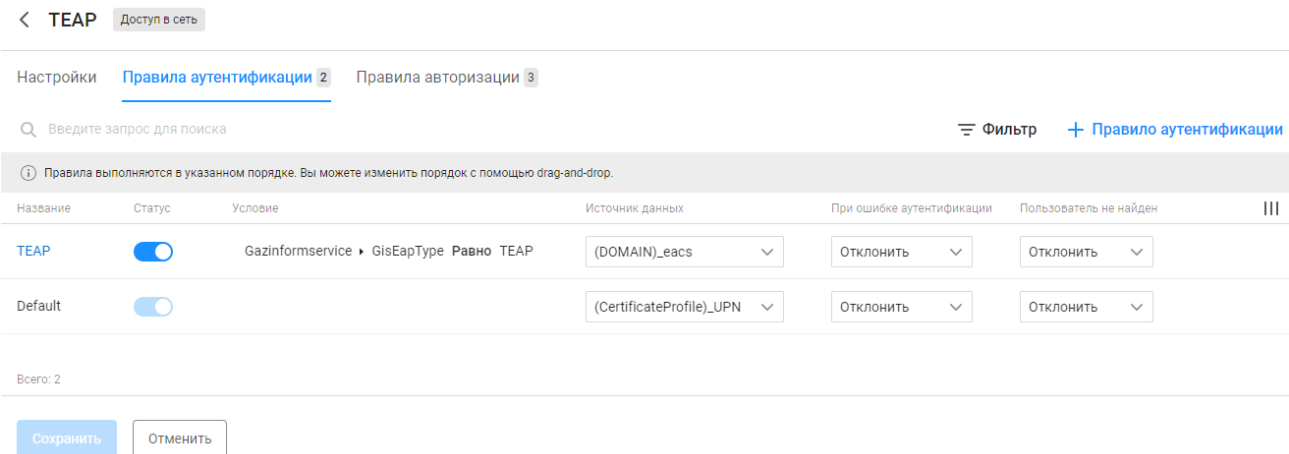


Рисунок 55 – Пример созданных правил аутентификации

Особенности заполнения полей созданного правила аутентификации описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Источник данных»: соединение Active Directory созданный ранее;
- в поле «Условия срабатывания правила»:
 - Gazinformservice / GisEapType Равно TEAP.

Для запрета доступа в сеть устройств, не соответствующих ранее созданным правилам аутентификации, необходимо в строке правила «Default» указать источник данных профиль сертификата созданный ранее.

7) Настроить правила авторизации:

- на странице созданной политики доступа в сеть перейти на вкладку «Правила аутентификации»;
- нажать кнопку « [+ Правило авторизации](#) ». Откроется страница создания правила авторизации. Заполнить поля страницы необходимыми параметрами. Пример созданных правил авторизации приведен на рис. 56.

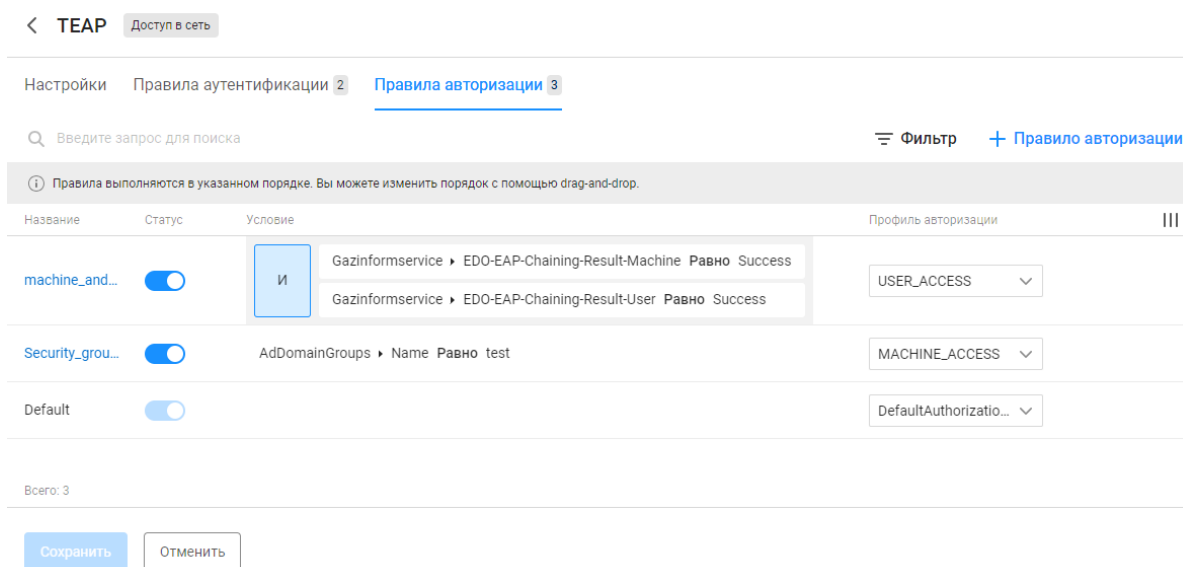


Рисунок 56 – Пример созданных правил авторизации

Особенности заполнения полей первого созданного правила авторизации для проверки успешной авторизации устройства и пользователя описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Профиль авторизации»: созданный ранее;
- в поле «Условия срабатывания правила»:
 - Gazinformservice / EDO-EAP-Chaining-Result-Machine Равно Success;
 - Gazinformservice / EDO-EAP-Chaining-Result-User Равно Success.

Особенности заполнения полей второго созданного правила авторизации для проверки наличия пользователя в группе соединения Active Directory описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Профиль авторизации»: созданный ранее;
- в поле «Условия срабатывания правила»:
 - AdDomainGroups / Name Равно {группа домена в ранее созданном AD соединении}

Устройства, не соответствующие ранее созданным правилам авторизации, должны переадресовываться для аутентификации. Для этого необходимо в строке правила по умолчанию «Default» указать профиль авторизации «DefaultAuthorizationProfile».

- ❗ Если создано несколько политик доступа, а внутри несколько правил аутентификации/авторизации, то при запросе подключения проверка по условиям срабатывания будет осуществляться по списку в указанном порядке (сверху вниз).

Приложение В

Рекомендуемая последовательность действий для настройки разграничения доступа к сети с использованием агента через VPN

- ❗ В начале необходимо убедиться, что все предварительные действия выполнены:
 - на устройстве пользователя установлен агент ПК «Efros DO»;
 - на устройстве пользователя установлен VPN-клиент;
 - настроен VPN-шлюз КриптоПро NGate, в том числе VLAN или ACL, для требуемых вариантов доступа к корпоративной сети;
 - настроены сертификаты VPN-шлюза КриптоПро NGate для применения возможностей изменение авторизации (CoA).

- ❗ В приложении В приведен пример заполнения минимально необходимых полей для настройки разграничения доступа к корпоративной сети с использованием агента ПК «Efros DO» через VPN.

Последовательность действий для настройки разграничения доступа к сети с использованием агента ПК «Efros DO» через VPN:

- 1) Создать политику безопасности (см. подраздел приложения А.3).
- 2) Создать профиль сетевого оборудования для VPN-шлюза:
 - перейти в раздел «Контроль доступа» → «Профили оборудования» → кнопка «+ Профиль»;
 - откроется страница создания профиля сетевого оборудования. Заполнить поля страницы необходимыми параметрами (рис. 57).

< Создание профиля сетевого оборудования

Название

Описание

Производитель

Словари RADIUS

Аутентификация / Авторизация

▼ Условия сценариев доступа

Проводная аутентификация по MAC-адресам (Wired MAB)

Беспроводная аутентификация по MAC-адресам (Wireless MAB)

Проводная аутентификация по стандарту 802.1X (Wired 802.1X)

Беспроводная аутентификация по стандарту 802.1X (Wireless 802.1X)

Управление сетевыми устройствами (Device Administration)

Удаленный доступ (VPN)

= +

> Проверка узлов по MAC-адресам (MAB)

Разрешения

Назначение VLAN

Назначение списков доступа (ACL)

Change of Authorization

📘 Изменение авторизации (CoA) настраивается для каждого сетевого устройства в разделе Контроль доступа/Сетевое оборудование

Перенаправление

Тип

Рисунок 57 – Создание профиля сетевого оборудования

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Производитель»: crypto-pro;
- поле «Словари RADIUS»: Radius.
- блок полей «Аутентификация/авторизация», блок полей «Условия сценариев доступа», для переключателя «Удаленный доступ (VPN)» установить положение «Активен»:
 - Radius / NAS-Port-Type = Virtual

Изменение авторизации (CoA) настраивается для каждого сетевого устройства в

разделе «Контроль доступа» → «Сетевое оборудование».

3) Создать сетевое оборудование – VPN-шлюз:

- перейти в раздел «Контроль доступа» → «Сетевое оборудование» → кнопка «**+** Устройство»;
- откроется страница создания сетевого оборудования. Заполнить поля страницы необходимыми параметрами. Пример создания сетевого оборудования приведен на рис. 58.

< Создание устройства

Свойства Группы

Название	NGATE-FW
Описание	Описание
IP-адрес	10.72.2.33
Профиль сетевого оборудования	NGATE-profile

Аутентификация

i Должен быть выбран хотя бы один протокол


RADIUS	<input checked="" type="checkbox"/>
Секретный ключ
Изменение авторизации (CoA) <i>i</i>	Отсутствует HTTPS
Сервер <i>i</i>	10.73.14.38
Порт	7019
API токен <i>i</i>	eyJlbmMiOiJBMjU2Q0JDLUhTNTYliwiYjpb[OiJBMjU2Q0JDLU
Клиентский сертификат <i>i</i>	certificate1.pfx
Пароль от файла
Корневой сертификат <i>i</i>	certificate2.cer
TACACS+	<input type="checkbox"/>

Создать Отменить


Рисунок 58 – Пример создания сетевого оборудования

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «IP-адрес»: IP-адрес VPN-шлюза;
- поле «Профиль сетевого оборудования»: созданный ранее;
- поле «RADIUS»: активен;
- поле «Секретный ключ»: секретный ключ, указанный в настройках подключения VPN-шлюза к серверу RADIUS;
- поле «Изменение авторизации (CoA)»: HTTPS;
- поле «Сервер»: доменное имя или IP-адрес VPN-сервера, которому отправляется запрос на изменение авторизации пользователя;
- поле «Порт»: по умолчанию 7019, допустимые значения 1-65535;
- поле «API токен»: любые символы в количестве до 4000;


 API токен используется для аутентификации запросов. Как правило, создается администратором оборудования в системе управления NGate. Настройки параметра API токена можно найти в настройках API на оборудовании NGate или запросить у администратора системы. Ознакомиться с подробной информацией об API-токенах NGate можно на сайте производителя КриптоПро.

- поле «Клиентский сертификат»: файл формата .pfx, зашифрованный паролем;
- поле «Пароль от файла»: пароль от файла клиентского сертификата;
- поле «Отпечаток сертификата SHA1»: отображается при добавленном клиентском сертификате;

 Отпечаток сертификата SHA1 клиентского сертификата API сервиса используется для верификации подлинности сертификата TLS. SHA сертификата можно получить через консоль управления NGate, при просмотре сертификата в хранилище текущего пользователя.

- поле «Корневой сертификат»: файл формата .cer, .crt, .der или .pem;
- поле «TACACS+»: неактивен.

4) Создать профиль авторизации для ограниченного доступа в сеть:

- перейти в раздел «Контроль доступа» → «Профили авторизации» → вкладка «Доступ в сеть» → кнопка « Профиль »;
- откроется страница создания профиля авторизации. Заполнить поля страницы необходимыми параметрами. Пример созданного профиля авторизации приведен на рис. 59.

← Ngate-PRF-LA

Название: Ngate-PRF-LA

Описание: Ngate-PRF-LA

Тип доступа: Разрешен | Запрещен

Профиль сетевого оборудования: NGATE-FW-RRF

Основные настройки

Загружаемый ACL

ACL

ACL контроллера точек доступа

Веб-перенадресация

VLAN

Настройка дополнительных атрибутов

Выберите атрибут = LIMITED +

Передаваемые параметры

Показать

Рисунок 59 – Пример созданного профиля авторизации для ограниченного доступа в сеть

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Тип доступа»: разрешен;
- поле «Профиль сетевого оборудования»: созданный ранее;
- поле «Настройка дополнительных атрибутов»: название ACL, указанный в настройках подключения VPN-шлюза, для ограниченного доступа в сеть.

5) Создать профиль авторизации для полного доступа в сеть, назначаемый после успешной авторизации:

- перейти в раздел «Контроль доступа» → «Профили авторизации» → вкладка «Доступ в сеть» → кнопка «**+ Профиль**»;
- откроется страница создания профиля авторизации. Заполнить поля страницы необходимыми параметрами. Пример созданного профиля авторизации приведен на рис. 60.

< Ngate-PRF-FA

Название: Ngate-PRF-FA

Описание: Ngate-PRF-FA

Тип доступа: Разрешен | Запрещен

Профиль сетевого оборудования: NGATE-FW-RRF

Основные настройки

Загружаемый ACL

ACL

ACL контроллера точек доступа

Веб-перенадресация

VLAN

Настройка дополнительных атрибутов

Cisco / Cisco-In-ACL = FULL +

Передаваемые параметры

Показать

Рисунок 60 – Создание профиля авторизации полного доступа в сеть, назначаемый после успешной авторизации

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Описание»: любое;
- поле «Тип доступа»: разрешен;
- поле «Профиль сетевого оборудования»: созданный ранее;
- поле «Настройка дополнительных атрибутов»: название ACL, указанный в настройках подключения VPN-шлюза, для полного доступа в сеть.

6) Создать политику доступа в сеть:

- перейти в раздел «Контроль доступа» → «Наборы политик» → вкладка «Доступ в сеть» → кнопка «**+** Политика»;
- откроется страница создания политики доступа в сеть. Заполнить поля страницы необходимыми параметрами. Пример созданных основных правил политики доступа в сеть приведены на рис. 61.

The screenshot displays the configuration page for a policy named "NGATE-POL". At the top, there are navigation links for "Настройки", "Правила аутентификации - 3", and "Правила авторизации - 8". The "Статус" (Status) is turned on. The "Название" (Name) and "Описание" (Description) fields both contain "NGATE-POL".

The "Условия срабатывания политики" (Policy Trigger Conditions) section is expanded, showing a logical operator "ИЛИ" (OR) selected. It contains three conditions:

- Condition 1: Logical operator "ИЛИ", field "НЕ" (NOT), attribute "Radius / NAS-Port-Type", operator "Равно" (Equal), value "Virtual".
- Condition 2: Logical operator "ИЛИ", field "НЕ", attribute "Radius / Service-Type", operator "Равно", value "Authenticate-Only".
- Condition 3: Logical operator "ИЛИ", field "НЕ", attribute "Radius / Service-Type", operator "Равно", value "Authorize-Only".

Each condition row includes a "Добавить" (Add) button, a copy icon, and a delete icon. Below the conditions are three dashed boxes with the text "Перенесите сюда условие" (Move condition here). At the bottom, there are "Сохранить" (Save) and "Отменить" (Cancel) buttons.

Рисунок 61 – Пример созданного основного правила политики

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- в поле «Условия срабатывания политики», установить логический оператор «ИЛИ»:
 - логический оператор «И»:
Radius / NAS-Port-Type Равно Virtual;
Radius / Service-Type Равно Authenticate-Only;
 - логический оператор «И»:
Radius / Service-Type Равно Authorize-Only;

В наборе правил «Условия срабатывания политики» используются атрибуты и значения, заданные в профиле оборудования. В зависимости от того, какое сетевое оборудование будет запрашивать доступ, для подключаемого устройства – могут быть использованы разные значения из профиля оборудования.

В данном случае применены условия, заданные в профиле сетевого оборудования → «Аутентификация / Авторизация» → «Условия сценариев доступа» см. п. 2.

7) Настроить правила аутентификации:

- на странице созданной политики доступа в сеть перейти на вкладку «Правила аутентификации» (см. рис. 61);
- нажать кнопку « + Правило аутентификации ». Откроется страница создания правила аутентификации. Заполнить поля страницы необходимыми параметрами. Пример созданных правил аутентификации приведен на рис. 62.

Название	Статус	Условие	Источник данных	При ошибке аутентификации	Пользователь не найден
NGATE-AUTH	<input checked="" type="checkbox"/>	Gazinformservice > GisAuthType Равно PAP	AllowAccess	Отклонить	Отклонить
Default	<input checked="" type="checkbox"/>	Gazinformservice > GisAuthType Равно PAP	DenyAccess	Отклонить	Отклонить

Рисунок 62 – Пример созданных правил аутентификации

Для запрета доступа в сеть устройств, не соответствующих ранее созданным правилам аутентификации, необходимо в строке правила «Default» указать источник данных «DenyAccess».

8) Настроить правила авторизации:

- на странице созданной политики доступа в сеть перейти на вкладку «Правила аутентификации» (см. рис. 61);
- нажать кнопку « + Правило авторизации ». Откроется страница создания правила авторизации. Заполнить поля страницы необходимыми параметрами. Пример созданных правил авторизации приведен на рис. 63.

Название	Статус	Условие	Профиль авторизации
Compliant	<input checked="" type="checkbox"/>	Radius > TNC-Status Равно Compliant	Ngate-PRF-FA
Indeterminate	<input checked="" type="checkbox"/>	Radius > TNC-Status Равно Indeterminate	Ngate-PRF-LA
non-compliant	<input checked="" type="checkbox"/>	Radius > TNC-Status Равно Non-Compliant	Ngate-PRF-LA
Default	<input checked="" type="checkbox"/>	Radius > TNC-Status Равно Non-Compliant	DefaultAuthorizationP...

Рисунок 63 – Пример созданных правил авторизации

Устройства, не соответствующие ранее созданным правилам авторизации, должны

переадресовываться для аутентификации. Для этого необходимо в строке правила по умолчанию «Default» указать профиль авторизации «DefaultAuthorizationProfile».

- ❗ Если создано несколько политик доступа, а внутри несколько правил аутентификации/авторизации, то при запросе подключения проверка по условиям срабатывания будет осуществляться по списку в указанном порядке (сверху вниз).

Приложение Г

Рекомендуемая последовательность действий для настройки разграничения доступа к сети с использованием политики профилирования

- ❗ В начале необходимо убедиться, что все предварительные действия выполнены:
 - настроен аутентификатор, в том числе ACL или VLAN, для требуемых вариантов доступа к корпоративной сети;
 - наличие устройства пользователя в разделе «Объекты сети» → «Конечные точки» (подробнее о подразделе «Конечные точки» см. в документе «Руководство пользователя. Часть 1. Администрирование»).

- ❗ В приложении Г приведен пример заполнения минимально необходимых полей для настройки разграничения доступа к корпоративной сети с использованием политики профилирования.

Для настройки разграничения доступа к корпоративной сети с использованием политики профилирования необходимо выполнить следующие действия:

- 1) Создать политику безопасности (аналогично созданию в Приложении А.3).
- 2) Создать профиль сетевого оборудования и само сетевое оборудование (аналогично созданию в Приложении А.6).
- 3) Создать профили авторизации и различных статусов соответствия требований безопасности устройства (аналогично созданию в Приложении А.7).
- 4) Создать политики профилирования (см. в Приложении Г.1).
- 5) Создать политику доступа в сеть. Настроить правила аутентификации и авторизации (см. в Приложении Г.2).

Г.1 Создание политик профилирования

Последовательность действий для создания политик профилирования:

- 1) перейти в раздел «Контроль доступа» → «Наборы политик» → вкладка «Профилирование» → кнопка «**+** Политика» (рис. 64);
- 2) откроется страница создания политики профилирования. Заполнить поля страницы необходимыми параметрами для устройства со статусом соответствия требованиям безопасности «Соответствует» (Compliant), полученный от источника профилирования «EDO-Agent» (рис. 65).
- 3) аналогично создать еще две политики профилирования для устройства со

следующими статусами соответствия требованиям безопасности:

- «Не соответствует» (Non-Compliant);
- «Не определено» (Indeterminate).

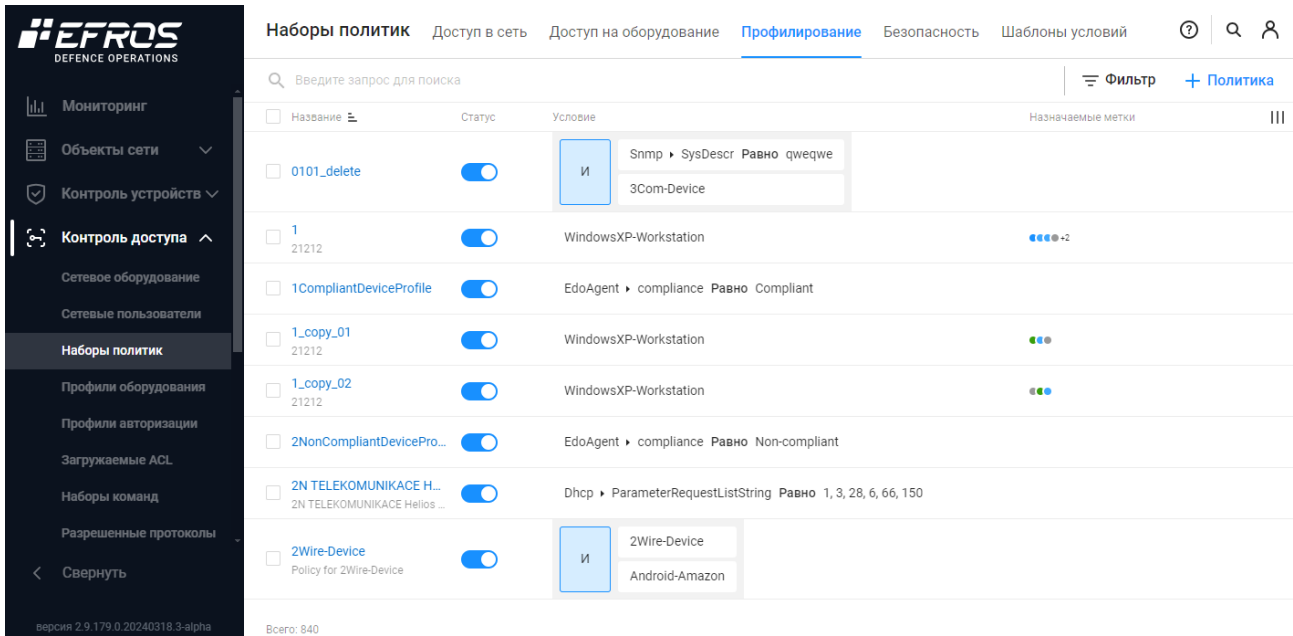


Рисунок 64 – Подраздел «Наборы политик», вкладка «Профилирование»

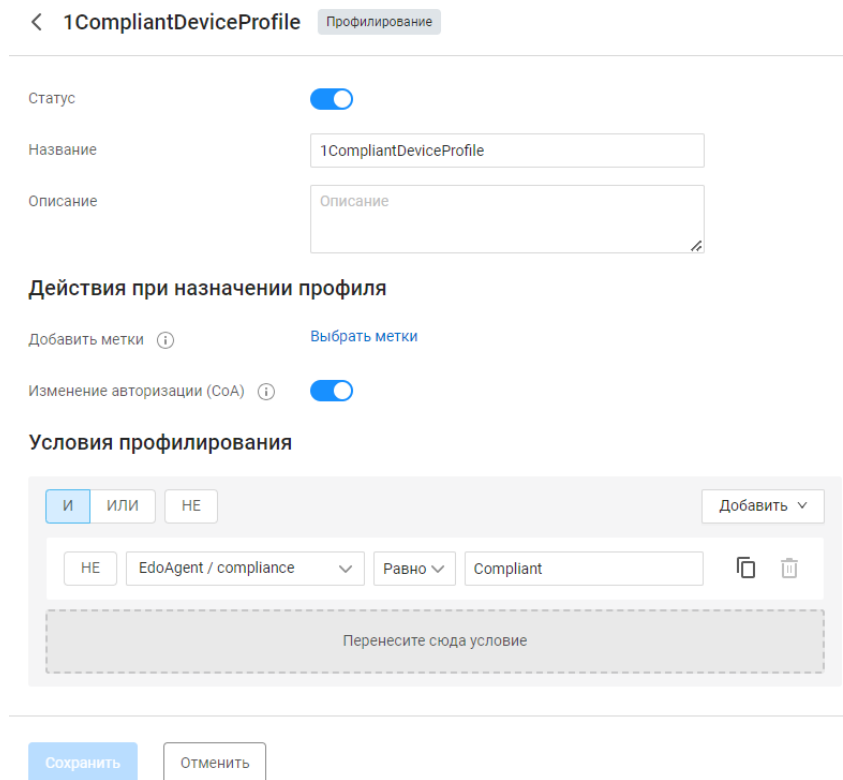


Рисунок 65 – Пример созданной политики профилирования

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Изменение авторизации (CoA)»: активен;
- варианты заполнения поля «Условия профилирования»:
 - EdoAgent / compliance Равно Compliant;
 - EdoAgent / compliance Равно Non-Compliant;
 - EdoAgent / compliance Равно Indeterminate.

Пример созданных политик профилирования приведен на рис. 66.

Наборы политик			
Доступ в сеть			
Доступ на оборудование			
Профилирование			
🔍 DeviceProfile			
<input type="checkbox"/>	Название	Статус	Условие
<input type="checkbox"/>	1CompliantDeviceProfile	<input checked="" type="checkbox"/>	EdoAgent ▶ compliance Равно Compliant
<input type="checkbox"/>	2NonCompliantDevicePro...	<input checked="" type="checkbox"/>	EdoAgent ▶ compliance Равно Non-compliant
<input type="checkbox"/>	3IndeterminateDevicePro...	<input checked="" type="checkbox"/>	EdoAgent ▶ compliance Равно Indeterminate

Рисунок 66 – Пример созданных политик профилирования

- i** Созданные политики профилирования предоставляют возможность назначения соответствующего профиля для устройства в зависимости от текущего статуса соответствия требованиям политики безопасности: 1CompliantDeviceProfile, 2NonCompliantDeviceProfile или 3IndeterminateDeviceProfile. Для каждого профиля устройства можно настроить требуемые правила политики доступа в сеть.

Г.2 Создание политики доступа в сеть на основе профилей

Последовательность действий для создания политики доступа в сеть на основе профилей:

- 1) перейти в раздел «Контроль доступа» → «Наборы политик» → вкладка «Доступ в сеть» → кнопка «**+** Политика »;
- 2) откроется страница создания политики доступа в сеть. Заполнить поля необходимыми параметрами для настройки условий срабатывания политики доступа в сеть (рис. 67).

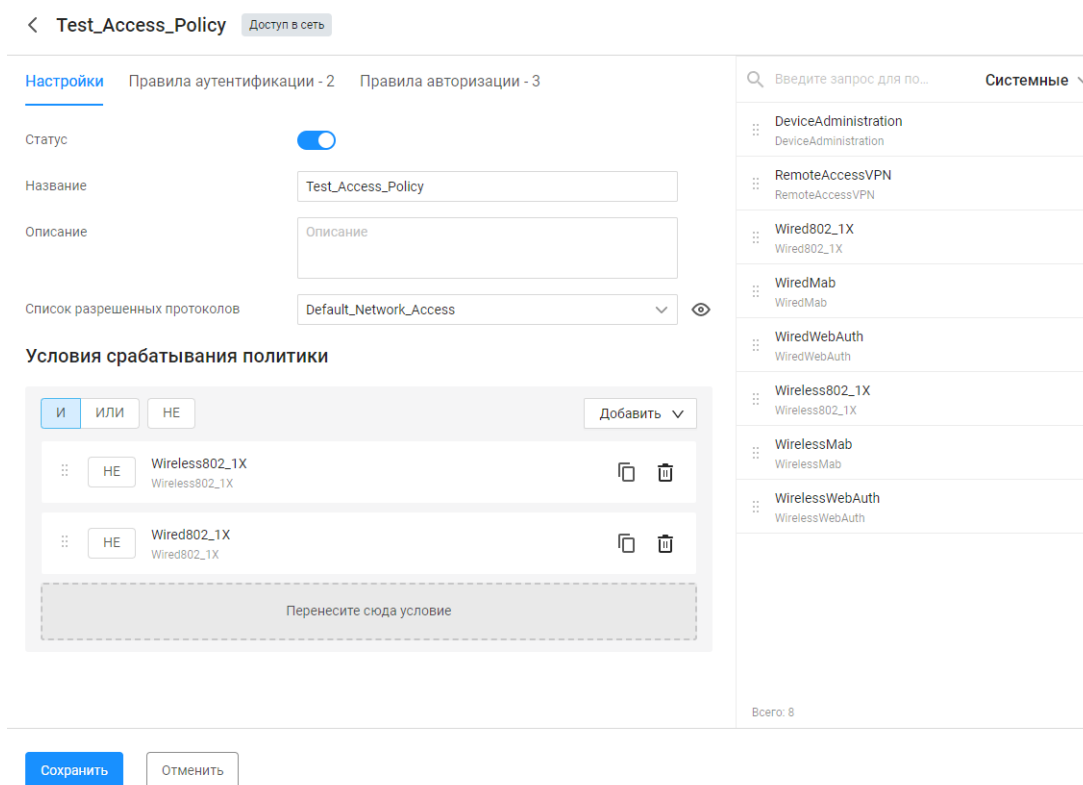


Рисунок 67 – Параметры политики доступа в сеть

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Список разрешенных протоколов»: Default_Network_Access (набор разрешенных протоколов по умолчанию);
- поле «Условия срабатывания политики»: «Wireless802_1X» и «Wired802_1X» (из шаблонов условий).

i Шаблоны условий «Wireless802_1X» и «Wired802_1X» – это наборы условий для беспроводной и проводной аутентификации устройств по стандарту 802.1x.

В наборе правил «Условия срабатывания политики» используются атрибуты и значения, заданные в профиле оборудования. В зависимости от того, какое сетевое оборудование будет запрашивать доступ, для подключаемого устройства – могут быть использованы разные значения из профиля оборудования.

3) Настроить правила аутентификации:

- на странице созданной политики доступа в сеть перейти на вкладку «Правила аутентификации» (см. рис. 67);
- нажать кнопку «+ Правило аутентификации». Создаваемое правило

- аутентификации предназначено для проверки протоколов подключения устройства, запрашивающего доступ в сеть;
- откроется страница создания правила аутентификации. Заполнить поля необходимыми параметрами (рис. 68).

< test11138a Доступ в сеть

Статус

Название

Проверка учетных данных

Источник данных

При ошибке аутентификации

Пользователь не найден

Условия срабатывания правила

И ИЛИ НЕ Добавить

НЕ

НЕ

НЕ

Перенесите сюда условие

Рисунок 68 – Создание правила аутентификации

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Источник данных»: InternalUsers;
- поле «При ошибке аутентификации»: продолжить;
- поле «Пользователь не найден»: отклонить;
- поле «Условия срабатывания правила»:
 - логический оператор: «И»;
 - Gazinformservice / GisEapType Равно PEAP;
 - Gazinformservice / GisEapAuthType Равно GTC;
 - Gazinformservice / GisTipe Равно PAP.

Для запрета доступа в сеть устройств, не соответствующих ранее созданным правилам аутентификации, необходимо в строке правила «Default» указать источник данных «DenyAccess» (рис. 69).

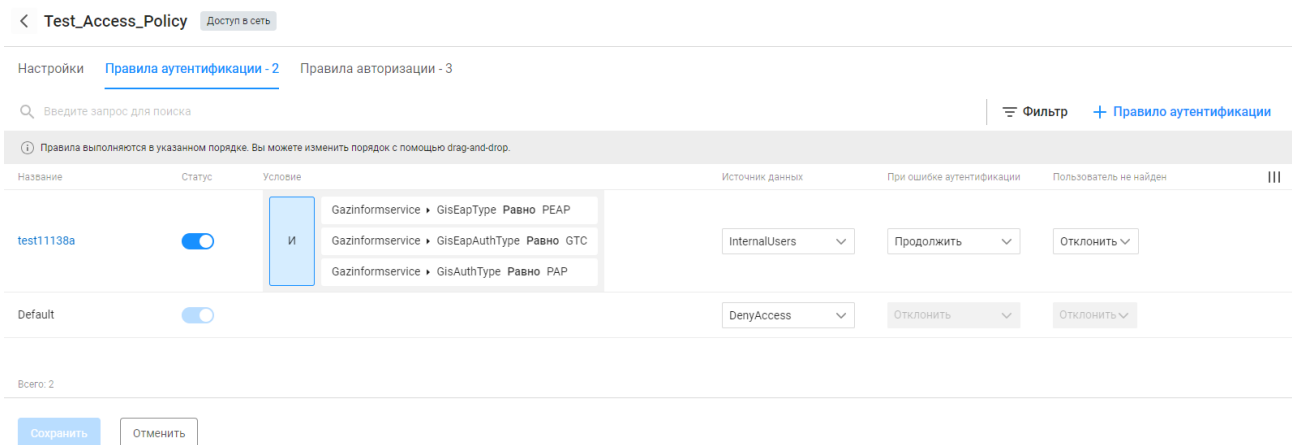


Рисунок 69 – Редактирование правила аутентификации «Default» для запрета доступа в сеть устройств, не соответствующим правилам аутентификации

4) Настроить правила авторизации:

- на странице созданной политики доступа в сеть перейти на вкладку «Правила авторизации» (см. рис. 68);
- нажать кнопку «[+ Правило авторизации](#)». Создаваемое правило авторизации предназначено для предоставления устройствам доступа на основе назначенных профилей
- откроется страница создания правила авторизации. Заполнить поля необходимыми параметрами для устройства с профилем статуса соответствия требованиям безопасности «Не соответствует» (Non-Compliant) и «Не определено» (Indeterminate). Пример созданного правила приведен на рис. 70;
- создать правило авторизации для устройства с профилем статуса соответствия требованиям безопасности «Соответствует» (Compliant). Пример созданного правила приведен на рис. 71.

< NonCompliantDeviceRule Доступ в сеть

Статус

Название

Действия при выполнении условий

Профиль авторизации ⓘ

Условия срабатывания правила

И ИЛИ НЕ Добавить ▾

⋮ НЕ EndPoints / BaseProfile ▾ Равно ▾ 2NonCompliantDeviceProfile ▾ ⋮ 📄 🗑️

⋮ НЕ EndPoints / BaseProfile ▾ Равно ▾ 3IndeterminateDeviceProfile ▾ ⋮ 📄 🗑️

Перенесите сюда условие

Рисунок 70 – Пример созданного правила авторизации

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Профиль авторизации»: название ранее созданного профиля авторизации;
- поле «Условия срабатывания правила»:
 - EndPoints / BaseProfile Равно {название созданной ранее политики профилирования};
 - EndPoints / BaseProfile Равно {название созданной ранее политики профилирования}.

CompliantDeviceRule Доступ в сеть

Статус:

Название:

Действия при выполнении условий

Профиль авторизации:

Условия срабатывания правила

И ИЛИ НЕ Добавить

НЕ EndPoints / BaseProfile Равно 1CompliantDeviceProfile

Перенесите сюда условие

Сохранить Отменить

Рисунок 71 – Пример созданного правила авторизации устройства со статусом «Соответствует»

Для пользователей, не соответствующих ранее созданным правилам авторизации, можно настроить переадресацию для последующего прохождения аутентификации. Для этого необходимо в строке правила «Default» указать предустановленный профиль авторизации «DefaultAuthorizationProfile» или ранее созданный профиль (рис. 72).

Test_Access_Policy Доступ в сеть

Настройки Правила аутентификации - 2 Правила авторизации - 3

Введите запрос для поиска Фильтр + Правило авторизации

Правила выполняются в указанном порядке. Вы можете изменить порядок с помощью drag-and-drop.

Название	Статус	Условие	Профиль авторизации
NonCompliantDeviceRule	<input checked="" type="checkbox"/>	ИЛИ EndPoints > BaseProfile Равно 2NonCompliantDeviceProfile EndPoints > BaseProfile Равно 3IndeterminateDeviceProfile	NonCompliantDevice...
CompliantDeviceRule	<input checked="" type="checkbox"/>	EndPoints > BaseProfile Равно 1CompliantDeviceProfile	CompliantDevicesAut...
Default	<input checked="" type="checkbox"/>		RADIUS11138

Всего: 3

Сохранить Отменить

Рисунок 72 – Редактирование правила авторизации «Default»

! Если создано несколько политик доступа, а внутри несколько правил аутентификации/авторизации, то при запросе подключения проверка по условиям срабатывания будет осуществляться по списку в указанном порядке (сверху вниз).

Перечень сокращений

ACL	–	Access Control List
AD	–	Active Directory
CoA	–	Change of Authorization
EAP	–	Extensible Authentication Protocol
FAST	–	Flexible Authentication via Secure Tunneling
GTC	–	Generic Token Card
IP	–	Internet Protocol
MAB	–	MAC Authentication Bypass
MAC	–	Media Access Control
MD5	–	Message Digest 5
MSCHAPv2	–	Microsoft Challenge–Handshake Authentication Protocol v 2
NAC	–	Network Access Control
PAP	–	Password Authentication Protocol
PEAP	–	Protected Extensible Authentication Protocol
RADIUS	–	Remote Authentication in Dial-In User Service
TACACS+	–	Terminal Access Controller Access Control System plus
TEAP	–	Tunnel Extensible Authentication Protocol
TLS	–	Transport Layer Security
TTLS	–	Tunneled Transport Layer Security
URL	–	Uniform Resource Locator
VLAN	–	Virtual Local Area Network
VPN	–	Virtual Private Network
ОС	–	Операционная система
ПК	–	Программный комплекс
ПО	–	Программное обеспечение