



Netopia Firewall Compliance

Контроль конфигураций без спешки при ограниченных бюджетах

Подход «целевого инструмента», релевантный для отечественных решений

Традиции, шаблоны и ключевые установки при сокращенных бюджетах

Подход «целевого инструмента»:

- Определение своих ключевых задач, соотносимых с классом решений;
- Выбор приоритетных (первоочередных) задач для закрытия при тестировании и возможном дальнейшем приобретении;
- Тестирование (PoC – prove of concept) нескольких решений от разных производителей;
- Выбор финального варианта, опираясь на близость соответствия;
- По итогам эксплуатации с вендором согласуется возможное исполнение дополнительных задач;

Главный вопрос: КАКИЕ ЗАДАЧИ РЕШИМ?



Практическая польза от решения контроля конфигураций Netopia FC

Польза на основе базовых функций:

- Сокращение объема действующих правил, оптимизация ACLs
- Создание «матриц доступа» и контроль межсегментного доступа
- Оценка конфигураций по Best Practice вендоров и по собственным требованиям
- Топология и картография сетевых сегментов (маршруты + ACL)
- Оперативная оценка блокировки приложений и сервисов по цепочкам доступов
- Насыщение данными по уязвимостям (scanners) и построение «векторов атак»
- Разграничение представляемых данных между службами IT и ИБ (RBAC, заявки)

Пилот из сложной «гонки за всем и сразу» превращается во взвешенную оценку понятной и практической пользы от решения.

Отличительные свойства решения Netopia FC

 Fortigate

 Check Point

 Cisco IOS

 Generic

 Cisco ASA

 Cisco Nexus

 UserGate

 Континент

 Huawei NE

 Huawei USG

 ViPNet

 PT NGFW

 Eltex

 C-Teppe

 Ideco

На текущее время эксклюзивно:

- Поддержка Positive Technologies NGFW
- Поддержка Max Patrol и Max Patrol VM «из коробки»

Отличительные свойства решения Netopia FC

Прозрачность и управляемость параметрами ИБ-проверок конфигураций

Шаблон проверки



Сохранить

- ☒ Проверить наличие требуемых строк конфигурации
- ☐ Проверить наличие лишних строк конфигурации

Наименование проверки:

195. Настройка парольной политики



Введите строку для поиска

```
1 password-policy lifetime *
2 password-policy minimum-length 14
3 password-policy minimum-changes *
4 password-policy minimum-uppercase 1
5 password-policy minimum-numeric 1
6 password-policy minimum-special 1
```

Устройство

NL_ASA-NAT



Введите строку для поиска

```
4 : Serial Number: 9A9128L6WXC
5 : Hardware:  ASAv, 2048 MB RAM, CPU
6 :
7 ASA Version 9.18(2)
8 !
9 terminal width 511
10 hostname ASA-NAT
11 domain-name netopia.pro
12 enable password ***** pbkdf2
13 service-module 0 keepalive-timeout 4
14 service-module 0 keepalive-counter 6
15 names
```

Пример для Cisco ASA, параметры парольной политики

Отличительные свойства решения Netopia FC

Прозрачность и управляемость параметрами ИБ-проверок конфигураций

Шаблон проверки

Сохранить

☒ Проверить наличие требуемых строк конфигурации
☐ Проверить наличие лишних строк конфигурации

Наименование проверки:

229. Защита от DoS атак типа SYN - флуд

Введите строку для поиска

```
1 "zones": [  
2   "dos_profiles" : [  
3     {  
4       "enable": true  
5       "aggregate": true  
6       "alert-threshold": 100  
7       "drop-threshold": 250  
8       "excluded-ips": [  
9         *  
10      ],  
11      "kind": "syn"
```

Устройство

ug7

dos_profiles

```
2179 {  
2180   "antispoof_invert": false,  
2181   "cc": false,  
2182   "description": null,  
2183   "dos_profiles": [  
2184     {  
2185       "aggregate": false,  
2186       "alert_threshold": 3000,  
2187       "drop_threshold": 6000,  
2188       "enabled": false,  
2189       "excluded_ips": [],  
2190       "kind": "syn"  
2191     },  
2192     {  
2193       "aggregate": false,  
2194       "alert_threshold": 3000,  
2195       "drop_threshold": 6000,
```

Пример для UserGate, защита от SYN –flood пакетов

Отличительные свойства решения Netopia FC

Для дубликатов и перекрывающихся объектов есть отметка о присутствии в конфигурации

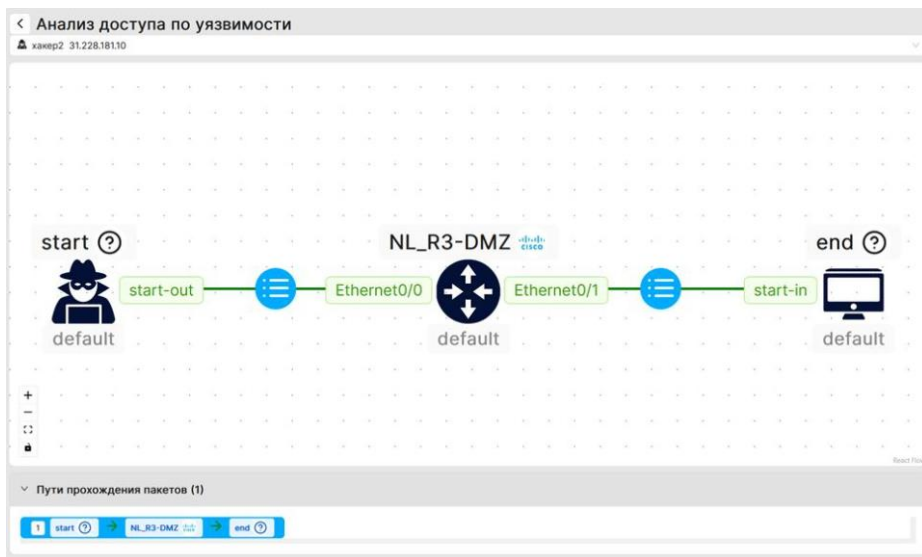
		Наименование	Тип объекта			Связанные правила		Устройство	Вендор
						NAT	SECURITY		
☒	group_obj_fbfe5b3-35da-4375-a1c1-5f8a8939036a IPRangeGroup	group_obj_fbfe5b3-35da-4375-a1c1-5f8a8939036a	IPRangeGroup			Нет связанных правил	Нет связанных правил	NL_ASA-NAT	Cisco ASA

Наименование	Тип объекта			Связанные правила		Устройство	Вендор
				NAT	SECURITY		
obj_66.6.16.242_66.6.16.242	IPRange			Нет связанных правил	dmz_access_in	- // -	- // -
obj_10.1.35.31_10.1.35.31	IPRange			Нет связанных правил	dmz_access_in	- // -	- // -

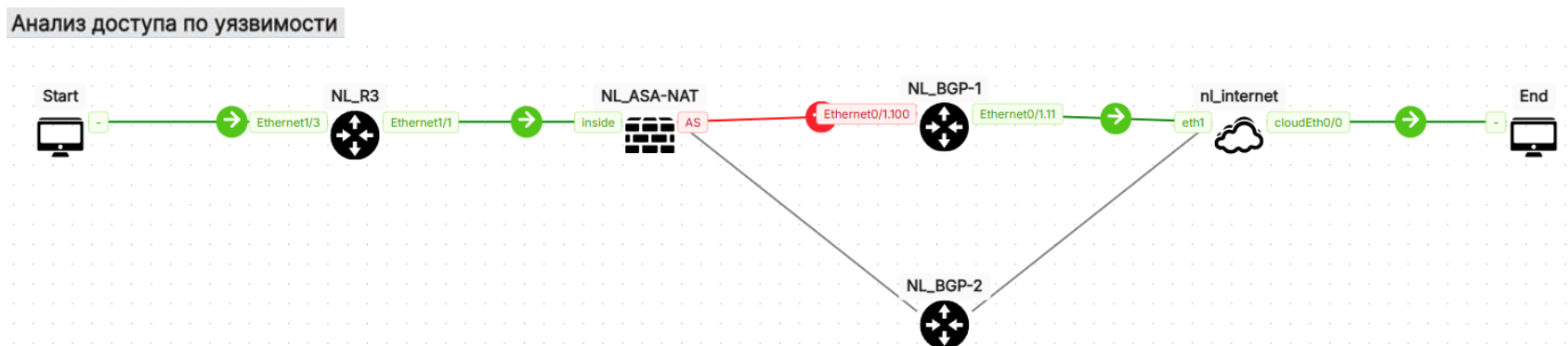
Моментально проверяется присутствие объекта во всех NAT и ACL-списках!

Отличительные свойства решения Netopia FC

Вектора атак и построение модели злоумышленника

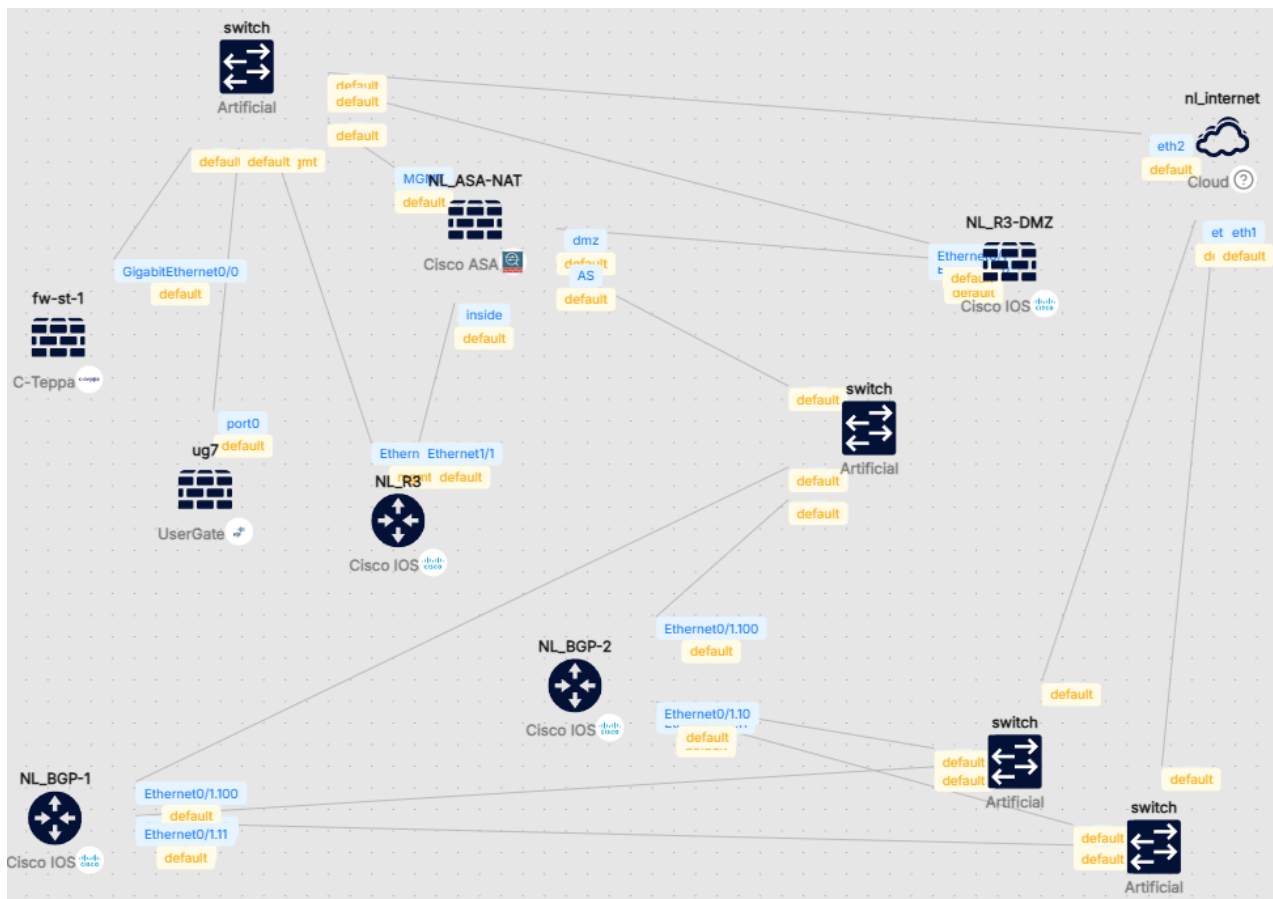


- Выгрузка данных по уязвимостям из Max Patrol / MP VM
- Классификация уязвимостей по BDU FSTEK, CVE/CPE, базам вендоров
- Построение модели злоумышленника (3 уровня хакера)
- Поиск множества связанных путей по топологии сети



Отличительные свойства решения Netopia FC

Топология и картография сети



- Для устройств МСЭ: учет маршрутов, NAT и ACLs
- Модель «слепков» текущих конфигураций (статика и динамика)
- Обновление данных по интервалам и syslog
- Формирование отдельных сохраняемых карт (по устройствам)
- Ожидается (2025) – поддержка VPN IPSec

Отличительные свойства решения Netopia FC

Текстовые и графические данные об изменениях доступов

<

Устройство: NL_ASA-NAT

Конфигурация

Таблица маршрутизации

↑

Различия версий конфигурации устройства

153	153	object network obj_10.5.35.0_24
154	154	subnet 10.5.36.0 255.255.255.0
155	155	object network 0.europe.pool.ntp.org-1
156	-	host 191.96.11.21
	156	+ subnet 191.96.11.0 255.255.255.0
157	157	object network 0.europe.pool.ntp.org-2
158	158	host 79.164.218.222
159	159	object network 0.europe.pool.ntp.org-3
		@@ -239,6 +239,18 @@
		@@ -301,7 +313,7 @@
301	313	access-group inside_access_in in interface inside
302	314	access-group as_access_in in interface AS
303	315	access-group dmz_access_in in interface dmz
304	-	access-group DC-KAZAN_access_in in interface DC-KAZAN
	316	+ access-group ONE-POLICY in interface DC-KAZAN
305	317	access-list MGMT_access_in extended permit ip user-group NETOPIA\\Analytics any any
306	318	access-list MGMT_access_in extended permit tcp object-group-user DM_INLINE_USER_1 any any eq ftp

Отличительные свойства решения Netopia FC

Текстовые и графические данные об изменениях доступов

Изменено (до)	3	inside_access_in	inside_access_in	⌵ any ⌵ any	⌵ obj_10.1.35.10 ⌵ any	[tcp:[25]]
Изменено (после)	3	inside_access_in	inside_access_in	⌵ any ⌵ any	⌵ obj_10.1.35.2 ⌵ obj_66.254.114.42	[udp:[53], tcp:[53]]
Изменено (до)	4	inside_access_in	inside_access_in	⌵ any ⌵ any	⌵ obj_10.1.35.0_24 ⌵ any	[tcp:[25]]
Изменено (после)	4	inside_access_in	inside_access_in	⌵ any ⌵ any	⌵ obj_10.1.35.2 ⌵ obj_66.254.114.41	[udp:[53], tcp:[53]]

Контакты

📍 Москва
115114, 1-й Дербеневский пер., 5 БЦ «Дербеневская Плаза»

📍 Санкт-Петербург
190000, Английская набережная, 70

📍 Казань
420107, Спартаковская, 23

+7 (495) 662 39 66

info@netwell.ru

netwell.ru

[Telegram-канал](#)

