



GIS
D A Y S

Сетевая безопасность - КОМАНДНАЯ РАБОТА

NAS, VPN, поведенческая аналитика

Сергей Никитин

Руководитель группы управления продуктами

ООО «Газинформсервис»

Немного статистики:



Кратный рост количества
APT-атак за последние 5 лет

MITRE

MITRE ATT&CK указывает
14 тактик и 240 техник кибератак

Актуально: как поломать NAC?

Инструментарий хакера

01

Сетевой хаб



02

Портативный PoE-инжектор



03

Специализированный ноутбук



Атака: ARP-spoofing aka ARP cache poisoning

MITRE

ID: T1557.002

Sub-technique of: T1557

① Tactics: Credential Access, Collection

① Platforms: Linux, Windows, macOS

Contributors: Jon Sternstein, Stern Security

Version: 1.1

Created: 15 October 2020

Last Modified: 22 July 2022

```

20, 12:56 PM net.sniff.mdns mdns 192.168.1.25 : PTR query for _airplay_tcp.local
20, 12:56 PM net.sniff.mdns mdns 192.168.1.25 : PTR query for _raop_tcp.local
20, 12:56 PM endpoint.new Detected 192.168.1.25 84:AD:8D:
20, 12:56 PM endpoint.lost Lost 192.168.1.25 84:AD:8D:
20, 12:56 PM mod.started arp.spoof
20, 12:56 PM sys.log WARNING: arp.spoof full duplex spoofing enabled, if the
20, 12:56 PM sys.log INFO: arp.spoof arp spoofer started, probing 3 targets.
    
```

36776	304.468178	Micro-St	84:ad:8d	ARP	60 192.168.1.92 is at d8:cb:8a
36825	304.473401	Micro-St	84:ad:8d	ARP	60 192.168.1.141 is at d8:cb:8a
37017	304.851396	30:24:32	84:ad:8d	ARP	60 192.168.1.161 is at 30:24:32
37435	305.554225	Micro-St	30:24:32	ARP	60 192.168.1.205 is at d8:cb:8a
37436	305.554328	30:24:32	Micro-St	ARP	60 192.168.1.161 is at 30:24:32
37437	305.554439	Micro-St	30:24:32	ARP	60 192.168.1.0 is at d8:cb:8a
37439	305.554640	Micro-St	30:24:32	ARP	60 192.168.1.1 is at d8:cb:8a
37440	305.554786	Micro-St	84:ad:8d	ARP	60 192.168.1.1 is at d8:cb:8a

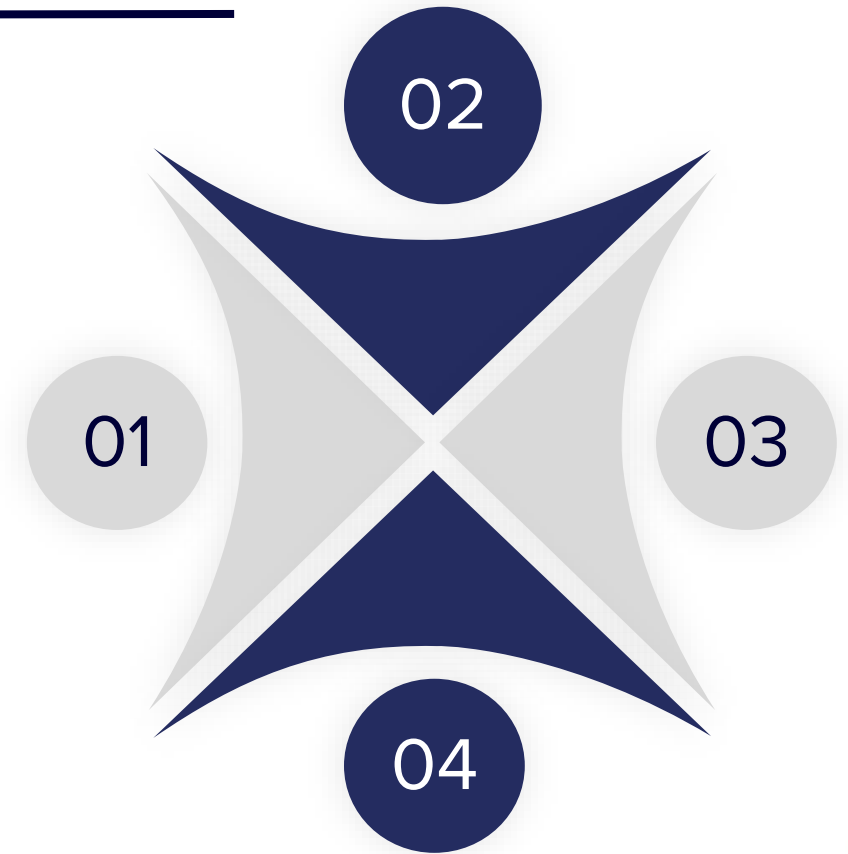
-▶
- «Угнали» пару IP+MAC,
 - Прошли аутентификацию,
 - Защита не обеспечена

Проблематика актуальна:

- 01  **Для интернета людей:** злоумышленник может устроиться в компанию под видом сотрудника
- 02  **Для интернета вещей:** можно подключиться в пару с IP-телефоном, IP-камерой, IP-датчиком и т. п.

Как решается с помощью **NAC** и...

- Правильных настроек **сегментации сети**
- **VPN-туннелей** с шифрованием
- Систем **поведенческой аналитики**



01

← Создание стандарта зонного анализа

Название: ZoneAnalyze_02_34

Описание: Описание

Использование: 3 профиля отчетов

Зоны: Z-tech-DMZ-01, users-admins, servers-main-02

Матрица доступа

Источник \ Назначение	Z-tech-DMZ-01	users-admins	servers-main-02
Z-tech-DMZ-01		Не учитывать	✓ Полное разрешение
users-admins	✗ Полный запрет		✓ Разрешено: TCP:22,24,133-333 UDP ICMP
servers-main-02	✓ Разрешено: TCP:22,24,133-333 UDP ICMP	✗ Запрещено: TCP/UDP TCP:22,24,133-333 UDP ICMP Протокол: 11-33	✓ Разрешено: TCP/UDP TCP:22,24,133-333, 445, 4446, 47... UDP ICMP Протокол: 11-33

Исключения:
Zone1 - Zone2, TCP:22,24,133-333
Zone2 - Zone3, Любой

Создать Отменить

версия 1.6.212.0 20221221.11

Z-tech-DMZ-01 - users-admins

Источник: Z-tech-DMZ-01

Назначение: users-admins

Описание: Описание

Тип доступа: Не учитывать, Запрет, Разрешение

Запрет: Полный, Частичный

Протокол / порт: Протокол

Остальные взаимодействия: Не учитывать, Полностью разрешены, Частично разрешены

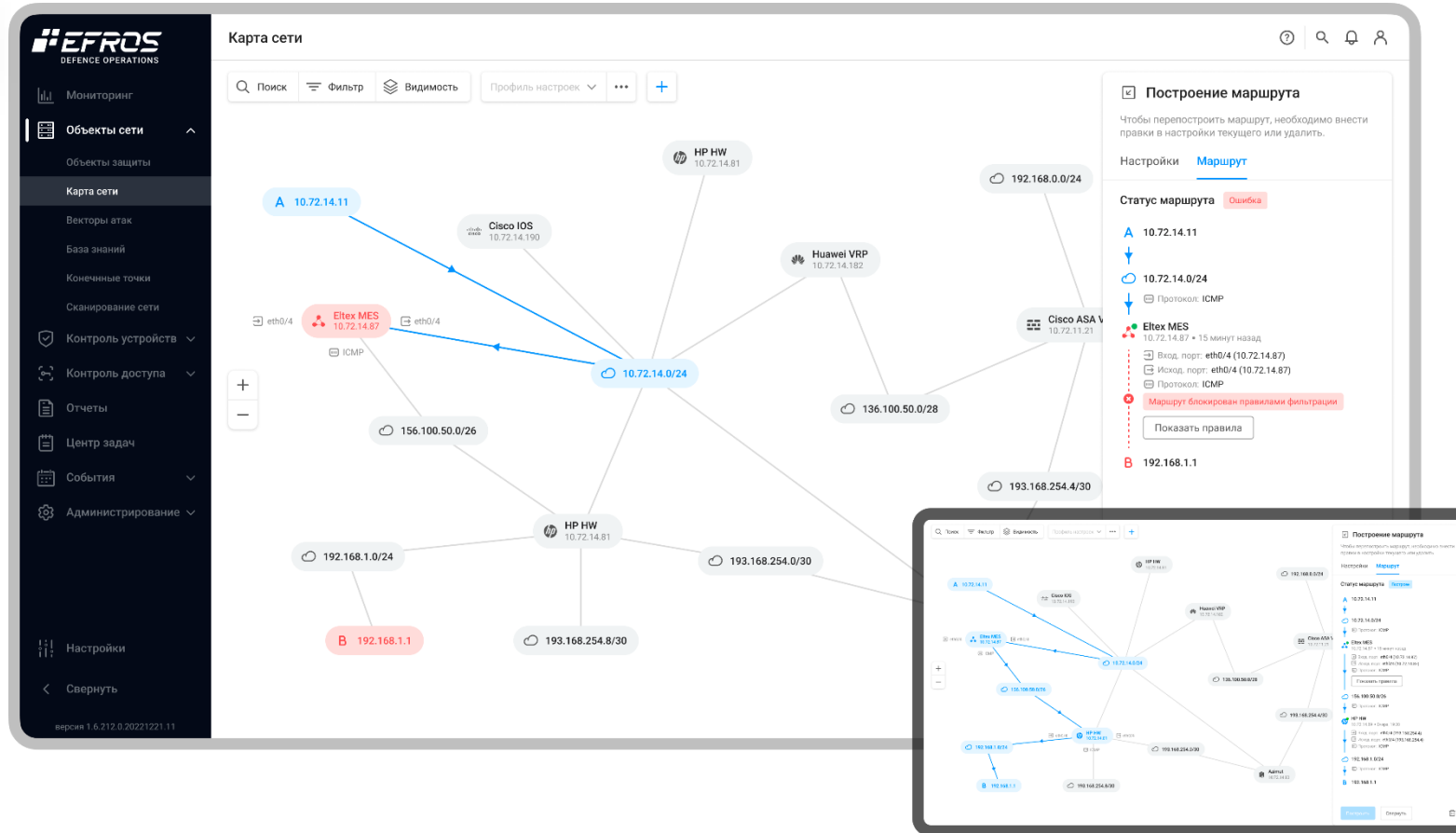
Исключения: Z-tech-DMZ-01, users-admins, Протокол

Удалить исключение

Добавить исключение

- Создание стандартов безопасности для сегментов сети
- Проверка соответствия правил доступа корпоративной политике

01



- Анализ связности и достижимости подсетей, выявление маршрутов распространения трафика включая VPN и NAT.
- Моделирование изменений сетевой инфраструктуры и оценка влияния вносимых изменений



02

The screenshot displays the EFRoS network management interface. On the left, a sidebar contains navigation options: Мониторинг, Объекты сети, Объекты защиты, База знаний, Карта сети, Векторы атак, Сканирование, Контроль устройств, Контроль доступа, Отчеты, События, and Администрирование. The main area shows a network map with various nodes and connections. A specific VPN tunnel configuration is highlighted, showing the path from an external IP (176.100.50.2) through an ASA firewall (10.72.11.21) to an internal IP (10.72.11.20). The NGate logo is prominently displayed in the center of the interface.

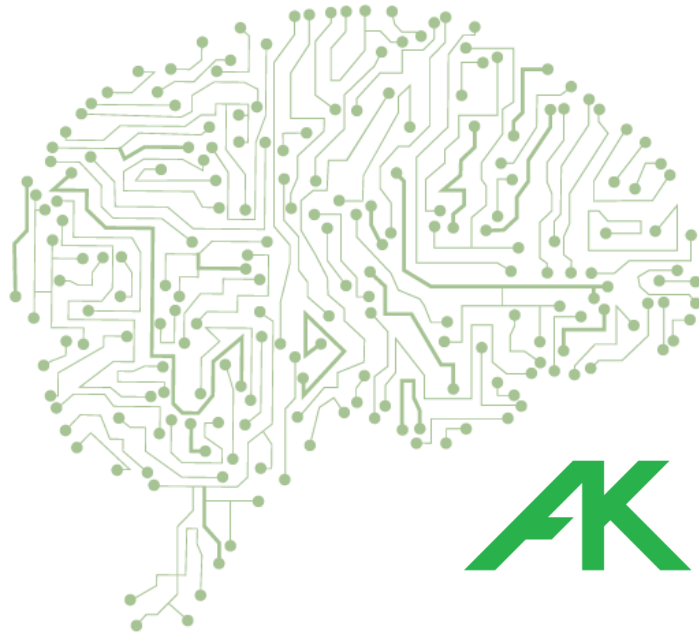
Пользователь подключается к корпоративной сети посредством VPN-шлюза N-Gate:

- формирование и отправка запроса на RADIUS-сервер Efros DO с целью аутентификации и авторизации пользователя.
- анализ полученного ответного значения RADIUS-атрибута и выбор соответствующего Access List.




Получение доступа только к определенным сегментам корпоративной сети, что соответствует правам доступа и принадлежности к доменной группе.

03

Выявления продолжения атаки
ARP-spoofing - задача **ASAP**



Ankey ASAP

-  аутентификация на нестандартном сервисе или нестандартным способом;
-  нетипичные команды при получении доступа;
-  нетипичное использование сетевых протоколов, ...

Аудит нетипичных действий на локальном хосте.

Партнеры

5 дистрибьюторов

60+ интеграторов

30+ технологических
партнеров





GIS
D A Y S

СПАСИБО ЗА ВНИМАНИЕ



www.gaz-is.ru

EFROS
DEFENCE OPERATIONS