



Инцидент-менеджмент: формирование регламентов реагирования при кибератаках и решение внутренних проблем и задач.

Реализаций подхода к противодействию кибератакам, и централизации доступа к сетевой инфраструктуре с применением принципов Нулевого доверия и Минимальных полномочий на базе продукта UnicNet

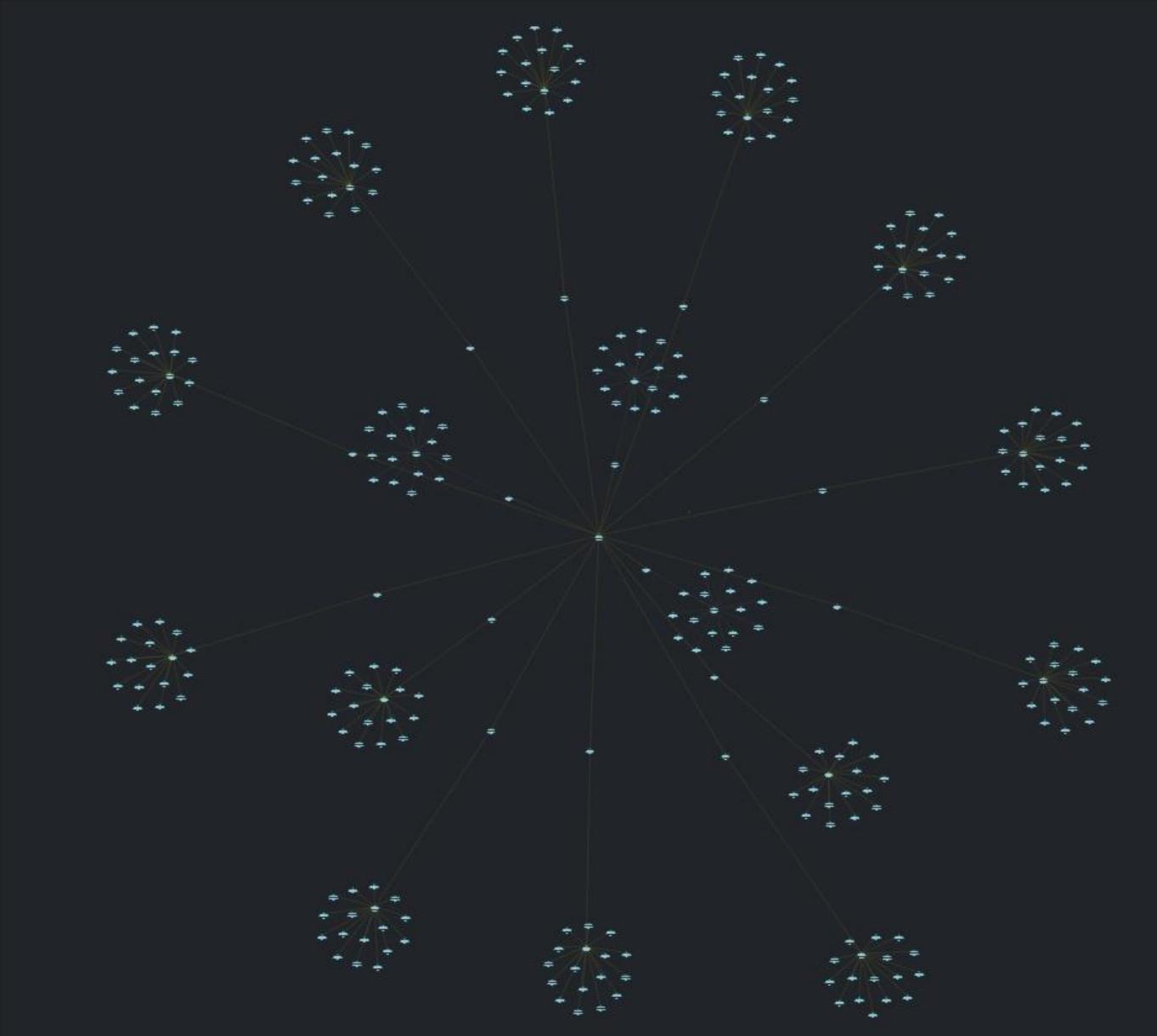


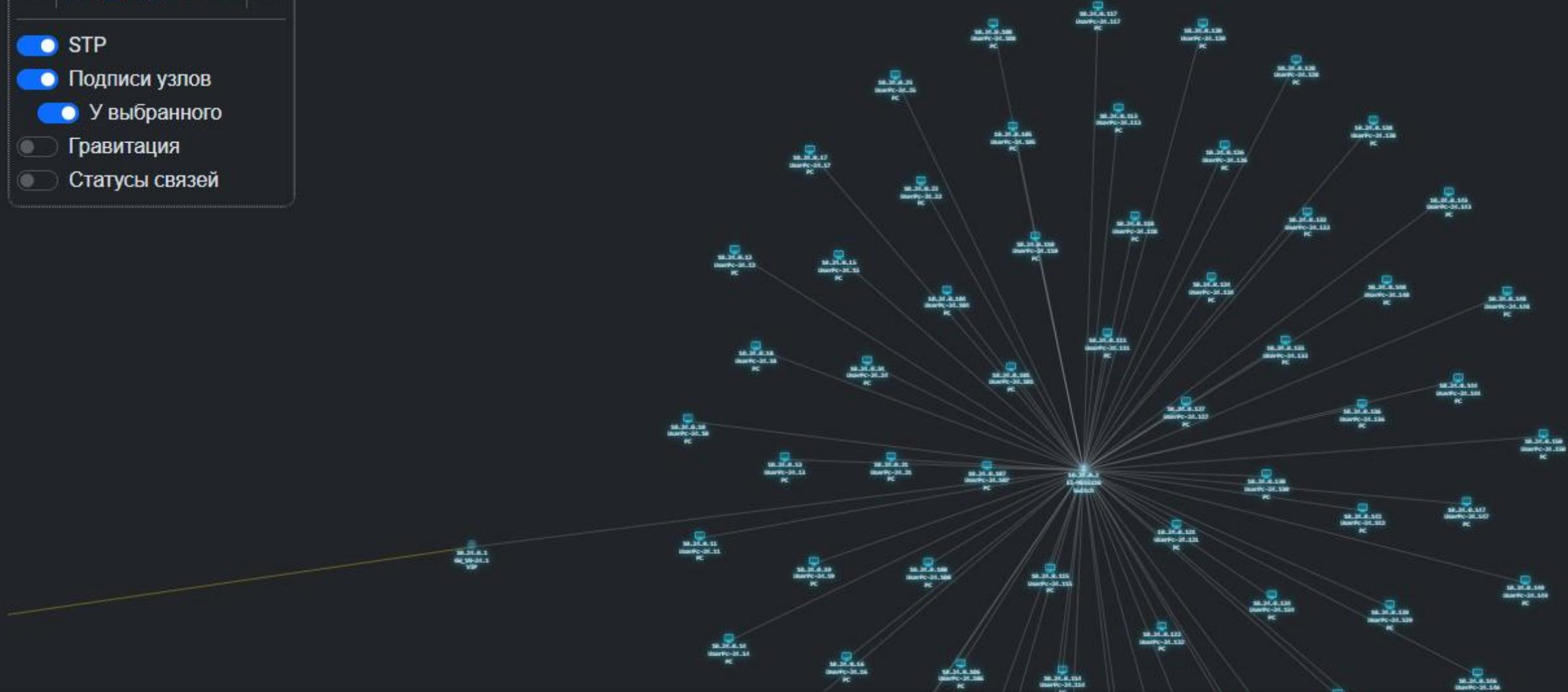
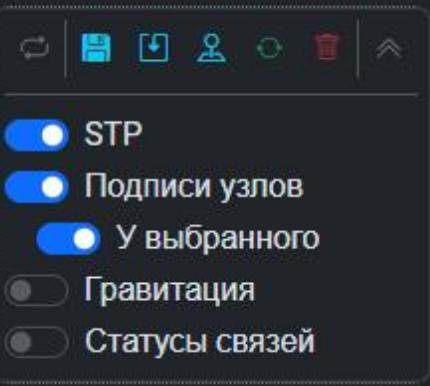
UnicNet



Векторы внутренних проблем

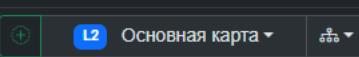
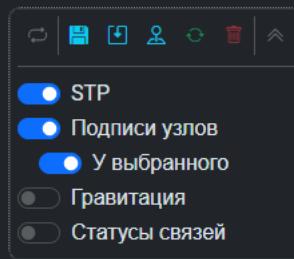
Модель типовой сети объектов КИИ с репликацией





Кейс 1 - Нагрузка на сеть → сеть ложится

Суть проблемы: штурм, перегрузка uplink, неверный порт



Статус портов 10.0.10.100

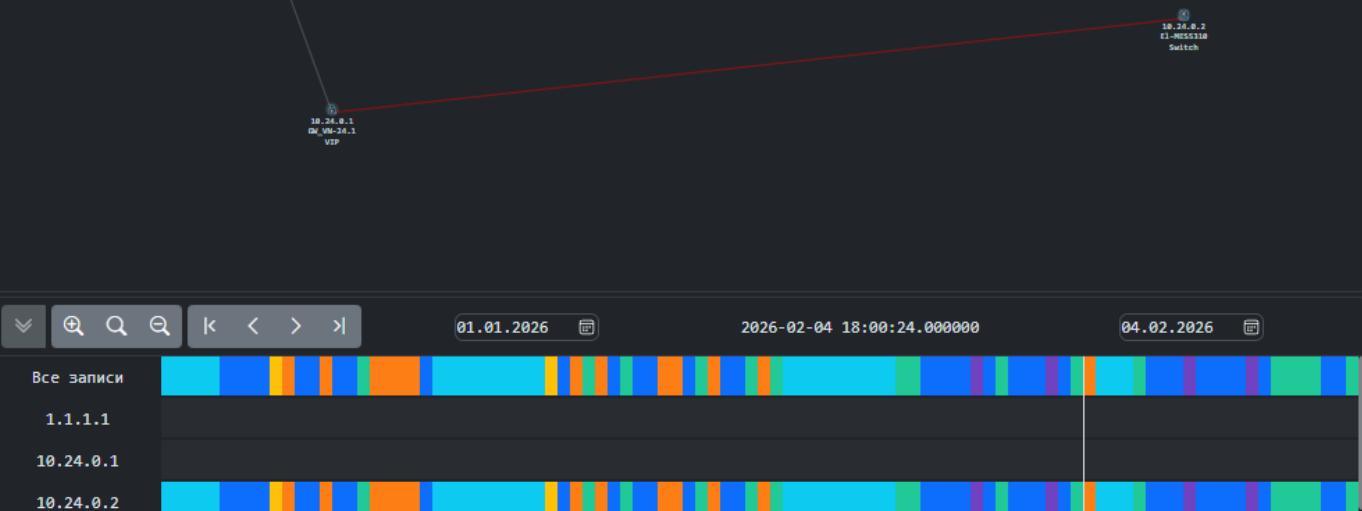
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2	3	4	1	2	3	4
1 Gbps	1 Gbps	1 Gbps	1 Gbps	100 Mbps	1 Gbps	1 Gbps	100 Mbps	1 Gbps	100 Mbps	1 Gbps	4 Gbps	4 Gbps	4 Gbps	4 Gbps																		

⟳ Автообновление портов

≡ Список портов устройства

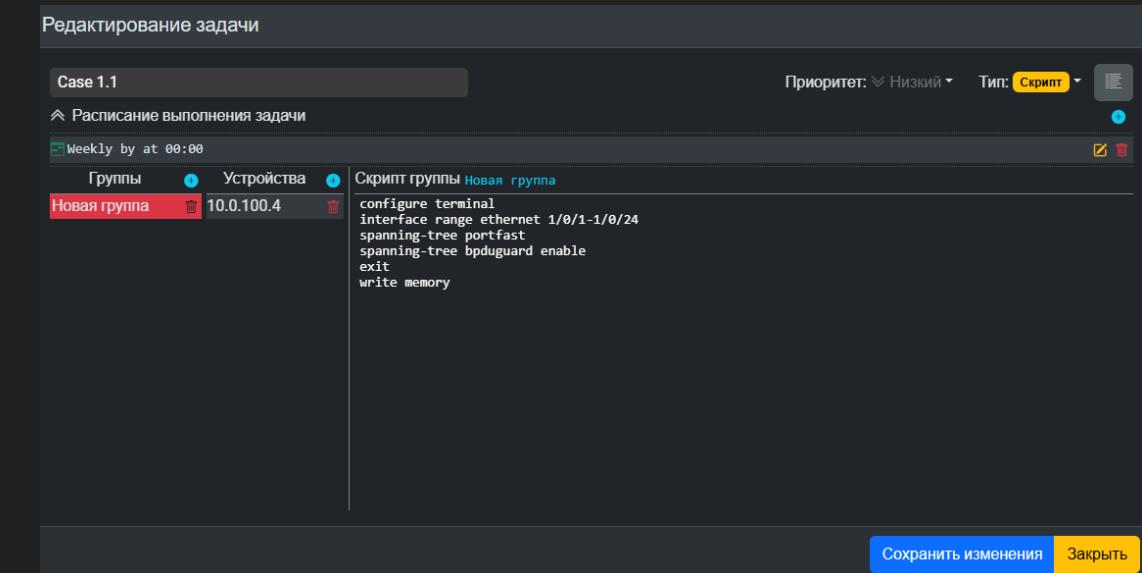
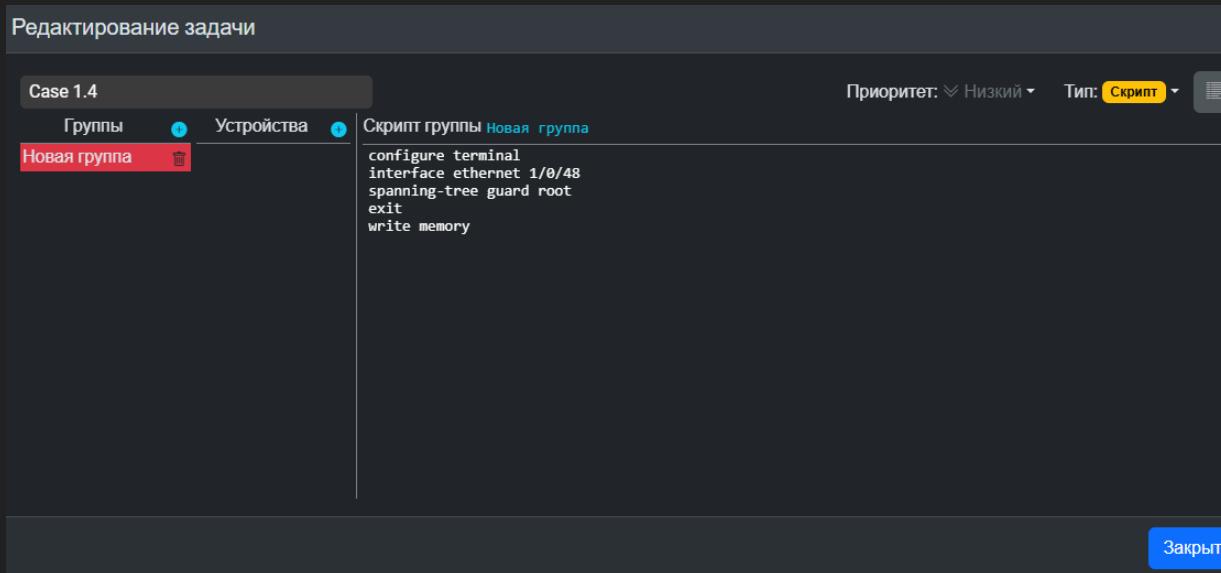
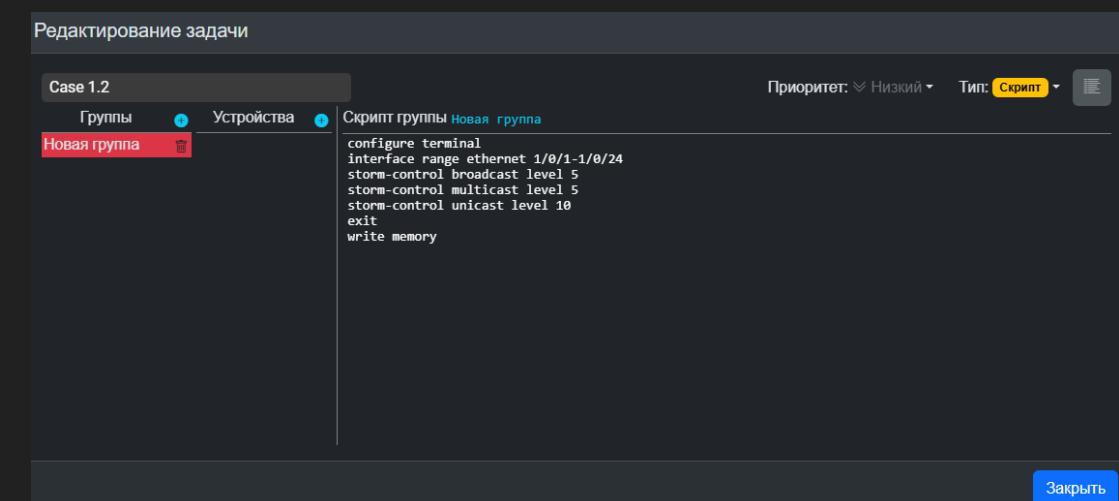


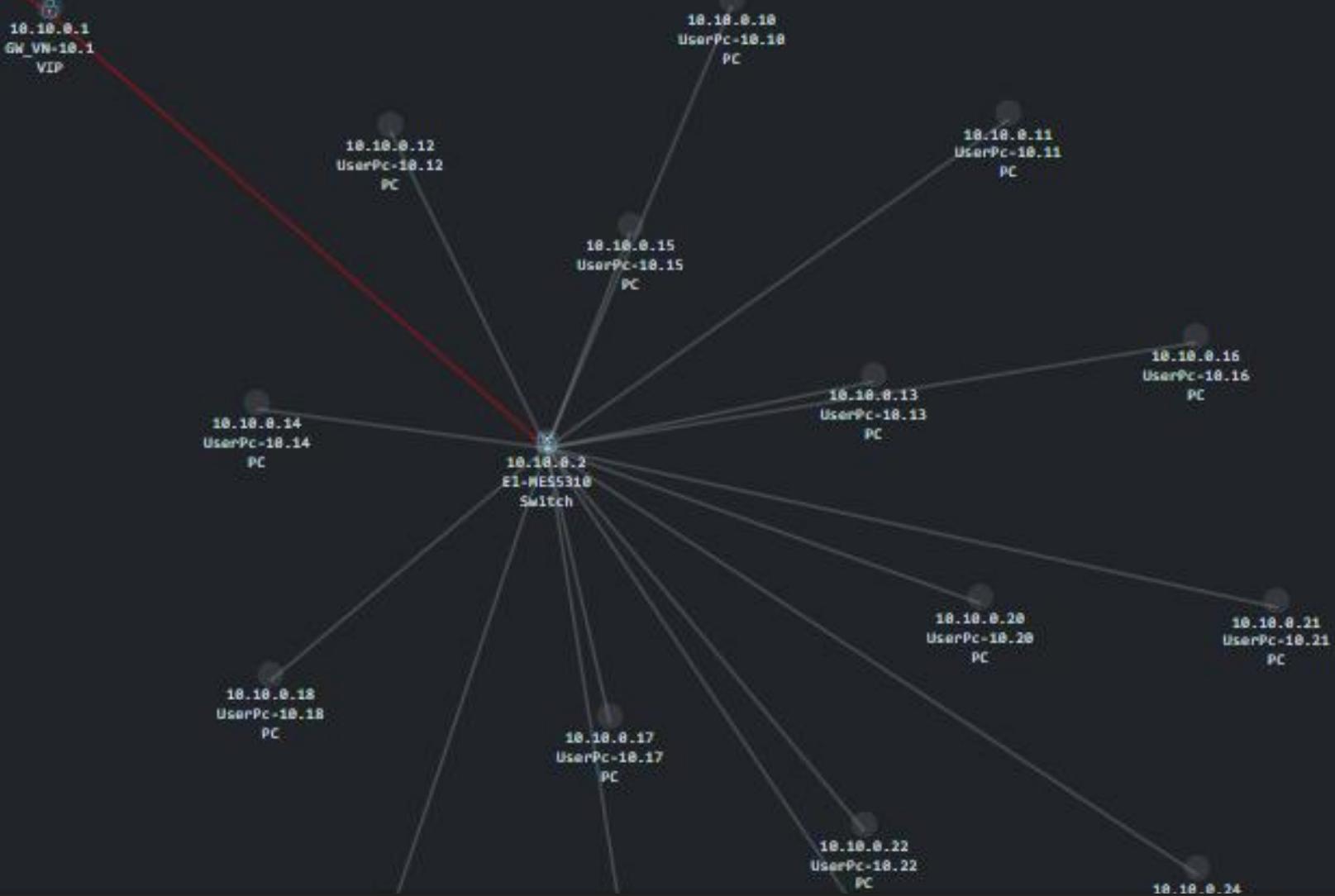
L2 топология → STP данные поступают с задержкой или не поступают вовсе
STP данные root bridge, изменения, блокировки портов

1.1.1
Cloudflare
Internet

. SYSLOG: смена топологии/ высокая нагрузка/ STP события

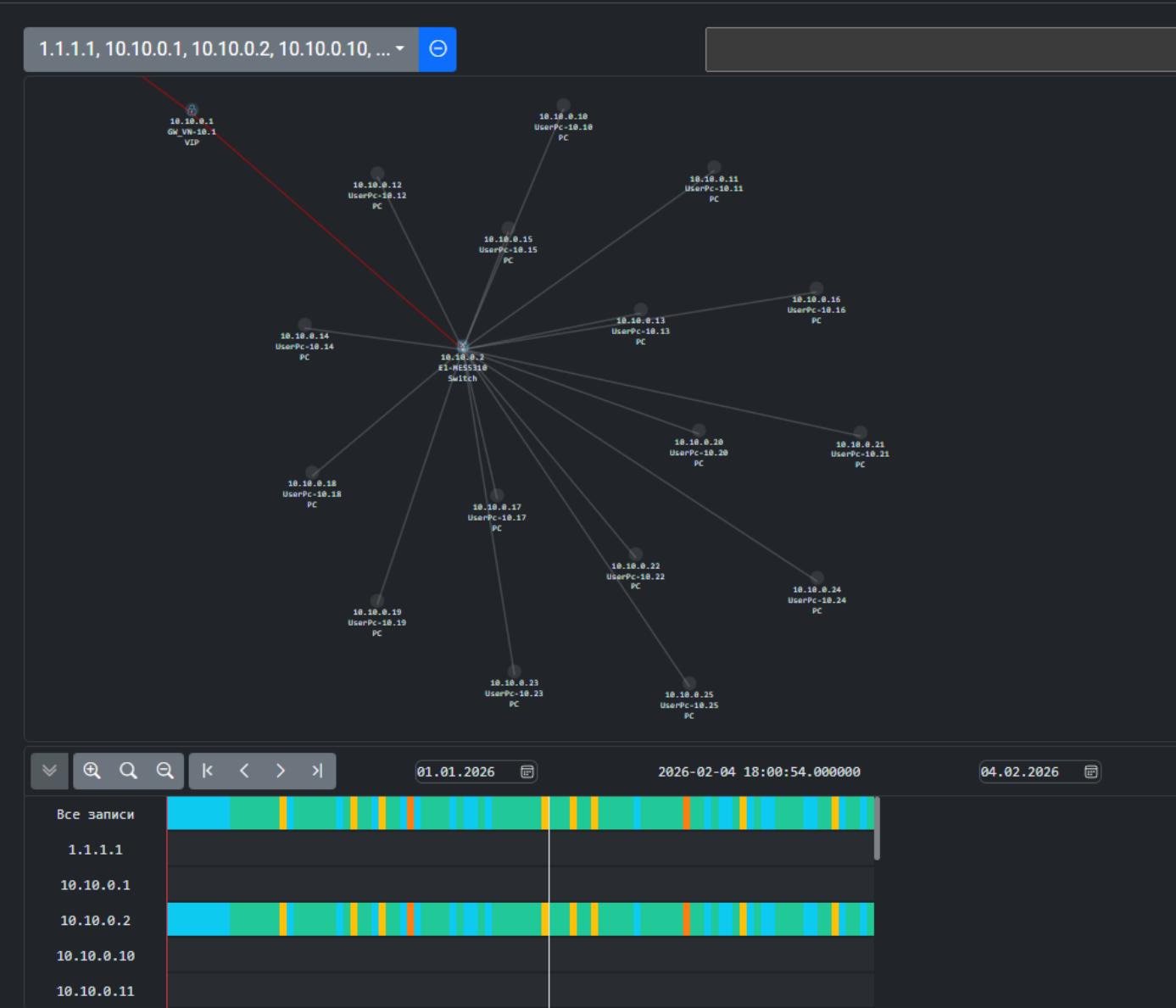
- 1. Превентивная защита: включить BPDU Guard на edge-портах
Смысλ: если кто-то воткнул "левый" свитч/петлю — порт сам уйдет в защиту, включить BPDU Guard / PortFast (если поддерживается)
- 2. Превентивная защита: storm-control (антиштурм по broadcast/multicast)
Смысλ: если начинается broadcast storm — сеть не умирает полностью.
- 3. Быстро "потушить пожар": выключить подозрительный порт
Смысλ: NOC/SOC увидели порт, где штурм → мгновенно вырубили.
- 4. Защита ядра: Root Guard на аплинках (чтобы никто не стал root)
Смысλ: "подключили свитч и он внезапно стал STP root" — классика аварий.
- 5. Задача - каждые N часов обновлять всю инфу - собирать STP/порты/таблицы" → раннее выявление изменений для реагирования и выработки подхода к решению.





Кейс 2 — Рост трафика, DDOS: лаги, DoS/перегрузка

Суть: временный всплеск нагрузки + хаос в маршрутизации/связности.



SYSLOG: “шторм” на контролльном коммутаторе L3

- 1. Включение rate-limit / storm-control (защита от флуда и “шумных клиентов”)
- 2. Отключение неиспользуемых портов (“Закрыть всё лишнее”: отключение неиспользуемых портов)
- 3. Включение нужных ACL/ограничений (**фильтрация трафика для мероприятия**):

3 показательных ACL-сценария:

Запрет управления сетью (SSH/Telnet/SNMP) из пользовательского VLAN

Разрешить только нужные сервисы наружу (например DNS/NTP/HTTP/HTTPS)

Антискан: запрет межклиентского общения внутри VLAN (частично)

Принцип:

“Один сценарий → применили к устройствам → однообразие конфигурации → готовность к повышению нагрузки, распределение нагрузки”.

Редактирование задачи

Case 2.1-2

Группы Устройства

Новая группа

Скрипт группы Новая группа

```
configure terminal
interface range ethernet 1/0/1-1/0/24
rate-limit input 10m
rate-limit output 50m
exit
write memory

configure terminal
interface range ethernet 1/0/1-1/0/24
broadcast suppression 2
exit
write memory|
```

Приоритет: Низкий Тип: Скрипт

Сохранить изменения Закрыть

Редактирование задачи

Case 2.2-1

Группы Устройства

Новая группа

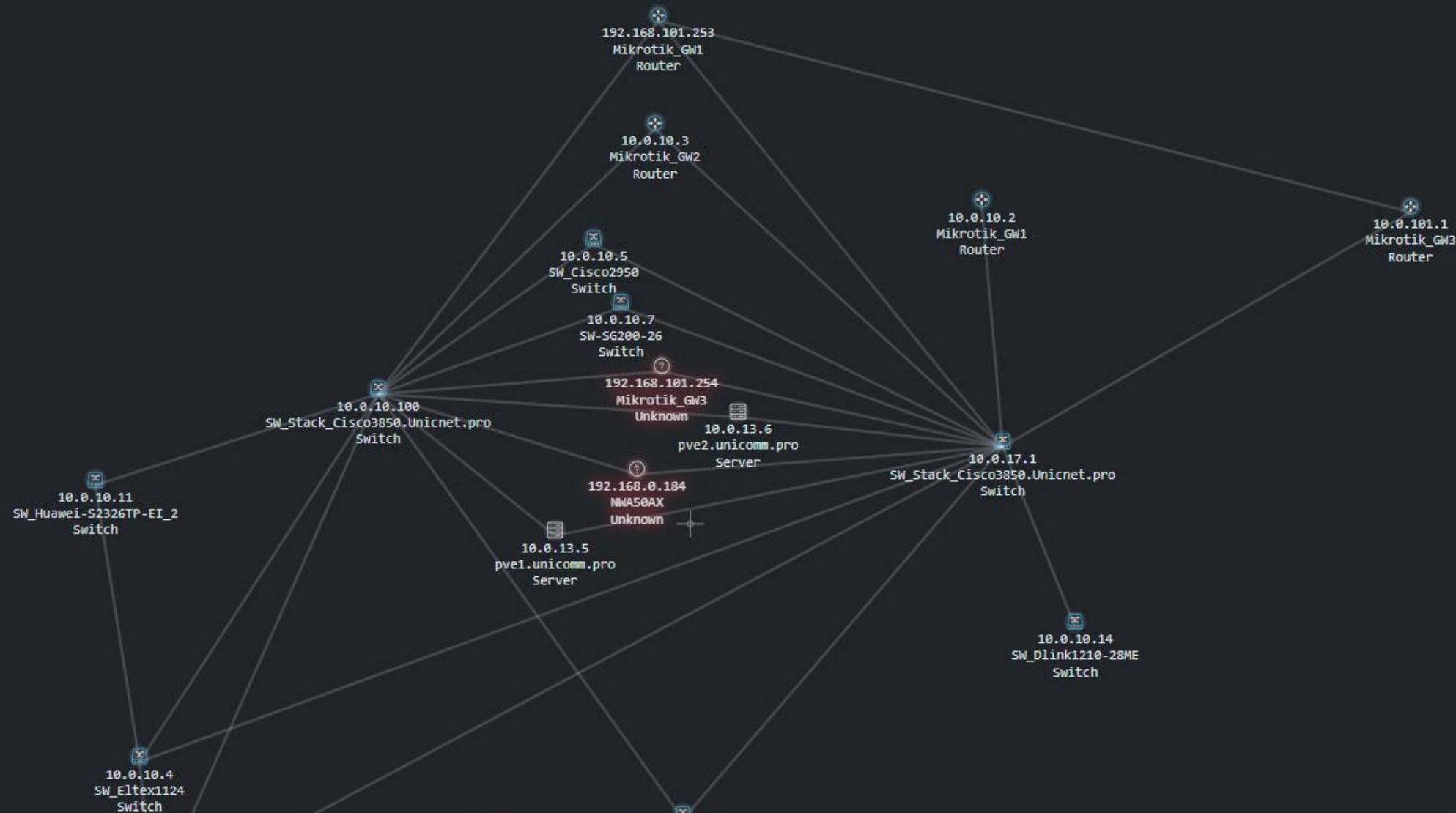
Скрипт группы Новая группа

```
configure terminal
interface range ethernet 1/0/13-1/0/46
shutdown
description UNUSED_EVENT_LOCKDOWN
exit
write memory

configure terminal
interface range ethernet 1/0/13-1/0/46
no shutdown
no description
exit
write memory|
```

Приоритет: Низкий Тип: Скрипт

Сохранить изменения Закрыть



Кейс 3 — Импортозамещение / горячая замена оборудования

Суть: меняем железо → неизвестно, что сломается: VLAN, маршруты, STP, соседство.

- Подготовка “миграционного чек-листа”:
 - какие порты должны быть trunk/access
 - какие VLAN должны быть разрешены
 - какие маршруты должны присутствовать
- Массовая команда: “привести конфигурацию к стандарту”
- Плановый сбор таблиц маршрутизации → контроль “не уехали ли next-hop”

Векторы кибератак



10.0.10.8	SW_HP-A3600-48	-	Hp	✓		02/03/2026		
10.0.10.9	SW_Huawei-S2326TP-EI_2	-	Huawei	⊕		02/03/2026		
10.0.10.10	SW_DLink-3420-52T	-	D-Link	✓		02/03/2026		
10.0.10.11	SW_Huawei-S2326TP-EI_2	-	Huawei	✗		02/03/2026		
10.0.10.12	SW_Juniper_EX2200	-	Juniper	⊕		02/03/2026		
10.0.10.13	R_Cisco_1841.unicnet.com	-	Cisco	✓		02/03/2026		
10.0.10.14	SW_Dlink1210-28ME	-	D-Link	⊕		02/03/2026		
10.0.10.17	FW_Fortigate-60C	-	Fortinet	⊕		02/03/2026		
10.0.10.100	🔥 SW_Stack_Cisco3850.Unicnet.pro	-	Cisco	⊕		02/03/2026		
10.0.17.1	10.0.17.1	-	Не указано	⊕		02/04/2026		
10.10.0.1	VPN GW_VN-10.1	-	VipNet	⊕		02/04/2026		
10.10.0.2	VPN El-MESS310	-	Eltex	⊕		02/04/2026		
10.10.0.10	VPN UserPc-10.10	-	LinuxPc	⊕		02/04/2026		
10.10.0.11	VPN UserPc-10.11	-	LinuxPc	⊕		02/04/2026		
10.10.0.12	VPN UserPc-10.12	-	LinuxPc	⊕		02/04/2026		
10.10.0.13	VPN UserPc-10.13	-	LinuxPc	⊕		02/04/2026		
10.10.0.14	VPN UserPc-10.14	-	LinuxPc	⊕		02/04/2026		
10.10.0.15	VPN UserPc-10.15	-	LinuxPc	⊕		02/04/2026		
10.10.0.16	VPN UserPc-10.16	-	LinuxPc	⊕		02/04/2026		
10.10.0.17	VPN UserPc-10.17	-	LinuxPc	⊕		02/04/2026		

Атака 1 — Внутренние и внешние атаки

Суть: подозрительная активность, изменения, странные подключения.

Дата	CON	OP	Все	Все	Содержимое	*	Все записи	10.0.10.8	10.0.10.10	10.0.10.12	10.0.10.14	10.0.10.100
2025.08.05 23:37:11	SSH	CON	10.0.10.100	MVinnikov			2025-08-05 14:00:21	10.0.10.100	%%STP-4-TOPLOGY: Topology change detected on VLAN 20			
2025.08.05 23:34:39	SSH	EXC	10.0.10.100	MVinnikov	exec backdoor		2025-08-05 14:00:22	10.0.10.100	%%IF-5-LINK_DOWN: Interface GE0/2 link down			
2025.08.05 22:56:36	TLN	DIS	10.0.10.14	MVinnikov			2025-08-05 14:00:23	10.0.10.100	%%DHCPO-3-POOL_EXHAUSTED: DHCP pool exhausted on VLAN20			
2025.08.05 22:25:56	TLN	DIS	10.0.10.100	MVinnikov			2025-08-05 14:00:24	10.0.10.100	%%SYS-4-WARN: Syslog rate high: 2500 msg/sec (possible storm)			
2025.08.05 21:30:29	TLN	CON	10.0.10.10	MVinnikov			2025-08-05 14:00:25	10.0.10.100	%%ARP-4-FLOOD: ARP request rate high on VLAN20 (pps=12000)			
2025.08.05 21:26:05	TLN	DIS	10.0.10.14	MVinnikov			2025-08-05 14:00:26	10.0.10.100	%%IF-5-STATE_DOWN: Interface GE0/2 changed state to down			
2025.08.05 21:24:09	TLN	EXC	10.0.10.14	MVinnikov	show ip		2025-08-05 14:00:27	10.0.10.100	%%ARP-4-FLOOD: ARP request rate high on VLAN20 (pps=8500)			
2025.08.05 21:22:18	SSH	EXC	10.0.10.100	AMaslenikov	show ip arp		2025-08-05 14:00:28	10.0.10.100	%%DHCPO-4-DECLINE: DHCP declined 192.168.20.111 (duplicate address detected)			
2025.08.05 21:18:41	TLN	DIS	10.0.10.10	MVinnikov			2025-08-05 14:00:29	10.0.10.100	%%IF-5-LINK_UP: Interface GE0/2 link up			
2025.08.05 21:12:07	SSH	CON	10.0.10.10	AMaslenikov			2025-08-05 14:00:30	10.0.10.100	%%FW-4-DROP: Firewall drop: src=10.20.15.44 dst=203.0.113.10 proto=TCP dpt=443 reason=rate-limit			
2025.08.05 20:45:49	SSH	DIS	10.0.10.10	MVinnikov			2025-08-05 14:00:31	10.0.10.100	%%SYS-4-WARN: Watchdog: system response slow			
2025.08.05 20:37:40	SSH	EXC	10.0.10.10	MVinnikov	exec backdoor		2025-08-05 14:00:32	10.0.10.100	%%OSPF-4-NEIGHBOR_UP: Neighbor 10.0.0.2 on GE0/0 state FULL			
2025.08.05 20:33:59	TLN	DIS	10.0.10.100	MVinnikov			2025-08-05 14:00:33	10.0.10.100	%%STP-5-TCN: TCN received from port GE0/10			
2025.08.05 20:33:01	TLN	DIS	10.0.10.10	AMaslenikov			2025-08-05 14:00:34	10.0.10.100	%%OSPF-4-NEIGHBOR_DOWN: Neighbor 10.0.0.2 on GE0/0 state FULL -> DOWN (Dead timer expired)			
2025.08.05 20:27:15	TLN	CON	10.0.10.14	AMaslenikov			2025-08-05 14:00:35	10.0.10.100	%%MGMT-4-SSH: SSH session from 192.168.20.50 timed out			
2025.08.05 20:21:08	TLN	EXC	10.0.10.100	MVinnikov	show arp		2025-08-05 14:00:36	10.0.10.100	%%ARP-4-FLOOD: ARP request rate high on VLAN20 (pps=12000)			
2025.08.05 20:06:56	TLN	EXC	10.0.10.100	AMaslenikov	conf t data		2025-08-05 14:00:37	10.0.10.100	%%CPU-3-HIGH: CPU utilization 97% (process=netstack)			
2025.08.05 20:00:36	SSH	EXC	10.0.10.10	AMaslenikov	show time		2025-08-05 14:00:38	10.0.10.100	%%IF-4-ERRORS: Interface GE0/1 input errors increased (crc=320, drops=5400)			
2025.08.05 19:54:55	SSH	DIS	10.0.10.10	AMaslenikov			2025-08-05 14:00:39	10.0.10.100	%%IF-5-LINK_DOWN: Interface GE0/2 link down			
2025.08.05 18:54:41	SSH	DIS	10.0.10.10	AMaslenikov			2025-08-05 14:00:40	10.0.10.100	%%STP-5-TCN: TCN received from port GE0/10			
2025.08.05 18:51:00	TLN	CON	10.0.10.10	AMaslenikov			2025-08-05 14:00:41	10.0.10.100	%%SYS-3-ERROR: Logging buffer overflow, messages dropped			
2025.08.05 18:49:45	TLN	EXC	10.0.10.14	MVinnikov	show ip arp							
2025.08.05 18:25:21	SSH	DIS	10.0.10.10	MVinnikov								
2025.08.05 18:04:08	TLN	EXC	10.0.10.100	MVinnikov	show int							
2025.08.05 17:58:07	TLN	DIS	10.0.10.10	MVinnikov								
2025.08.05 17:42:44	SSH	DIS	10.0.10.14	AMaslenikov								
2025.08.05 17:42:24	TLN	DIS	10.0.10.100	MVinnikov								
2025.08.05 17:41:43	SSH	DIS	10.0.10.14	AMaslenikov								
2025.08.05 17:17:48	SSH	DIS	10.0.10.100	AMaslenikov								

Показано записей 100 из 560

Показано записей 100 из 831

Сопоставление логов UnicNet и SYSLOG:

- “кто запускал команды, кто менял доступ/учетки”
- “что происходило на устройствах в это же время”



Атака 2 — Кража учетных данных устройств

Суть: злоумышленник получил доступ к SSH/Telnet/SNMP

Ролевая модель

Разделение:

- “оператор видит, но не может выполнять опасные команды”
- “админ может выполнять”
- Минимальные полномочия для всех

Текущие	User ID	Логин	Имя	E-Mail	Группы	Статус	Создано	🔍
Архив								
	06b83e043976	abramovaa	Alexey Abramov		1	✓	28.08.2025	🔗
	5ca1f8ebf831	admin			3	✓	05.02.2025	🔗
	458d81d8ef0b	adrinskyi	Test		2	✓	07.07.2025	🔗
	b4ae01b4aba0	amaslennikov	Александр Масленников	amaslennikov@unicomm.pro	3	✓	31.01.2025	🔗
	4ab98b77bfdd	mandreev	Max Andreev		2	✓	07.04.2025	🔗
	977f0310ae75	mvinnikov	Макс Винников	mixer57@gmail.com	4	✓	31.01.2025	🔗
	08f19334e9d7	norlov	Nikolay Orlov		3	✓	17.09.2025	🔗
	17672bc4c362	skonstantinov	Semen Konstantinov		2	✓	28.08.2025	🔗
	b46e6e909a8f	slavaqa	Вячеслав Тестович		1	✓	28.03.2025	🔗
	1b3459f9d205	ssarkisyan	Серго Саркисян		3	✓	04.02.2025	🔗
	f3cfb86ab85d	test123	test user	test123@test123.xyz	2	✗	10.07.2025	🔗
	68cf9a35535b	test321	test321 test321	test321@test.xyz	2	✗	14.07.2025	🔗

🏠 Главная 🚧 Права 📄 Учётные данные 🌐 Настройки

Владелец	Тип	♂	Порт	Название
— Добавить новую запись —								
unicnet_admin_group	SNMP v2	-	161	SNMP_V2	08/25/2025 / 08/28/2025			
unicnet_superuser_group	SNMP v2	-	161	SNMP_V2	08/25/2025			
unicnet_user_group	SNMP v2	-	161	SNMP_V2	08/25/2025			
unicnet_admin_group	SNMP v3	-	161	SNMP_V3	Unicnet	08/25/2025 / 08/28/2025		
unicnet_superuser_group	SNMP v3	-	161	SNMP_V3	Unicnet	08/25/2025		
unicnet_user_group	SNMP v3	-	161	SNMP_V3	Unicnet	08/25/2025		
unicnet_admin_group	SSH	-	22	SSH	UnicNet	08/25/2025 / 08/28/2025		
unicnet_superuser_group	SSH	-	22	SSH	UnicNet	08/25/2025 / 08/28/2025		
unicnet_user_group	SSH	-	22	SSH	UnicNet	08/25/2025 / 08/28/2025		
unicnet_admin_group	Telnet	-	23	TelnetAdm	UnicNet	08/25/2025 / 08/28/2025		
unicnet_superuser_group	Telnet	-	23	TelnetSup	UnicNet	08/25/2025 / 08/28/2025		
unicnet_user_group	Telnet	-	23	TelnetUsr	UnicNet	08/25/2025 / 08/28/2025		

- **Назначение наборов учетных данных группам пользователей**

Контроль:

- Нулевое доверие



Атака 3 — Кража учетных данных ПО

Суть: злоумышленник пытается использовать UnicNet как “панель управления сетью”.

- аудит действий в ПО кто запускал пакетные команды, когда, на какие устройства
- ограничение по группам и учеткам

Суть:

UnicNet не должен быть “супер-ключом от всего”, доступ должен быть сегментирован.

чётные данные  Настройки

Права

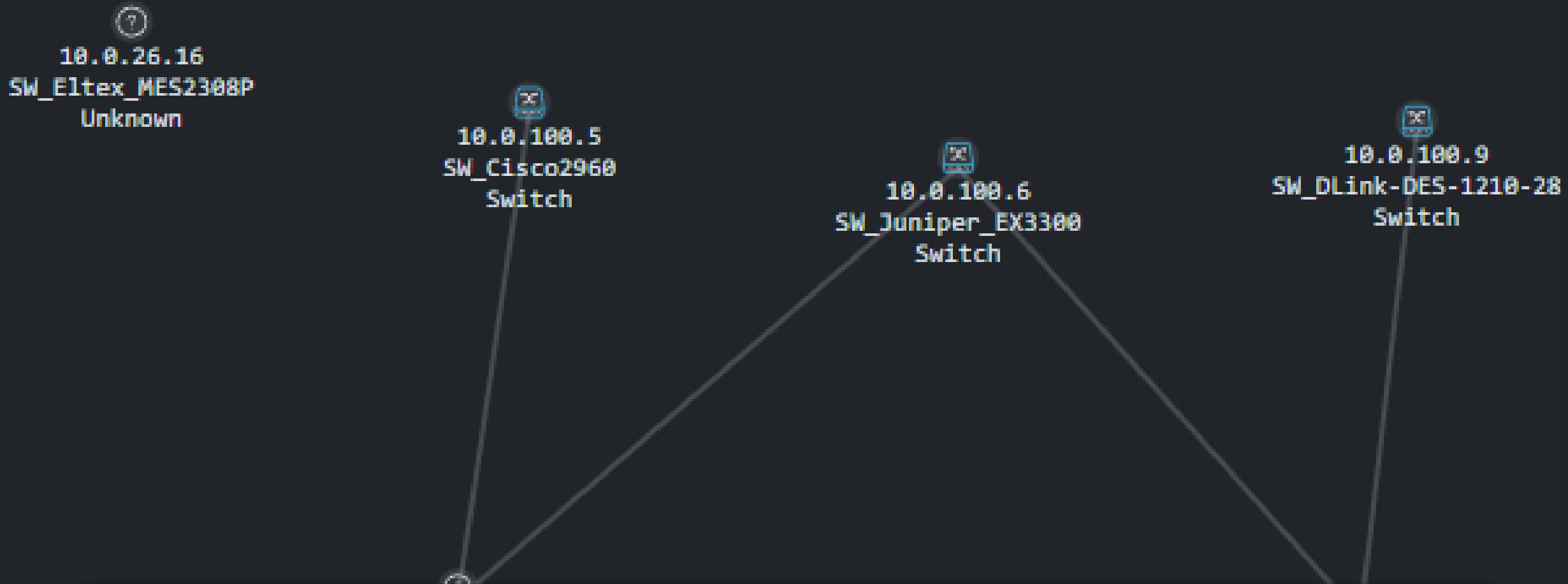
Edit User

X

Логин	UserID: ad59a855-26c7-4e7d-9bd9-b4ae01b4aba0
Логин	amaslennikov
Имя	Александр Масленников
Пароль	
E-Mail	amaslennikov@unicomm.pro
Группы	unicnet_admin_group  unicnet_superuser_group  unicnet_user_group 
Статус	
Создано	31.01.2025

test321 test321 test321 test321@test.xyz 2 

2025.08.05 12:52:23			10.0.10.14	MVinnikov
2025.08.05 12:49:36			10.0.10.14	AMaslennikov
2025.08.05 12:49:32			10.0.10.10	AMaslennikov
2025.08.05 12:44:56			10.0.10.100	AMaslennikov
2025.08.05 12:44:24			10.0.10.14	MVinnikov
2025.08.05 12:28:07			10.0.10.10	AMaslennikov
2025.08.05 12:12:18			10.0.10.14	AMaslennikov
2025.08.05 12:11:48			10.0.10.14	AMaslennikov
2025.08.05 11:55:29			10.0.10.100	AMaslennikov
2025.08.05 11:40:32			10.0.10.100	MVinnikov
2025.08.05 11:33:14			10.0.10.10	MVinnikov
2025.08.05 11:28:35			10.0.10.100	MVinnikov
2025.08.05 11:22:22			10.0.10.100	MVinnikov
2025.08.05 11:01:45			10.0.10.10	AMaslennikov
2025.08.05 10:52:37			10.0.10.100	AMaslennikov
2025.08.05 10:42:36			10.0.10.10	AMaslennikov
2025.08.05 10:33:30			10.0.10.100	AMaslennikov
2025.08.05 10:13:38			10.0.10.10	MVinnikov
2025.08.05 10:04:45			10.0.10.10	AMaslennikov
2025.08.05 09:53:03			10.0.10.100	AMaslennikov
2025.08.05 09:52:04			10.0.10.14	AMaslennikov
2025.08.05 09:45:52			10.0.10.100	MVinnikov
2025.08.05 09:37:04			10.0.10.14	MVinnikov
2025.08.05 09:34:38			10.0.10.14	MVinnikov
2025.08.05 09:18:48			10.0.10.100	AMaslennikov
2025.08.05 08:51:27			10.0.10.10	MVinnikov
2025.08.05 08:36:37			10.0.10.14	AMaslennikov
2025.08.05 08:32:28			10.0.10.100	MVinnikov
2025.08.05 08:28:14			10.0.10.10	AMaslennikov
2025.08.05 08:12:45			10.0.10.10	AMaslennikov
2025.08.05 08:09:34			10.0.10.14	AMaslennikov



Атака 4 — Скан сети и поиск неучтенного оборудования

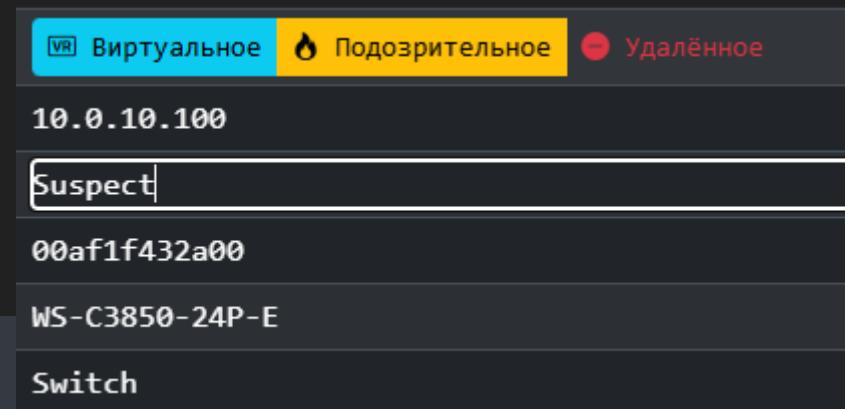
Суть: в сети появляются “левые” устройства: rogue switch, Wi-Fi, “серый” маршрутизатор.

- скан диапазона → найдено новое устройство
- ARP таблицы / MAC на порту → где физически сидит
- L2 топология → “новая ветка”
- теги:

- отметить как unknown
- переместить в группу “на проверку”

Решение

- пакетно отключить порт(ы) / перевести в quarantine VLAN
- создать регламент: “ежедневный скан + отчет по новым устройствам”



Редактирование задачи

SCAN 10.0.10.2-15+100

Приоритет: ! Критический
Тип: Дискаверинг
Режим: Обновить все

Начальный IP	Конечный IP-адрес	
+	0.0.0.0	
1 10.0.10.2	10.0.10.15	
2 10.0.10.100	10.0.10.100	
3 10.0.17.1	10.0.17.1	

Закрыть