

КОНТРОЛЬ СОСТОЯНИЯ СЕТИ

С ПЛАТФОРМОЙ
NETOPIA FIREWALL COMPLIANCE

Модульность и гибкость

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ И УГРОЗАМИ (VULNERABILITY AND THREAT MANAGEMENT)

- Интеграция с системами управления уязвимостями и сканерами уязвимостей.
- Маркировка критичных активов.
- Оценка опасности угроз.

- Анализ векторов атак.
- Сверхприоритизация устранения уязвимостей.

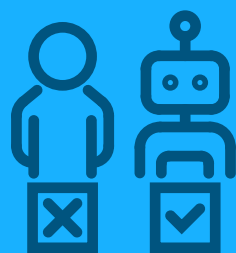
УПРАВЛЕНИЕ ПОЛИТИКОЙ БЕЗОПАСНОСТИ (SECURITY POLICY MANAGEMENT)

- Анализ и контроль политик доступа и сегментации сети.
- Контроль конфигураций.
- Анализ и контроль правил доступа и их изменений.
- Визуализация сети.

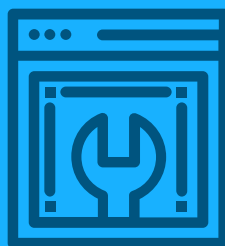
Возможные сценарии



АНАЛИЗ И ОПТИМИЗАЦИЯ
ПРАВИЛ ДОСТУПА



КОНТРОЛЬ СЕГМЕНТАЦИИ СЕТИ



АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ
ЖИЗНЕННЫМ ЦИКЛОМ
ДОСТУПОВ



НЕПРЕРЫВНЫЙ АУДИТ
И РЕСЕРТИФИКАЦИЯ ПРАВИЛ



АНАЛИЗ ВЕКТОРОВ АТАК
И УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ



ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ

Netopia Firewall Compliance



АУДИТ ПОЛИТИК
(FIREWALL ASSURANCE)



УПРАВЛЕНИЕ
ПОЛИТИКАМИ (CHANGE
MANAGEMENT)

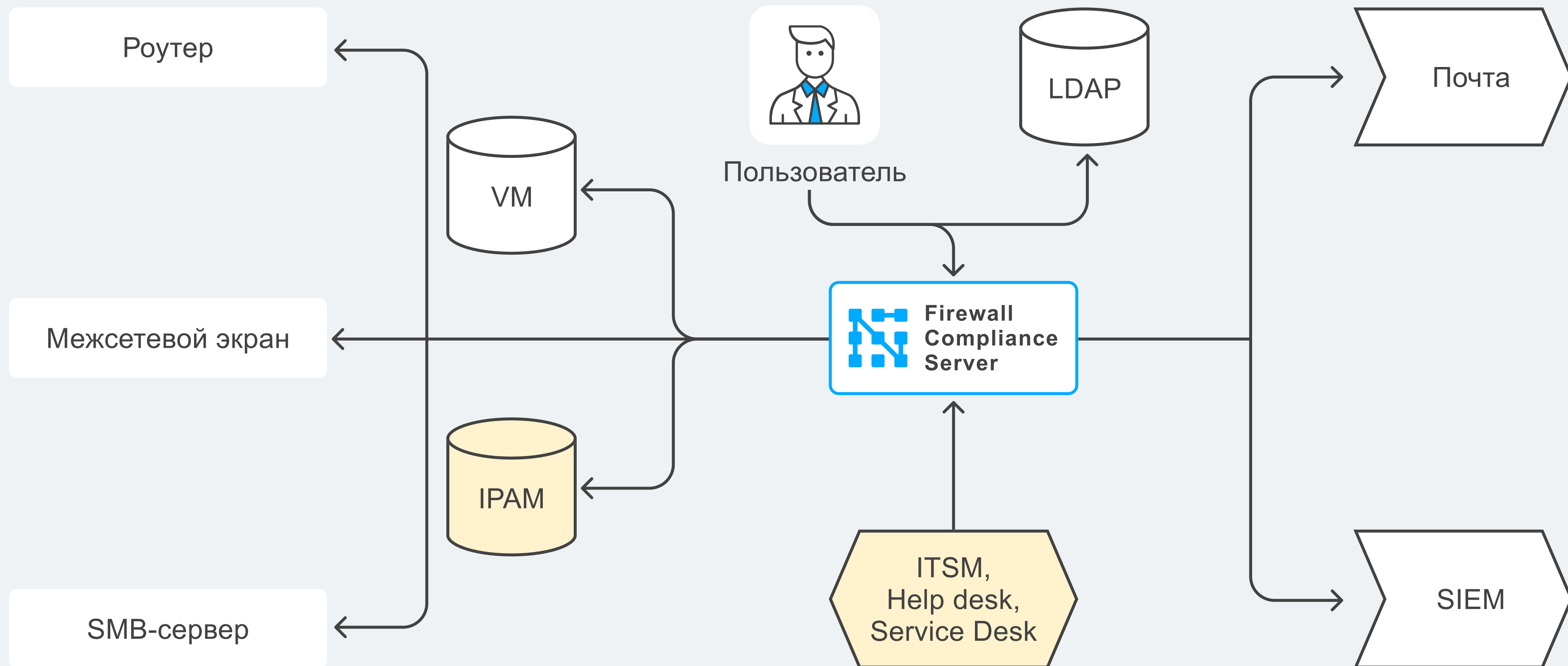


АУДИТ СЕТИ (NETWORK
ASSURANCE)



ПРИОРИТИЗАЦИЯ
УЯЗВИМОСТЕЙ
(VULNERABILITY
CONTROL)

ТИПОВАЯ СТРУКТУРА ВЗАИМОДЕЙСТВИЯ



ПОДДЕРЖИВАЕМЫЕ СИСТЕМЫ

Почта

БPM-системы

SIEM

AD/LDAP



Vulnerability Management

IPAM

Security Scanner

ITSM

ИНТЕГРИРУЕМЫЕ СИСТЕМЫ

NAUMEN

NAUMEN SERVICE DESK

BPMSOFT

BPM SOFT

**Security
Vision**

SECURITY VISION VM

 **positive technologies**

POSITIVE TECHNOLOGIES VM / POSITIVE TECHNOLOGIES MAXPATROL 8

 **Microsoft
Active Directory**

MICROSOFT ACTIVE DIRECTORY / LDAP



IPAM



SIEM

ДОБАВЛЕНИЕ СИСТЕМ ВОЗМОЖНО ПО ЗАПРОСУ

СПИСОК ПОДДЕРЖИВАЕМОГО ОБОРУДОВАНИЯ И ПО



IOS

ASA Firewall



HUAWEI



Континент



В БЛИЖАЙШЕЕ ВРЕМЯ:



МОДУЛЬ «АУДИТ СЕТИ» (NETWORK ASSURANCE) ПОМОГАЕТ ПОНЯТЬ

КАК ВЫГЛЯДИТ ВАША СЕТЬ?

**КАК СКОНФИГУРИРОВАНО СЕТЕВОЕ
ОБОРУДОВАНИЕ?**

КАК СЕГМЕНТИРОВАНА ВАША СЕТЬ?

ПРИНЦИП РАБОТЫ МОДУЛЯ «АУДИТ СЕТИ» (NETWORK ASSURANCE)



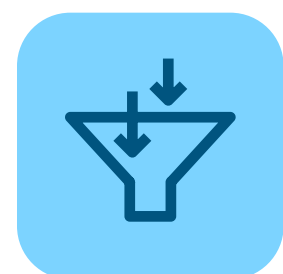
Полная видимость сети

ИНТЕРАКТИВНАЯ КАРТА СЕТИ

КОНТРОЛЬ КОНФИГУРАЦИЙ

КОНТРОЛЬ ПОЛИТИКИ СЕГМЕНТИРОВАНИЯ

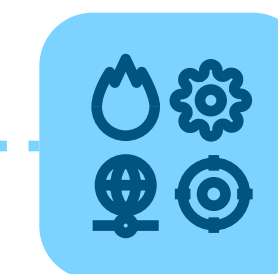
КАК ЭТО РАБОТАЕТ?



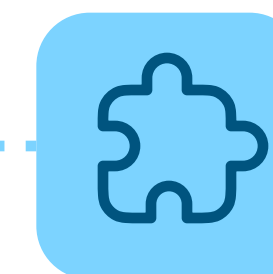
1. Сбор и нормализация



2. Моделирование



3. Детальный анализ



СБОР КОНФИГУРАЦИЙ



Устройство: ASA-v-active

0 шт.

Конфигурация

Таблица маршрутизации

Интерфейсы

NAT

Политика

Каталог объектов

Различия версий конфигурации устройства

1diff previous currant
2--- previous
3+++ currant
4@@ -54,10 +54,6 @@
5 same-security-traffic permit intra-interface
6 no object-group-search access-control
7 access-group ACL_LAB global
8-access-list ACL_LAB extended deny tcp host 172.16.240.31 172.16.242.0 255.255.255.0 eq www
9-access-list ACL_LAB extended deny tcp host 172.16.240.31 172.16.242.0 255.255.255.0 eq 81
10-access-list ACL_LAB extended deny tcp host 172.16.240.31 172.16.242.0 255.255.255.0 eq 82
11-access-list ACL_LAB extended permit ip any any
12 access-list ACL_LAB extended permit ip 172.16.240.0 255.255.255.0 172.16.242.0 255.255.255.0
13 access-list ACL_LAB extended permit ip 172.16.241.0 255.255.255.0 172.16.242.0 255.255.255.0
14 access-list ACL_LAB extended deny ip 172.16.241.0 255.255.255.0 172.16.243.0 255.255.255.0
15 @@ -66,13 +62,13 @@
16 access-list ACL_LAB extended permit udp 172.16.243.0 255.255.255.0 any eq domain
17 access-list ACL_LAB extended permit tcp 172.16.243.0 255.255.255.0 any eq www
18 access-list ACL_LAB extended permit tcp 172.16.243.0 255.255.255.0 any eq https
19+access-list ACL_LAB extended permit icmp 172.16.242.0 255.255.255.0 172.16.243.0 255.255.255.0 echo-reply
20 access-list ACL_LAB extended deny ip 172.16.242.0 255.255.255.0 172.16.243.0 255.255.255.0
21 access-list ACL_LAB extended deny ip 172.16.243.0 255.255.255.0 172.16.242.0 255.255.255.0
22 access-list ACL_LAB extended permit tcp 10.0.0.0 255.255.255.0 host 172.16.240.1 eq ssh
23 access-list ACL_LAB extended permit tcp 10.0.0.0 255.255.255.0 host 172.16.241.1 eq ssh
24 access-list ACL_LAB extended permit ip 10.0.0.0 255.255.255.0 172.16.0.0 255.255.0.0
25 access-list ACL_LAB extended permit tcp host 172.16.240.31 172.16.243.0 255.255.255.0 eq pop3
26-access-list DMZ_CAP_ACL extended permit tcp any host 172.16.242.30 eq 8080
27 pager lines 23
28 mtu LAB_240 1500
29 mtu LAB_241 1500
30

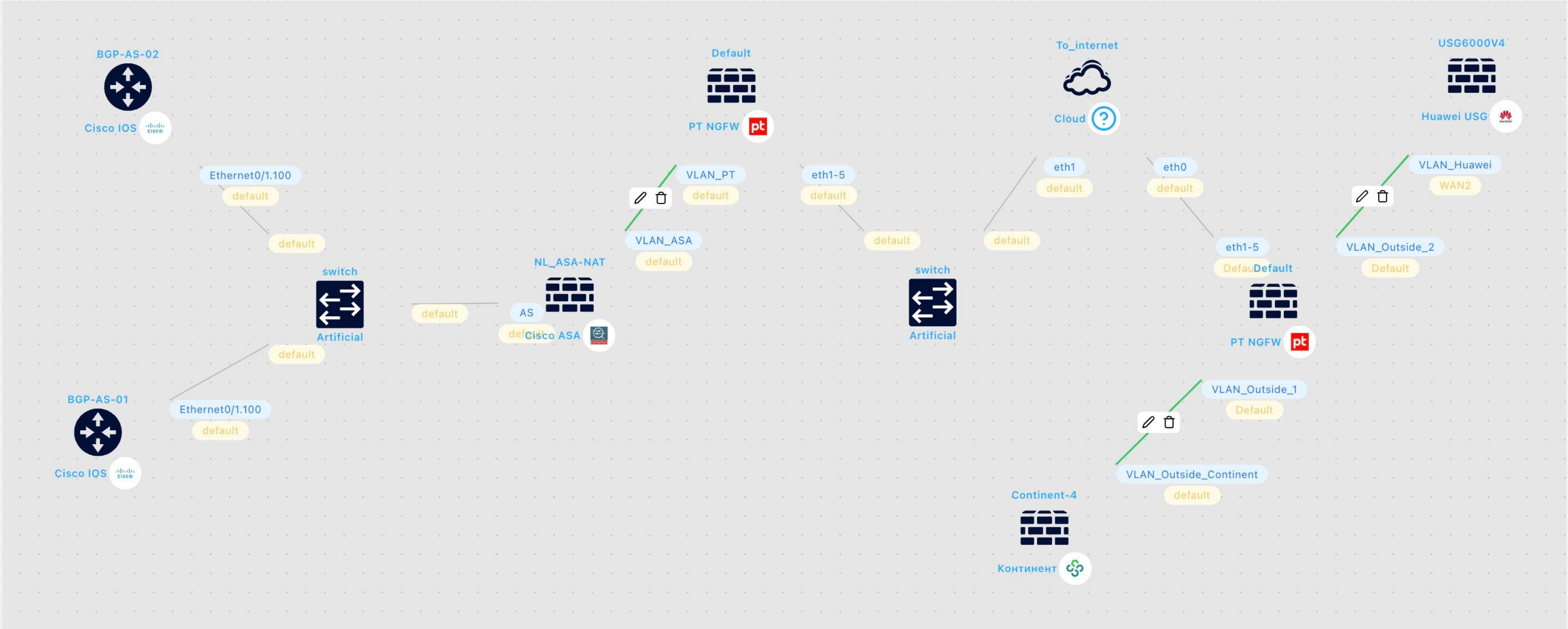
История версий

30 дней

Дата и время	Версия ПО	Исполнители	Раскрыть
2026.07.06 16:17	9.24(1)		
Описание			
2026.06.29 16:22	9.24(1)		
Описание			
2026.06.29 16:08	unknown		
Описание			
2026.06.29 16:01	9.24(1)		
Описание			

v3.16.0

- Сбор конфигураций по событию или по времени.
- Ретроспективный анализ изменений.



Построение карты сети (уровня L3) и визуализация сетевой инфраструктуры.

ДЕТАЛЬНЫЙ АНАЛИЗ



Контроль конфигураций устройств

КонтрольПеременныеБаза проверок

УстройстваПроверки

Список устройств214 шт.

Колонки

Устройства	Вендор / тип	Теги	Проверки
☐ usghuawei	 Межсетевой экран	 Huawei USG  Huawei USG	0 / 0 >
☐ USG6000V4	 Межсетевой экран	 Huawei USG  Huawei USG	0 / 0 >
☐ UserGate_6-1-9	 Межсетевой экран	 UserGate  UserGate	0 / 7 >
☐ usergate	 Межсетевой экран	 UserGate  UserGate	0 / 7 >
☐ test_without_licence	 Маршрутизатор	 Cisco IOS  Cisco IOS	0 / 27 >
☐ Test QTech devicee	 Маршрутизатор	 Qtech  Qtech  test QT	0 / 0 >
☐ s-terra	 Межсетевой экран	 C-Terra  C-Terra	4 / 15 >

Проверки устройства: s-terra15 шт.

Наименование	Статус	Дата последнего запуска
280. Настройка протоколирования событий	Пройдена	2026.07.24, 18:09:26
273. Запрет стандартной строки SNMP	Пройдена	2026.07.24, 18:09:26
283. Настройка активизации процесса обмена сообщениями, подтверждающими активность	Пройдена	2026.07.24, 18:09:26
275. Настройка имени хоста	Пройдена	2026.07.24, 18:09:26
274. Настройка SNMPv2c	Не пройдена	2026.07.24, 18:09:25
269. Настройка зашифрованного пароля для режима конфигурации	Не пройдена	2026.07.24, 18:09:26
279. Защита от внешних нарушителей с адресом из стандартного пула адресов	Не пройдена	2026.07.24, 18:09:26

Анализ соответствия конфигураций сетевых устройств заданным стандартам (Анализ настроек на Hardening и Best Practices, нормативные документы (ГОСТ 57580, ПДН, ГИС, КИИ)).

МОДУЛЬ «АУДИТ ПОЛИТИК» (FIREWALL ASSURANCE) ПОМОГАЕТ ПОНЯТЬ

ОПТИМАЛЬНЫ ЛИ ВАШИ ПРАВИЛА?

СООТВЕТСТВУЮТ ЛИ ПРАВИЛА ЗОНАМ БЕЗОПАСНОСТИ?

КАК МЕНЯЮТСЯ ПРАВИЛА ДОСТУПА?

ПРИНЦИП РАБОТЫ МОДУЛЯ «АУДИТ ПОЛИТИК» (FIREWALL ASSURANCE)

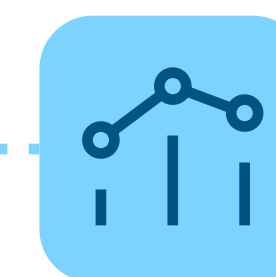
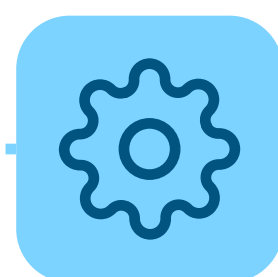
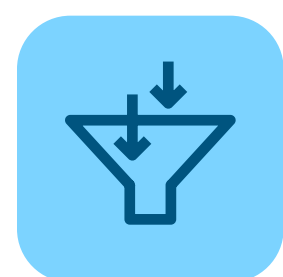


АНАЛИЗ ПРАВИЛ ДОСТУПА
И ИХ ОПТИМИЗАЦИЯ

КОНТРОЛЬ
ЗОН БЕЗОПАСНОСТИ

КОНТРОЛЬ ИЗМЕНЕНИЙ
ПРАВИЛ ДОСТУПА

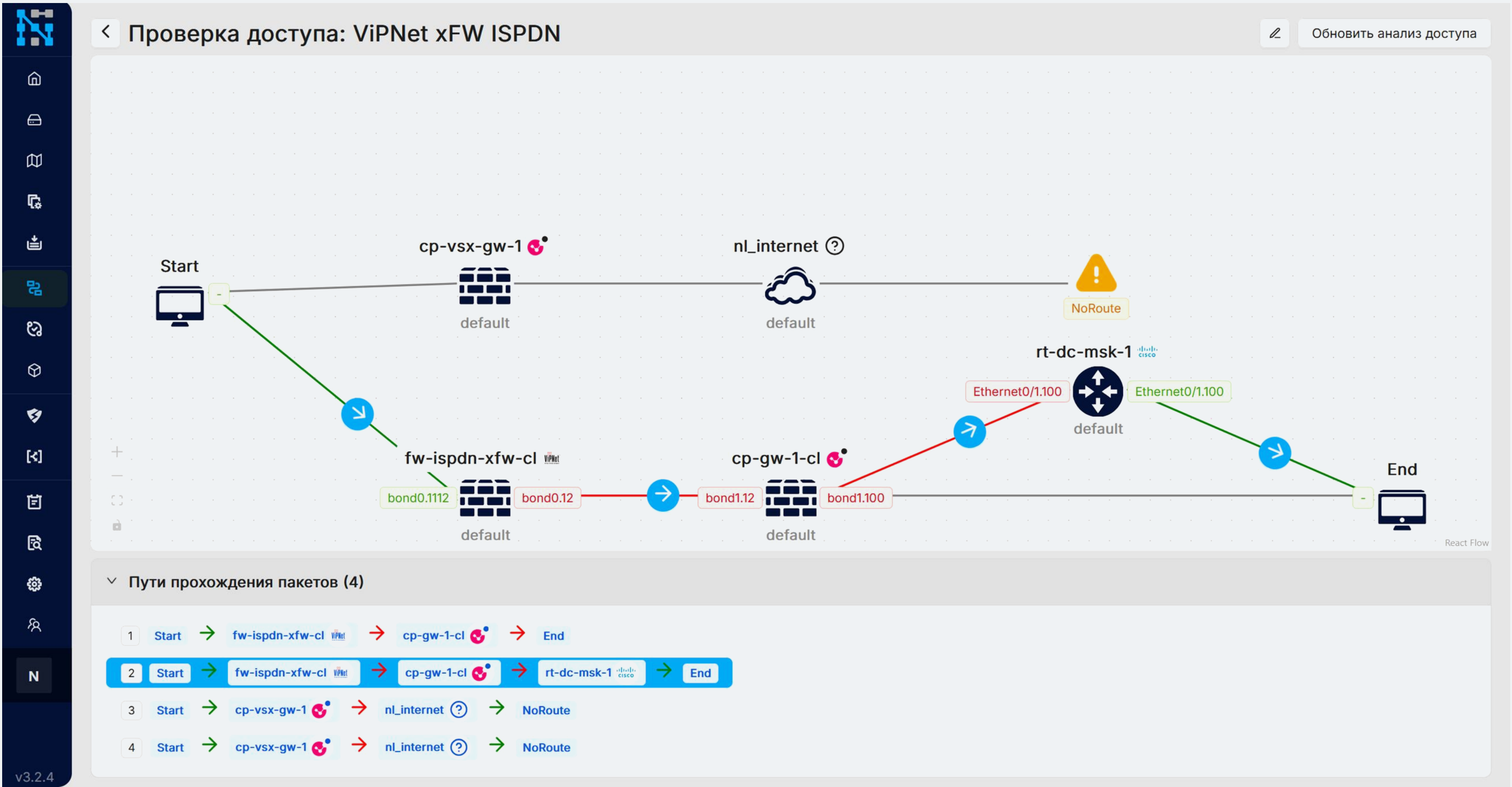
КАК ЭТО РАБОТАЕТ?



1. Сбор и нормализация

2. Анализ. Настраиваемые
задачи и проверки

3. Отчёты и реагирование



- Анализ пути прохождения трафика по сети.
- Контроль наличия или отсутствия доступа в правилах межсетевых экранов по всему пути прохождения трафика.

ОПТИМИЗАЦИЯ СЕТЕВЫХ ПРАВИЛ



Анализ правил

Политика NAT Проверки

281057 шт.

Параметры поиска по правилам ▾

Параметры оптимизации ▾

Колонки 00

№	UID	Устройство	Имя правила	Имя политики	Интерфейс	Источник	Назначение	Сервис	Действие	Приложения	Описание	Оптимизации
1	019f233c-beba-7671-b42d-5b36e7f347f7	Default	_netopla_5d536588	pre-rules from Global	any any	Backdoor	DST_NET_242	tcp:(82)	deny	any		
1	019e0208-8b6f-726d-9afb-5fa72fc6e52	Default	For_clone	pre-rules from device_group_INT	any any	106.168.1.1	any	any	deny	any		
1	019b4fac-c5c4-7888-9437-df92b05c4982	Default	lasdkfj9	pre-rules from device_group_PT-2	any any	host_1.1.1.1 10.0.0.0	host_2.2.2.2	any	accept	any		
1	019e1c78-5c31-7ce6-9540-9b0b5a842e0f	Default	_netopla_dbb0a22e	post-rules from device_group_PT-2	any any	10.3.7.0/24	10.2.7.7	tcp:(87)	accept	any		
1	019a91f5-1d25-7bd9-a75a-af86e452c8f6	Default	2o2w50d5	post-rules from device_group_INT	any any	host_1.1.1.1	host_2.2.2.2	any	accept	any		
1	019d489a-de71-7de7-9170-5971cbf44374	Default	Deny any	post-rules from Global	any any	any	any	any	deny	any		

Строк на странице 20 1 2 3 4 5 ... 14053 > >>

**Оптимизация политик
(затенённые правила,
давно не работающие
правила, правила со
слишком большим
избыточным доступом
и другие оптимизации).**

ОПТИМИЗАЦИЯ ОБЪЕКТОВ ПОЛИТИК



Анализ объектов

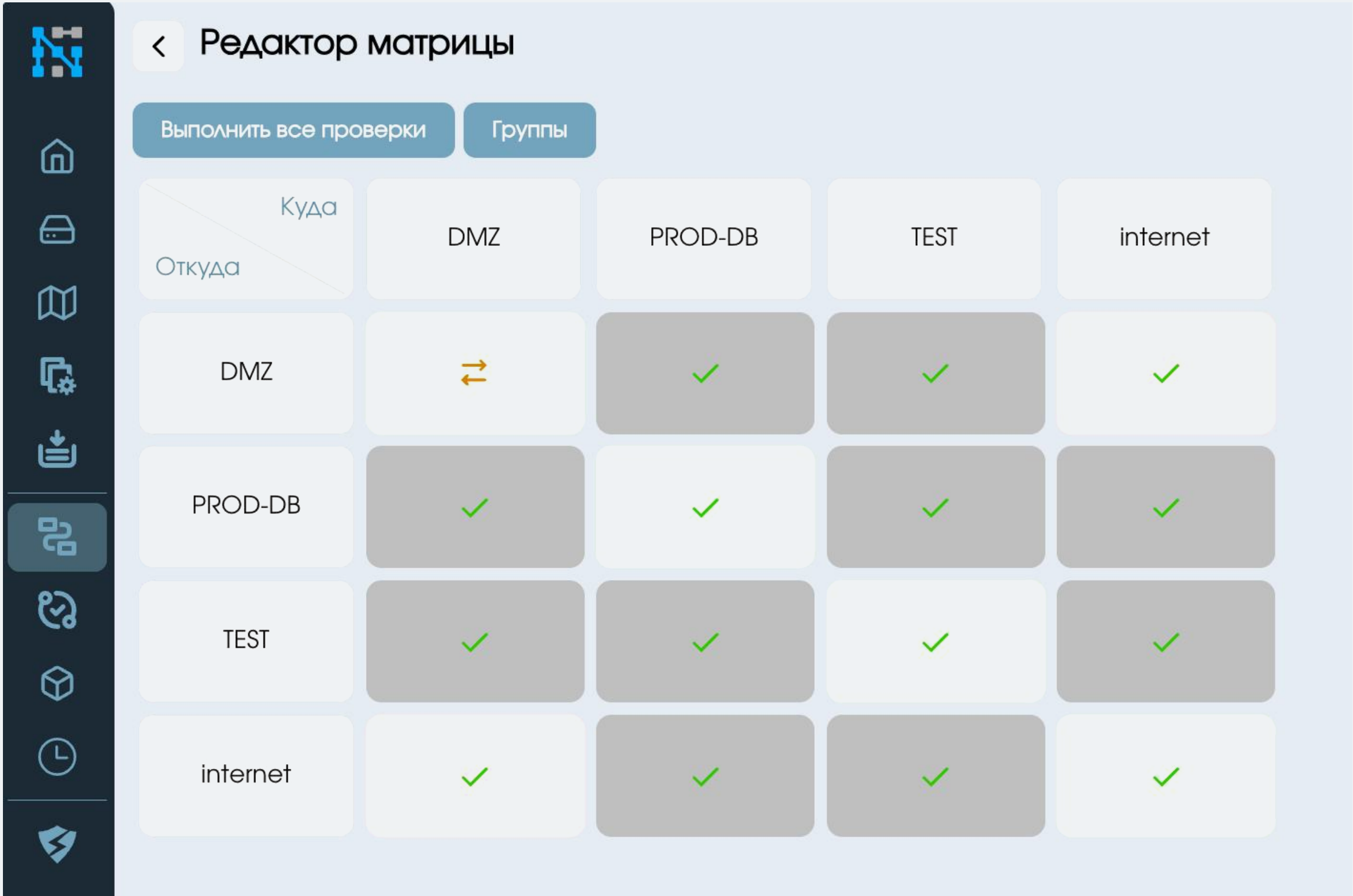
Список объектов

Поиск

Колонки

				Связанные правила			
Наименование	Тип объекта			NAT	SECURITY	Устройство	Вендор
0.0.0.0 0.255.255.255	Wildcard		0	Нет связанных правил	140	IOS_RDPC	Cisco IOS
0.0.0.0 0.255.255.255	Wildcard		0	Нет связанных правил	90	IOS_DPC	Cisco IOS
0.0.0.0-172.16.250.255 0.0.0.0 - 172.16.250.255	IPRange		0	Нет связанных правил	Нет связанных правил	s-terra	C-Teppa
0.0.0.0-192.168.22.255 0.0.0.0 - 192.168.22.255	IPRange		0	Нет связанных правил	Нет связанных правил	s-terra	C-Teppa
0.0.0.0-255.255.255.255 0.0.0.0 - 255.255.255.255	IPRange		3	Нет связанных правил	BSS_SZDFM_IN_97 BSS_PREP_IN_250 BSS_DRT_PROD_IN_3513 +10	Pochta_Huawei	Huawei USG
0.0.0.0-255.255.255.255 0.0.0.0 - 255.255.255.255	IPRange		3	Нет связанных правил	BSS_SZDFM_IN_97 BSS_PREP_IN_250 BSS_DRT_PROD_IN_3201 +13	Pochta_Huawei2	Huawei USG

Оптимизация объектов политик (объекты, не привязанные ни к каким правилам, дублирующиеся объекты).



Матрица доступа — визуальная зональная структура на платформе Netopia, задающая и контролирующая соблюдение правил доступа к сети.

Отображает разрешённый / запрещённый трафик между сегментами сети (зонами) для соответствия требованиям безопасности (ГОСТ 57580, ПДН, ГИС, КИИ, HIPAA, PCI DSS и т.д.), снижая риски и предоставляя оповещения о нарушениях в режиме реального времени для упрощения сегментации и управления сетью.

СОЗДАНИЯ ПРАВИЛ

- Анализ маршрута.
- Определение задействованных устройств.
- Оценка влияния планируемых изменений.

ПЕРЕСМОТРА ПРАВИЛ (РЕСЕРТИФИКАЦИИ)

- Напоминание о сроках пересмотра правил.
- Управление доступом.
- Верификация изменений.

УДАЛЕНИЯ ПРАВИЛ

Автоматическое применение изменений

МОДУЛЬ «УПРАВЛЕНИЕ ПОЛИТИКАМИ» (CHANGE MANAGEMENT)



<

ID: 56cdeeb0-7177-426b-ba5f-65f8b74cae91 | Название: Заявка новая

Удалить заявку

Шаг 1

Шаг 2

Шаг 3

Шаг 4

Шаг 5

Шаг 6

Данные заявки

Редактировать

Тип заявки:

Изменение доступа

Доступ:

Закрытие доступа

Описание:

Тут пусто...

Заявитель запрашивает изменение доступа

1

Источник:

10.0.0.24/32

Назначение:

10.0.0.25/32

Сервис:

ip

Поиск по логину/имени

Роли

Логин	Имя	Роль	Действия
anton	Антон	Администратор FC	
Anton_test	Anton_test	Администратор FC	
arseniy	ars	Администратор FC	
autotest	autotest	Администратор FC	

Исполнители

Заявитель

Victoria

Администратор FC

Согласующие

Порядок согласования

Один из назначенных

Выбор согласующих

По умолчанию

Согласующие не назначены

Исполнители

Порядок исполнения

Один из назначенных

Выбор исполнителей

По умолчанию

Исполнители не назначены

История

История событий

Оставить комментарий

- Управление изменениями политик / конфигураций межсетевых экранов в автоматизированном режиме.
- Внесение и валидация изменений на межсетевых экранах.
- Интеграция с существующими системами управления изменениями в организации (ITSM, PAM, BPM и др.) посредством API.

УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ



Управление пользователями

Список пользователей 23 шт.

+ Колонки 00

☐	Состояние ▾	Логин ▾	Имя ▾	Роль ▾	Происхождение ▾	Парольные политики ▾	Действия
☐	●	Test123	Test123	Администратор FC	Netopia Local	Базовая политика	<button>🔒</button> <button>✎</button> <button>♂</button> <button>🗑️</button>
☐	●	netopia	netopia	Владелец	Netopia Local	Базовая политика	
☐	●	lev	lev	Администратор FC	Netopia Local	Базовая политика	<button>🔒</button> <button>✎</button> <button>♂</button> <button>🗑️</button>
☐	●	test2	test2	Администратор FC	Netopia Local	Базовая политика	<button>🔒</button> <button>✎</button> <button>♂</button> <button>🗑️</button>
☐	●	user1	user1	Администратор FC	Netopia Local	Базовая политика	<button>🔒</button> <button>✎</button> <button>♂</button> <button>🗑️</button>
☐	●	anton	anton	Администратор FC	Netopia Local	Базовая политика	<button>🔒</button> <button>✎</button> <button>♂</button> <button>🗑️</button>
☐	●	igor	igor	Администратор FC	Netopia Local	Базовая политика	<button>🔒</button> <button>✎</button> <button>♂</button> <button>🗑️</button>
☐	●	elena	elena	Администратор FC	Netopia Local	Базовая политика	<button>🔒</button> <button>✎</button> <button>♂</button> <button>🗑️</button>

⬇ ↻ ✎ 0 шт.

Строк на странице 20 < 1 2 >

Источники уч. записей Парольные политики

Список источников +

Наименование	Действия
Netopia Local	<button>🔒</button>

- Возможность управлять локальными учётными записями пользователей и ролями (создавать, изменять, удалять).
- Управление и создание различных парольных политик.
- Интеграция с AD/LDAP.
- Гибкая ролевая модель.

СОБЫТИЯ СИСТЕМЫ



События системы

Журнал событий

Ошибки системы

SIEM-интеграции

2026-07-27 – 2026-07-27

За сегодня

За 3 дня

За месяц

За 3 месяца

За год

Настройки логирования

Список событий 25 шт.

Колонки

Дата/время события	Статус	Пользователь	Роль	Категория	Действие	Наименование объекта
27.07.2026 11:37:22	Успех	autotest	Администратор FC	Пользователи	Вход в систему	-
27.07.2026 11:37:21	Успех	autotest	Администратор FC	Пользователи	Вход в систему	-
27.07.2026 11:37:21	Успех	autotest	Администратор FC	Аудит администратора	Настройки аудита изменены	Настройки аудита
27.07.2026 11:26:25	Успех	autotest	Администратор FC	Пользователи	Вход в систему	-
27.07.2026 11:26:25	Успех	autotest	Администратор FC	Пользователи	Вход в систему	-
27.07.2026 11:26:25	Успех	autotest	Администратор FC	Аудит администратора	Настройки аудита изменены	Настройки аудита
27.07.2026 11:21:05	Успех	netopia	Владелец	Другое	Обновление объекта	-
27.07.2026 11:20:55	Успех	netopia	Владелец	Другое	Обновление объекта	-
27.07.2026 11:20:47	Успех	netopia	Владелец	Другое	Обновление объекта	-
27.07.2026 11:16:51	Успех	kostya	Администратор FC	Другое	Обновление объекта	-
27.07.2026 11:16:50	Успех	kostya	Администратор FC	Другое	Обновление объекта	-
27.07.2026 11:15:46	Успех	kostya	Администратор FC	Другое	Создание объекта	-

**Возможность
отслеживать все
произошедшие события
в системе.**

ЗАДАЧИ МОДУЛЯ «ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ» (VULNERABILITY CONTROL)



МОДУЛЬ «ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ»
(VULNERABILITY CONTROL) ПОМОГАЕТ ПОНЯТЬ

ОБО ВСЕХ ЛИ УЯЗВИМОСТЯХ ВЫ ЗНАЕТЕ?

**КАКИЕ УЯЗВИМОСТИ ЯВЛЯЮТСЯ РЕАЛЬНО
ОПАСНЫМИ ИМЕННО ДЛЯ ВАШЕЙ
ИНФРАСТРУКТУРЫ?**

**КАК ОПТИМАЛЬНО И БЫСТРО УСТРАНИТЬ
ОПАСНЫЕ УЯЗВИМОСТИ?**

ПРИНЦИП РАБОТЫ МОДУЛЯ «ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ» (VULNERABILITY CONTROL)



Автоматическая оценка опасности уязвимостей

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ

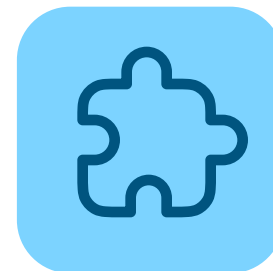
РАСЧЁТ ВЕКТОРОВ АТАК В КОНТЕКСТЕ СЕТИ

РАСЧЁТ ПРИОРИТЕТОВ И РЕАГИРОВАНИЕ

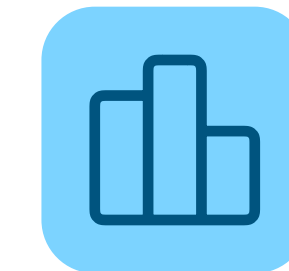
КАК ЭТО РАБОТАЕТ?



1. Выявление



2. Анализ



3. Приоритизация



4. Реагирование

АНАЛИЗ И ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ



Управление уязвимостями

АктивыУязвимостиИсточникиЗлоумышленникиФормулы

Список активов

Поиск по имени и ip-адресу

↺+Колонки00

☐	Наименование	IP	Количество уязвимостей	Оценка риска	Номинальный ущерб	Источник	Срок актуальности, дни	☐	☒
☐	asset_000000	74.29.112.88	1	85.8	0	Netopia	Осталось: 19	☐	☒
☐	sdf	1.1.1.1	0	0	0	Netopia	Осталось: 19	☐	☒
☐	asset_test123	13.0.121.130	1	58.3	0	Netopia	Осталось: 20	☐	☒
☐	asset_d119d9	215.11.11.12	1	85.8	0	Netopia	Осталось: 20	☐	☒
☐	222	2.2.2.2	0	0	333	Netopia	Осталось: 22	☐	☒
☐	10.0.0.20	10.0.0.20	12	93.8	0	MPVM2	Осталось: 26	☐	☒
☐	10.0.0.22	10.0.0.22	36	68.6	0	MPVM2	Осталось: 26	☐	☒
☐	10.0.0.35	10.0.0.35	3	40.7	0	MPVM2	Осталось: 26	☐	☒
☐	10.0.0.36	10.0.0.36	7	52.8	0	MPVM2	Осталось: 26	☐	☒
☐	10.0.0.4	10.0.0.4	58	76.2	0	MPVM2	Осталось: 26	☐	☒
☐	172.16.252.18	172.16.252.18	1	0	0	MPVM2	Осталось: 26	☐	☒
☐	172.16.252.31	172.16.252.31	10	56.3	0	MPVM2	Осталось: 26	☐	☒

- **Корреляция текущих уязвимых активов с их доступностью по сети: из интернета, из сетей подрядчиков или иных внешних источников.**
- **Приоритизация устранения уязвимостей исходя из их достижимости.**

ПОСТРОЕНИЕ ВЕКТОРОВ АТАК



ИСПДн-server

▼

Сервис

Введите сервис. Например: tcp/22

Проверить

Наименование

ИСПДн-server

IP адресс

192.168.12.123

Источник

Значимость

0

Группа достижимых активов

Уровень критичности 0

1 шт.

Достижимые активы

maxpatrol8.netopia.app >

Выявление векторов атак и достижимости по сети критических защищаемых данных через существующие уязвимости.

Модуль	Описание	Лицензирование
«Аудит сети» (Network Assurance)	Анализ соответствия конфигураций сетевых устройств заданным стандартам; ретроспективный анализ изменений конфигураций, анализ настроек на харденинг и лучшие практики сетевой безопасности, построение карты сети и визуализация сетевой инфраструктуры.	По количеству маршрутизирующих устройств.
«Аудит политик» (Firewall Assurance)	Анализ пути прохождения трафика и контроль доступа. Анализ правил доступа, политик и их оптимизация (затенённые правила, давно не работающие правила, правила со слишком большим избыточным доступом и другие оптимизации). Контроль наличия или отсутствия доступа в правилах межсетевых экранов по всему пути прохождения трафика.	По количеству межсетевых экранов. Включает в себя модуль «Аудит сети» (Network Assurance). FA NA
«Управление политиками» (Change Management)	Управление изменениями политик межсетевых экранов в автоматизированном режиме с поддержкой цепочек согласований, присвоением номера тикетов правилам, интеграцией с существующими системами управления изменениями в организации (ITSM, PAM и др.) посредством API.	По количеству межсетевых экранов, на которых будут проводиться изменения политик доступа. Для работы модуля обязательно наличие лицензии «Аудит политик» (Firewall Assurance). ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ: CM FA
«Приоритизация уязвимостей» (Vulnerability Control)	Корреляция текущих уязвимых активов с их доступностью по сети: из интернета, из сетей подрядчиков или иных внешних источников. Приоритизация устранения уязвимостей исходя из их достижимости. Выявление векторов атак и достижимости по сети критических защищаемых данных через существующие уязвимости (Multi-hop атаки).	По количеству активов в сети. Для эффективной работы модуля требуется как можно более полная информация о сети из модулей «Аудит политик» (Firewall Assurance) — обязательно и «Аудит сети» (Network Assurance). ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ: VC FA NA

ОЦЕНИТЕ ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ РЕШЕНИЯ NETOPIA FIREWALL COMPLIANCE!

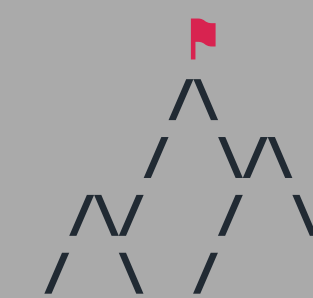


ООО «НЕТОПИЯ»

121205, г. Москва, муниципальный округ Можайский, территория инновационного центра «Сколково», б-р Большой, д. 42, стр. 1, этаж 2, помещение № 162/№ 4

Порядковый номер
в реестре отечествен-
ного ПО — 17109

Резиденты
Сколково



ПРЕМИЯ
ЦИФРОВЫЕ
ВЕРШИНЫ 2025

+7 (495) 255-35-82 / info@netopia.pro