

Применение методов формальной верификации для анализа правил фильтрации сетевого трафика

Дурнов Алексей Николаевич

Московский физико-технический институт
Физтех-школа радиотехники и компьютерных технологий
Кафедра инфокоммуникационных систем и сетей

Научный руководитель: к.ф-м.н. Ефанов Николай Николаевич

Консультант: Ларин Дмитрий Викторович

Москва, 2026 г.

Рост киберугроз

- Ежегодный рост числа кибератак на 20–30%
- Усложнение атак: АРТ, многовекторные атаки, атаки на уровне приложений

Средства защиты класса NGFW

- Next-Generation Firewall становится одним из ключевых элементов сетевой безопасности
- В России активно развивается рынок отечественных решений: Kaspersky, Positive Technologies, UserGate, Континент, Ideco и др.
- Оставшиеся зарубежные решения: Check Point, Fortinet, Palo Alto Networks и др.

Цена ошибки

- Ошибки конфигурации политики безопасности – одна из главных причин инцидентов ИБ
- Средний ущерб от утечки данных в России - 11.5 млн рублей

Цель:

Разработка системы автоматического анализа и верификации правил фильтрации сетевого трафика для выявления ошибок конфигурации

Задачи:

- ① Провести исследование существующих методов анализа правил фильтрации
- ② Разработать унифицированную вендоро-независимую модель представления правил различных форматов. Модель должна поддерживать отечественные решения
- ③ Выбрать и адаптировать методы формальной верификации для анализа правил
- ④ Реализовать алгоритмы обнаружения ошибок конфигурации в наборах правил
- ⑤ Разработать прототип системы анализа правил фильтрации
- ⑥ Провести тестирование на реальных конфигурациях

Политика сетевой безопасности в первую очередь определяется набором **правил фильтрации** сетевого трафика.

Основные классы правил фильтрации:

- ① **ACL** (Access Control List) – Cisco, Juniper, Huawei и др.
 - Анализ на уровне **L3-L4** (protocol, src/dst IP, src/dst port)
 - Небольшое количество дополнительных опций, простые сетевые объекты, наборы портов
 - **Линейный поиск** правил (first-match)
- ② **iptables** – Linux-системы, MikroTik
 - Анализ на уровне **L3-L4**
 - Дополнительные опции и простые объекты
 - Линейный поиск, но с **механизмом цепочек** (chains)
- ③ **Политики безопасности NGFW** – Kaspersky, Positive Technologies, Fortinet и др.
 - Анализ на уровне **L7** (приложения, сервисы, пользователи)
 - Богатый набор объектов: зоны, приложения и др.
 - Часто используется нелинейный поиск правил

- Приоритет правила
- Действие - allow/deny/chain/return
- Условие совпадения:
 - Сетевые объекты (wildcard-маски, диапазоны IP, Geo-IP, FQDN)
 - Пользователи (группы, профили, идентификаторы)
 - Зоны безопасности и тип правила для работы с зонами
 - Сервисы (наборы портов и протоколов)
 - Приложения (прикладной протокол, сервис или группа приложений)
- Расписания
- Групповой профиль безопасности - объединяющий профиль движков безопасности (IDPS, AV, DNS Security)
- Дополнительные данные (число срабатываний, время последнего срабатывания, время первого срабатывания и тд)

Правил:

- ! **Shadowing** – правило затенено, т.е. никогда не срабатывает
- ! **Redundancy** – избыточное правило
- ! **Generalization** – правило перекрывает более специфичное
- ! **Correlation** – частичное пересечение правил
- **Expired** – правило с истекшим сроком действия
- **Disabled** – правило отключено
- **Unused** – правило не используется

Объектов:

- **Unattached** – объект не привязан к правилу
- **Duplicate** – дублирующий объект
- **Unused within rule** – объект не используется с правилом

Критерий	Семантический анализ	Тестирование на трафике	Формальная верификация
Точность	Все типы ошибок	Не все логические ошибки	Все типы ошибок
Интерпретируемость	Легко	Может быть сложно	Легко
Требует реального трафика/исполнения	Нет	Да	Нет
Сложность	$O(n^2)$	Высокая (много тестов)	Обычно $O(n)$, в худшем случае $O(n^2)$
Проверка реального поведения	Нет	Да	Нет

Header Space Analysis - метод моделирования сети

- Каждый пакет представлен как точка в многомерном пространстве заголовков сетевого пакета: $\{0, 1\}^n$, где n - число битов в заголовке
- Для удобства вводят специальный символ wildcard x для обозначения любого бита
- На этом пространстве определены теоретико-множественные операции: пересечение, объединение, разность, дополнение и т.д.
- Правило фильтрации - это функция отображения в этом пространстве.

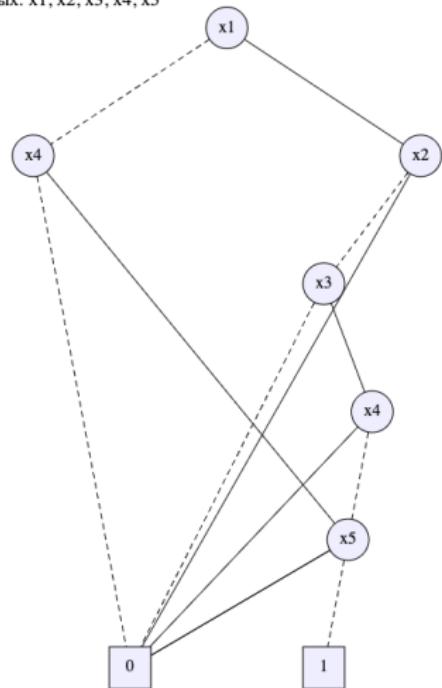
Множество пакетов P - это множество точек в пространстве заголовков, или объединение выражений с символами '0', '1' и 'x'. Это множество также можно задать с помощью булевой формулы.

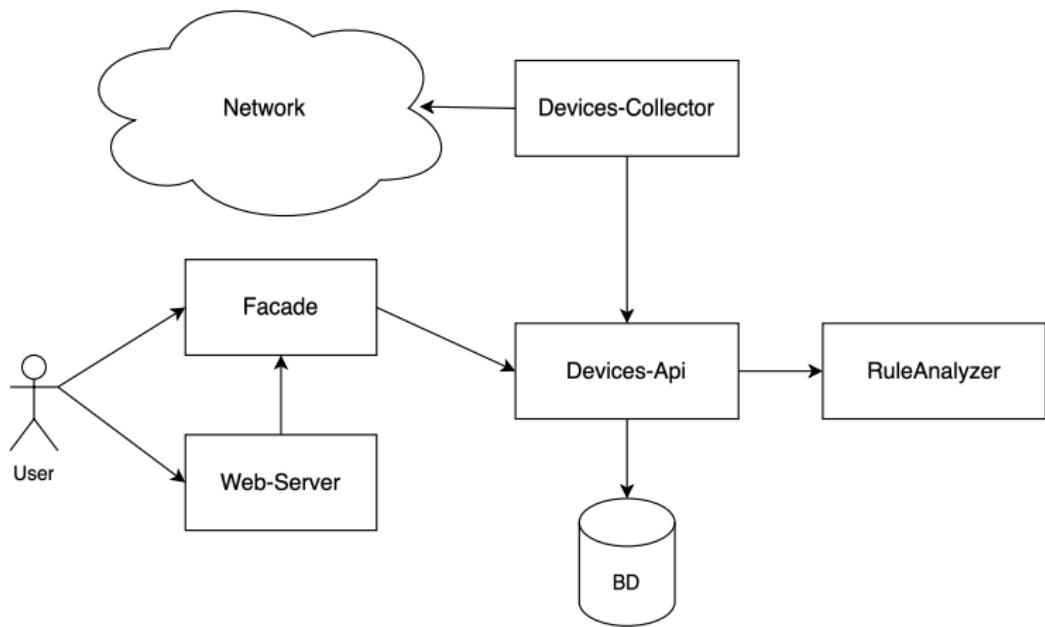
$$P = 0xx10 \cup 10100 \iff F(X) = (\neg x_1 \wedge x_4 \wedge \neg x_5) \vee (x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4 \wedge \neg x_5)$$

Binary Decision Diagrams (BDD)

- Компактное представление булевых функций
- Эффективные операции: пересечение, объединение, проверка эквивалентности

Формула: $(\neg x_1 \wedge x_4 \wedge \neg x_5) \vee (x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4 \wedge \neg x_5)$
Порядок переменных: x_1, x_2, x_3, x_4, x_5





Система анализа правил фильтрации

Hadal

17/07/2025, 11:43:19 17/07/2025 11:43:19 → 10/12/2025 13:24:14 ⏪ ⏴

Policy Analysis Hide Charts ▾

Rules Distribution



Total Rules: 1,068 (All rules across devices)

Rules for Audit: 84 (7.9% of total)

Total Objects: 245 (All objects across devices)

Objects for Audit: 34 (13.9% of total)

Objects Distribution



Unused within Rule

Duplicate

Unattached

Generalizing

Filters

Rule Types

- Normal
- Shadowed
- Redundant
- Generalizing
- Correlating
- Expired
- Disabled
- Unused

Apply Filter Clear Filters

Devices for Audit. List of all devices with selected rules and objects

HOSTNAME	MANAGEMENT IP	VENDOR	FAMILY	MODEL	VERSION	RULES FOR AUDIT	OBJECTS
cisco-router-01	192.168.1.1	Cisco	IOS XE	ISR 4331	16.09.05	Shadowed: 1 Redundant: 1 Generalizing: 1 Unused: 1	-
cisco-asa-02	192.168.2.1	Cisco	ASA OS	ASA 5516-X	9.14[1]	Shadowed: 1 Redundant: 1 Disabled: 1 Unused: 1	-
checkpoint-quantum-01	172.16.2.1	Check Point	Gaia	Quantum 6200	R81.10	Shadowed: 1 Redundant: 1 Expired: 1 Disabled: 1 Unused: 1	-
fortigate-100f	172.16.1.1	Fortinet	FortiOS	FortiGate 100F	7.2.2	Shadowed: 1 Redundant: 1 Expired: 1 Disabled: 1	-

Rows per page: 20 ▾ 1–10 of 10 < >

Система анализа правил фильтрации

17/07/2025, 11:43:19 17/07/2025 11:43:19 → 10/12/2025 13:24:14 ⏪ ⏴

Device Information

Hostname: cisco-router-01 IP: 192.168.1.1 Vendor: Cisco IOS XE Model: ISR 4331 Version: 16.09.05

Device Details		Rules & Objects		ACL-CORP-1		ACL-INSIDE-IN	
General		Objects		Only with recommendations 4 of 13		Custom	
General		Objects					
Configuration History		Network Objects (17)					
Raw Outputs		Transport Ports Groups (5)					
Policy Analysis		ACL-CORP-1					
Tables		INGRESS INTERFACES:		PRIORITY	ACTIVE	ACTION	RULE TYPE
Interfaces		GigabitEthernet0/0		10	✓	Deny	Universal
Managed IPv4 Addresses		GigabitEthernet0/1		20	✓	Deny	Universal
XDP Neighbors		EGRESS INTERFACES:		30	✓	Deny	Universal
STP VLANs		GigabitEthernet0/0		40	✓	Deny	Universal
Switchport		GigabitEthernet0/1		50	✓	Deny	Universal
VLANs		ACL-INSIDE-IN		60	✓	Deny	Universal
STP Virtual Ports		warning redundant		70	✓	Deny	Universal
MAC Table		ACL-OUTSIDE-IN		80	✓	Allow	Universal
ARP Entries		ACL-EXTENDED-101		90	✓	Allow	Universal
IPv4 Routing Table		ACL-STANDARD-10		100	✓	Allow	Universal
		ACL-OUTBOUND-OUT		110	✓	Allow	Universal
				120	✓	Allow	Universal
				130	✓	Deny	Universal

Выполнено:

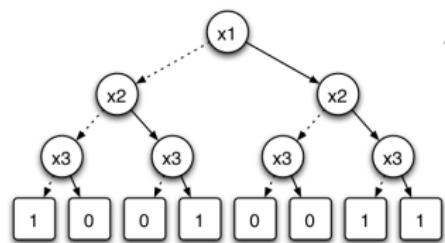
- Проведён анализ существующих методов верификации правил фильтрации
- Разработана унифицированная модель представления правил
- Выбран и адаптирован метод на основе BDD для анализа конфликтов
- Реализованы алгоритмы обнаружения основных типов аномалий
- Разработан прототип системы анализа

Практическая значимость:

- Снижение рисков мисконфигурации сетевых устройств
- Автоматизация аудита политик безопасности
- Поддержка мультивендорной инфраструктуры, в том числе и отечественных решений

- Оптимизация работы алгоритма для больших наборов правил (>100'000 правил)
- Автоматическая оптимизация наборов с помощью анализа достижимости на модели сети
- Интеграция с системами управления политиками (policy orchestration)

Спасибо за внимание!



x_1	x_2	x_3	f
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

