



Исследование компилятора clang в составе Ideco NGFW

Заглядывая за грань требований

Коренберг Марк Михайлович
Технический директор ООО «Айдеко»

О компании Ideco



Ideco — российский разработчик решений для защиты корпоративных сетей от кибератак и фильтрации трафика.

2005 год основания

5500+ компаний-заказчиков

250+ сотрудников в команде

3 мажорных релиза каждый год

Соответствие требованиям регулятора

Сертификат ФСТЭК №4503 от 28.12.2021 г.

- + Требования доверия (4)
- + Требования к МЭ
- + Требования к СОВ
- + Профиль защиты МЭ (А 4-го класса защиты ИТ.МЭ.А4. ПЗ)
- + Профиль защиты МЭ (Б 4-го класса защиты ИТ.МЭ.Б4. ПЗ)
- + Профиль защиты СОВ (4-го класса защиты ИТ.СОВ.С4. ПЗ)

Сертификат ФСБ

Ведем работы
по сертификации ГОСТ VPN

Решение входит
в реестр российского ПО
Минцифры РФ

Линейка сертифицированных аппаратных платформ



Высокопроизводительные платформы для бизнеса любого масштаба.



Ideco SX+ ФСТЭК

до 100 активных
пользователей интернет



Ideco LX ФСТЭК

от 300 до 1000 активных
пользователей интернет



Ideco EX ФСТЭК

для крупных компаний, дата-центров
и высоконагруженных сетей

Архитектура Ideco NGFW VPP

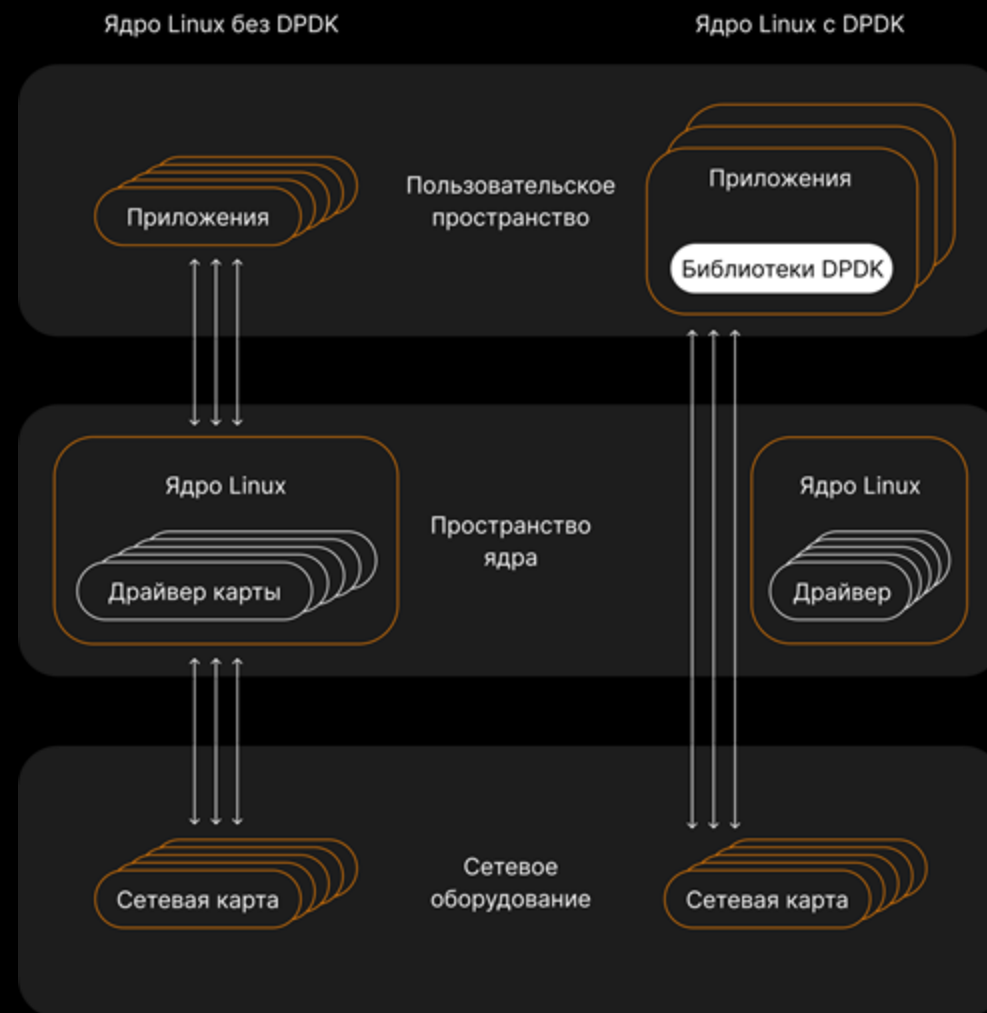


- + Linux 6.x;
- + Vector Packet Processing platform;
- + Userspace.

Архитектура Ideco NGFW VPP оптимальна для быстрого развития стабильного и производительного продукта.

Она позволяет:

- + перейти с последовательной обработки пакетов к параллельной;
- + эффективно утилизировать многоядерные процессоры;
- + работать с десятками тысяч правил и политик;
- + получить ускорение за счет аппаратных возможностей CPU и сетевых карт.



Компилируемый фаервол



Dev

Название: Без названия 23000007...

Панель мониторинга

Пользователи

Мониторинг

Правила трафика

Фаервол

Ограничение скорости

Предотвращение вторжений

Объекты

Профили безопасности

Контроль приложений

Предотвращение вторжений

Контент-фильтр

TLS/SSL-инспекция

Сервисы

Отчёты и журналы

Управление сервером

Инженерная панель

Фаервол

Работает

Создать бэкап

FORWARD

DNAT

INPUT

SNAT

+ Добавить

Фильтры

Отображение

Поиск

Название	Протокол	Источник		Назначение		Действие	Время действия	Профили безопа...	Комментарий	Управление					
		Адрес	Порты	Адрес	Порты										
разреш. началь...	TCP	192.168.0.0...	* Любой	172.16.0.0/...	* Любой	Разрешить	* Любой	-							
расшифровка	TCP	* Любой	* Любой	* Любой	* Любой	Разрешить	* Любой	test pro...							
Правило по умо...	* Любой	* Любой	* Любой	* Любой	* Любой	Запретить	* Любой	-	Правило по						

1 строка выбрана

Строк на странице: 100 1-3 из 3



gcc/SECURITY.txt



Compiling untrusted sources can result in arbitrary code execution and unconstrained resource consumption in the compiler. As a result, compilation of such code should be done inside a sandboxed environment to ensure that it does not compromise the host environment.

Модификация компилятора Clang



вес меньше на **83%**

Стандартный пакет Clang для Fedora 39 занимает 536 мегабайт на диске. Сокращенный пакет Clang занимает 91 мегабайт.

быстрее на **25%**

Дополнительным результатом стало ускорение компилятора. Тестирование оригинального компилятора с использованием полного набора тестов llvm-lit занимает 26.82 секунд, в то время как модифицированный Clang тестируется за 19.98 секунд.

##	system clang	minimized clang
# 50 rules		
task-clock:u,msec	1,885.17	1,772.47
page-faults:u	22,616	17,225
cycles:u	4,086,991,141	3,876,692,759
instructions:u	3,308,537,300	3,151,656,140
branches:u	628,559,978	605,888,596
branch-misses:u	13,669,351	13,431,089
# 100 rules		
task-clock:u,msec	2,072.36	1,953.07
page-faults:u	23,109	17,722
cycles:u	4,512,246,026	4,208,287,221
instructions:u	3,910,559,990	3,739,260,591
branches:u	746,460,521	722,407,287
branch-misses:u	16,160,156	15,903,207
# 500 rules		
task-clock:u,msec	2,818.43	2,696.09
page-faults:u	28,419	22,988
cycles:u	6,187,706,025	5,957,729,245
instructions:u	6,304,356,638	6,083,309,728
branches:u	1,208,835,544	1,180,488,457
branch-misses:u	23,103,854	23,160,918

# 1000 rules		
task-clock:u,msec	4,297.51	4,129.53
page-faults:u	37,853	32,556
cycles:u	9,515,906,117	9,181,346,471
instructions:u	10,850,001,664	10,554,816,677
branches:u	2,095,999,133	2,061,517,726
branch-misses:u	40,134,331	39,517,168
# 5000 rules		
task-clock:u,msec	27,377.00	26,818.44
page-faults:u	113,768	107,271
cycles:u	61,877,112,647	60,665,706,582
instructions:u	69,317,970,419	68,439,013,289
branches:u	13,694,140,192	13,608,305,308
branch-misses:u	280,977,496	280,021,954
# 10000 rules		
task-clock:u,msec	82,735.14	82,197.12
page-faults:u	230,719	224,981
cycles:u	187,998,859,985	186,845,729,337
instructions:u	202,837,019,424	201,712,677,526
branches:u	40,479,352,603	40,411,265,526
branch-misses:u	877,315,709	883,140,252

Изоляция процесса компиляции



Реализована изоляция процесса компиляции, позволяющая ограничить доступ компилятора к следующим ресурсам:

системные вызовы

файловая система

сеть

оперативная память

процессорное время



Коренберг Марк Михайлович
Технический директор ООО «Айдеко»

e-mail: mmarkk@ideco.ru
tg: @socketpair

