Как выбрать корпоративный межсетевой экран? Обзор рынка и результаты сравнения

Илья Шабанов
Генеральный директор
Anti-Malware.ru

Определимся с терминами

Многие ли понимают разницу?

- NGFW (Next Generation Firewall)
- UTM (Unified Threat Management)
- USG (Unified Security Gateway)
- Enterprise Firewall

Что такое NGFW?

Что отличает NGFW:

- DPI (Deep Packet Inspection)
- Для настройки МЭ не нужно знать протоколы и порты
- Правила МЭ на уровне приложений (L7 в сетевой модели OSI)
- «Все в одном» (прокси, антивирус, антиспам, веб-фильтрация, DLP и тд)

+ все это должно работать на больших скоростях

Если ваш МЭ это не умеет, то он не NGFW

Ключевые функции UTM/NGFW

- Межсетевой экран и контроль приложений
- Система обнаружения/предотвращения вторжений
- Антивирусная защита
- Антибот-защита
- Антиспам
- Веб-фильтрация
- Обнаружение утечек информации (DLP)
- Sandbox и Threat Intelligence
- Защита от DDoS-атак
- Прокси
- IPSec VPN и SSL VPN

Российский рынок NGFW

Source: Gartner (September 2019)

UserGate

Код Безопасности

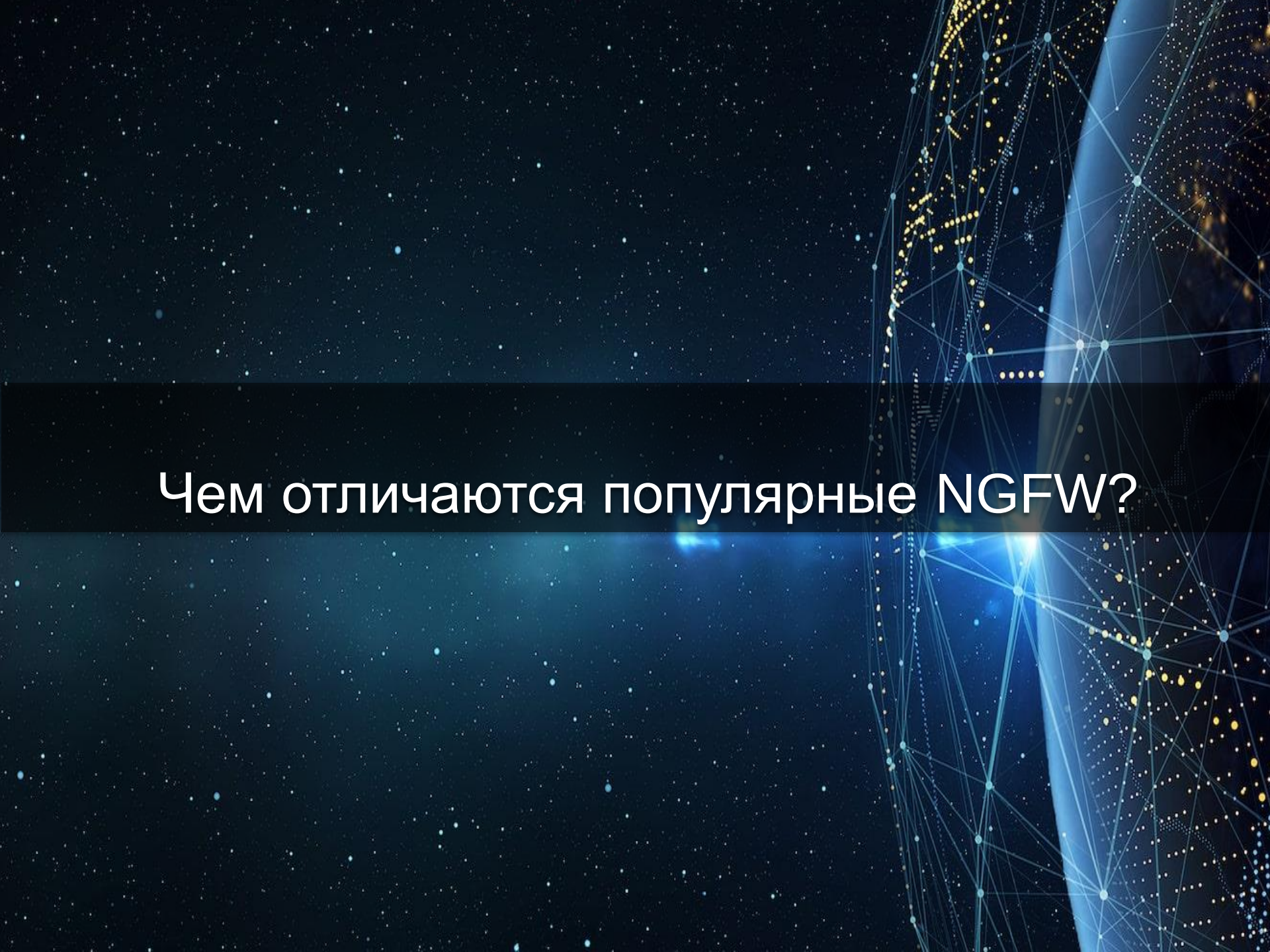
infotecs

ideco

SMART-SOFT

интернет контроль сервер

TCC


Чем отличаются популярные NGFW?

Первое публичное сравнение

- Cisco Firepower
- Check Point Security Gateway
- Fortinet FortiGate
- Huawei USG
- Palo Alto Networks NGFW

Импортозаместители:

- Континент («Код Безопасности»)
- UserGate («Юзергейт»)

Опубликовано в сентябре 2019 на www.anti-malware.ru

Первое публичное сравнение

7 продуктов, более 160 критериев

- Архитектура решений
- Поддержка сетевых сервисов
- Основные функции безопасности NGFW
- Создание виртуальных частных сетей VPN
- Функции прокси-сервера
- Аутентификация
- Высокая доступность и кластеризация
- Централизованное управления
- Мониторинг работы и отчетность
- Возможности интеграции
- Техническая поддержка
- Лицензирование

Параметр сравнения	Cisco	Check Point	Fortinet	Huawei	Palo Alto Networks	Код Безопасност
Компания	Cisco Systems Inc.	Check Point Software Technologies Ltd.	Fortinet	HUAWEI	Palo Alto Networks	ООО «Код Безопасности»
Веб-сайт	cisco.com	checkpoint.com	fortinet.com	huawei.com	paloaltonetworks.com	securitycode.ru
Штаб-квартира	Сан-Хосе, США	Тель-Авив, Израиль	Саннивейл, США	Шэньчжэнь, Китай	Саннивейл, США	Москва, Россия
Полное название системы	Межсетевые экраны нового поколения Cisco Firepower	Программный комплекс сетевой безопасности нового поколения Check Point Software Technologies	Межсетевой экран следующего поколения FortiGate	Межсетевые экраны нового поколения Huawei	Palo Alto Networks Next Generation Firewall	"Континент" 4.0
Сравниваемая линейка продуктов (модели, версии ОС)	Серия Cisco Firepower (1010, 1100, 2100, 4100, 9300) на FTD OS 6.4	Серия Check Point Secure Gateways и Check Point Sandblast Network на R80.20	Серия FortiGate на FortiOS 6.0 (от FG-30D до FG-5001)	Huawei USG v5 (6320, 6330, 6350, 6360, 6370, 6380, 6390, 6620, 6630, 6650, 6660, 6670, 6680, 9560, 9580)	Серия Palo Alto Networks на PAN-OS 9.0.2 (аппаратные NGFW от PA-220 до PA-7080 и виртуальных от VM-50 до VM-700)	Континент 4.0.3 (IP 10, IPC-25, IPC-50, 100, IPC-500, IPC-5 IPC-600, IPC-800F, 1000F, IPC-3000F, I 3000FC, IPC-1000N IPC-3000NF2)
Целевой сегмент	Малый, средний и крупный бизнес, государственный и коммерческий сектор	Малый, средний и крупный бизнес, государственный и коммерческий сектор	Малый, средний и крупный бизнес, государственный и коммерческий сектор	Малый, средний и крупный бизнес, государственный и коммерческий сектор	Средний и крупный бизнес, государственный и коммерческий сектор	Малый, средний и крупный бизнес, государственный и коммерческий сект
Сертификаты	Сертификат ФСТЭК России №3973 со сроком действия до 25.07.2021 на межсетевой экран серии Cisco ASA 5500-X (ASA 5506-X, ASA 5508-X, ASA 5516-X) с установленным программным обеспечением Cisco ASA версии 9.x , профиль защиты МЭ по новым требованиям (А шестого класса защиты. ИТ.МЭ.А6.ПЗ, Б шестого класса защиты. ИТ.МЭ.Б6.ПЗ). В процессе	Сертификат ФСТЭК России №3634, срок действия до 03.10.2019, на R77.10 для МЭ и СОВ по новым требованиям; Положительное заключение ФСТЭК для R77.30 (шлюзы, песочницы, в планах - агенты).	Сертификат ФСТЭК России №3720 со сроком действия до 16.03.2020 на FortiGate под управлением FortiOS 5.x, профили защиты СОВ (сети четвертого класса защиты, ИТ.СОВ.С4.ПЗ), профиль защиты МЭ (А четвертого класса защиты ИТ.МЭ.А4.ПЗ, Б четвертого класса защиты ИТ.МЭ.Б4.ПЗ).	Сертификат ФСТЭК №4083, срок действия до 04.02.2024, на версию V500, профиль защиты МЭ по новым требованиям (А четвертого класса защиты ИТ.МЭ.А4.ПЗ, Б четвертого класса защиты ИТ.МЭ.Б4.ПЗ).	Нет	Планируется получение сертификатов: ФСТЭК по требова к межсетевым экра тип "А" 4-го класс СОВ уровня сети 4 класса, ФСБ на СКЗИ кла КС3

«Сравнение NGFW», Anti-Malware.ru, 2019

* Вторая часть сравнения

- Juniper Networks SRX
- Forcepoint NGFW

Импортозаместители:

- Ideco ICS
- ViPNet xFirewall («ИнфоТеКС»)
- Traffic Inspector NG («Смарт Софт»)
- Интернет Контроль Сервер (ИКС от «А-Реал»)
- Diamond VPN/FW (ТСС)

* Ожидается в ноябре 2019 на www.anti-malware.ru

Сертификация ФСТЭК

- Huawei – МЭ (4-й класс, профиль А и Б) до 04.02.2024
- UserGate – МЭ (4-й класс, профили А и Б) и СОВ (4-й класс) до 26.03.2021

- Континент 4 и Cisco Firepower в процессе сертификации
- Check Point на R77.10 – истек в октябре 2019
- Fortinet на FortiOS 5.x – истекает в марте 2020
- Cisco на ASA 5500-X – истекает 2021 году

На что смотреть при выборе?

- Какие функции реально будут использоваться
  - Межсетевой экран + IDS
  - Антивирус
  - Песочница
  - Веб-фильтрация
  - Прокси
- Наличие сертификата ФСТЭК, если необходим
- Масштабируемость и аппаратное ускорение
- Возможности управления и отчетности

Это значительно сократит выбор оптимальной системы

Что есть не у всех?

- ГОСТ SSL VPN и IPsec VPN
- Раскрытие TLS 1.3
- Поддержка SD WAN
- Режим зеркалирования SSL во внешнюю систему по SPAN
- Поддержка ICAP для передачи трафика во внешние системы
- Функции прокси
- Встроенный DLP и антиспам
- Аппаратное ускорение (SPU, FPGA, ASIC и тд)

Итоги сравнения

- ТОП-5 зарубежных лидеров практически идентичны по набору функций
- Имеют значения детали (ГОСТ VPN, SD WAN, TLS 1.3 и тп)
- Российские продукты пока не обладают необходимым набором функций USG/UTM:
  - Функциональность в угоду регуляторам
  - Нет широты модулей безопасности
  - «Сырой» интерфейс, отчетность и настройки
- Проблемы с сертификацией:
  - Комплексная защиты vs. Базовая защита, но с бумажкой

А что с производительностью?

- Производительность по «даташитам» не имеет ничего общего с реальностью
- Производительность зависит от профиля трафик
  - Протоколы, шифрованный трафик, размер пакетов и тп
- Производительность будет зависеть от включенных модулей, настроек и даже отдельных правил фильтрации
  - SSL-инспекция и антивирус могут убить производительность
- Публичные тесты не заслуживают доверия, затачиваются под «спонсоров»

Важно протестировать на реальном трафике
и индивидуальных настройках

Рекомендации

- Необходимость сертификации значительно сузит выбор и качество продукта
- Выбирайте USG/NGFW по скоринговой модели на базе нашего сравнения:
  - Каждому критерию в таблице присваивается вес
  - Вес перемножается на оценку 1/0.5/0 за наличие функции
  - Полученные баллы суммируются
  - Лучшие по количеству баллов идут в пилотирование
- Тестируйте производительность на боевых настройках

Контакты

Генеральный директор
ilya.shabanov@anti-malware.ru

www.anti-malware.ru

@anti_malware

@Anti_Malware

antimalwareru