NGFW в эпоху перемен: задачи и вызовы при защите современного периметра

Иван Панин

Руководитель группы развития решений
по инфраструктурной безопасности

Лаборатория Касперского

09.12.2024

kaspersky

20 минут

План доклада:

- Вызовы с которыми сталкиваются компании при защите корпоративного периметра
- Роль и вызовы NGFW
- Понятие современного периметра
- Ограничения при расшифровке TLS-трафика
- Сценарий: Защита удаленного доступа
- Datasheet & Производительность
- Лучшие практики оптимизации NGFW

kaspersky

Об авторе презентации

CCNP, CCNP Security, CCDP, MBA CSO

2005-2010 **Фармкомпания, Инженер**

- Настроил свои первые Cisco ASA и ISA Server.

2010-2014 **Step Logic, Микротест, Инженер**

- Пресейл и внедрение Fortinet, Palo Alto, Checkpoint, Stonesoft, Blue Coat, VipNet, S-Terra и АПКШ Континент.

2014-2022 **Cisco Systems, Архитектор**

- Портфель ИБ, включая ASA, Firepower, Meraki, IronPort и SASE.
- Руководитель практики IOS Security & VPN виртуальных инженеров Cisco WW.

2022- **Лаборатория Касперского, Руководитель группы развития решений по инфраструктурной безопасности**

- Экспертная техническая поддержка пресейловых команд: SD-WAN и NGFW.
- Разработка сценариев использования и лабораторные работы.

Вызовы при защите корпоративного периметра

с которыми сталкиваются профильные специалисты

Инструменты
эффективность доступных NGFW против современных угроз

Миграция
пересмотр архитектуры сетевого периметра под возможности NGFW

Ресурсы
ограничение во времени, квалификации и финансировании

Роль и вызовы NGFW

при защите современного периметра

Сценарии использования:

1. Защита периметра:

- Контроль доступа к сети Интернет и облачным приложениям.
- Публикация сервисов.
- Распределённая сеть Site-to-Site VPN.
- Удаленный доступ к корпоративной сети Remote Access VPN.

2. Внутренняя сегментация.

3. Мониторинг и аналитика трафика.

4. Соответствие требованиям.

Эволюция периметра и угроз:

- Размывание периметра при работе с облаками и удаленной работе.
- Рост сложности кибератак - необходимость расшифровки и глубокой инспекции трафика.

Статистика за 2023 год*:

- 85,9% угроз доставлены через зашифрованные каналы.
- Рост числа шифрованных атак на 24,3% по сравнению с 2022 годом.

* Encrypted attack 2023 stats from Zscaler: https://info.zscaler.com/resources-industry-reports-threatlabz-2023-state-of-encrypted-attacks-report

Современный периметр

Сеть без границ

Расшифровка TLS-трафика

Ограничения NGFW

- Certificate Pinning (Gmail & Chrome).
- Криптография на основе постквантовых алгоритмов Kyber, ML-KEM*.
- Протокол QUIC (HTTP/3).
- End-to-End Encryption (WhatsApp, Telegram).
- Неподдерживаемые криптоалгоритмы, например, ГОСТ.
- Web/SSL VPN (Client certificate).
- Обфускация Shadowsocks и Obfsproxy.
- TLS 1.3 & ECH: расшифровка трафика «дорого» для NGFW.
- Фильтрация DNS over HTTPS (DoH).

**Cloudflare Radar (RU): QUIC 38%
Постквантовое шифрование 12,5%

Варианты решения:

- Интеграция / использование EDR на стороне клиента.
- Интеграция с XDR / использование ML/AI для анализа зашифрованного трафика: интервалы между запросами, размер пакетов, заголовки пакетов, параметры шифрования, неизвестные домены и сертификаты, трафик нехарактерный для браузера.

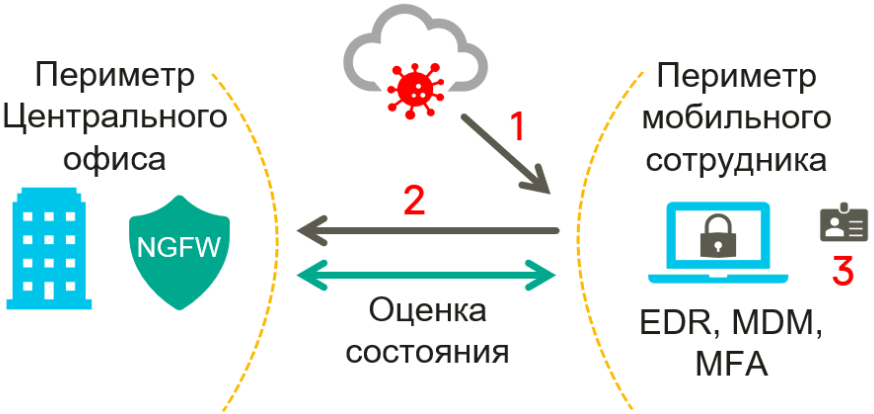
* FortGate: https://community.fortinet.com/t5/FortiGate/Technical-Tip-ERR-SSL-PROTOCOL-ERROR-when-using-Flow-based-Deep/ta-p/35755
* Palo Alto: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HED5CAO&lang=en_US
** Cloudflare Radar в России: https://radar.cloudflare.com/adoption-and-usage/ru

Защита удаленного доступа

Требования к функциям NGFW

- Безопасный TLS/IPSec/ГОСТ доступ.
- Все возможности NGFW для защиты мобильных пользователей.
- Интуитивный мастер настройки.
- Инструменты для мониторинга и диагностики.
- Оценка состояния хоста клиента, динамическая авторизация ZTNA.

- Защита мобильных сотрудников EDR, MDM.
- Многофакторная аутентификация MFA.
- Интеграция с XDR.



Векторы атаки на корпоративный периметр:

1. VPN Off.
2. VPN Split Tunnel.
3. Компрометация User Credentials.

Производительность NGFW

Datasheet

Функции	Mbps
Stateful FW (L4) + NAT?	40,000
FW + Application (HTTP, Mix?)	20,000
FW + Application + IPS = NGFW	10,000
FW + Application + IPS + Malware** = Threat Protection* (1024B/64KB/Mix?)	5,000
IPS	20,000
TLS (Decrypt & Encrypt only) Resumption rate?	1,000
IPSec VPN	2,000
Maximum concurrent (1024B) / New sessions (1B) L4/L7 mode?	15M / 200K

* Threat Intelligence, URL, DLP, DNS Security ?

** Malware = AV + Cloud Lookup + Sandbox ?

Средний размер пакета при веб-сёрфинге 600–800 Byte

Пример задачи:

- NGFW до 500 Mbps в режиме Threat Protection
- Доля веб & TLS-трафика = 50%

TLS Decryption снижает производительность NGFW на 50-90%***

NGFW до 2,750 Mbps = CPU 100%

Рекомендации при проектировании NGFW:

- Загрузка на 50-60% для возможности роста
- Пиковая загрузка до 80-90% при отражении атак
- NGFW до 4,583 Mbps в режиме Threat Protection = CPU 60%

*** NSS Labs: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/nss-labs-2018-ngfw-comparative-report-performance.pdf

Оптимизация производительности NGFW

Лучшие практики по управлению правилами безопасности

- Конкретные Source, Destination, избегать Any.
- Часто используемые правила вверх.
- Фильтрация на ранних этапах: IP, порты, User-ID, репутационные списки, GeoIP, URL и DNS Security.
- Application Control и IPS для важных сегментов и приложений.
- Исключения при расшифровке TLS-трафика: онлайн-банкинг, ЕМИАС.
- Целевое использование ресурсоемких функций: TLS, Malware, Cloud Lookup и Sandbox.
- Проверка правил на избыточность, дублирование.
- Комментарии к правилам для упрощения аудита.
- Сегментация внутренних хостов для снижения межзонного трафика.
- Журналирование: инциденты безопасности, а сетевые соединения только для отладки или compliance.
- Аналоги Intelligent Application Bypass.

FortiGate Best Practice: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Best-practice-for-performance-enhancement/ta-p/194420

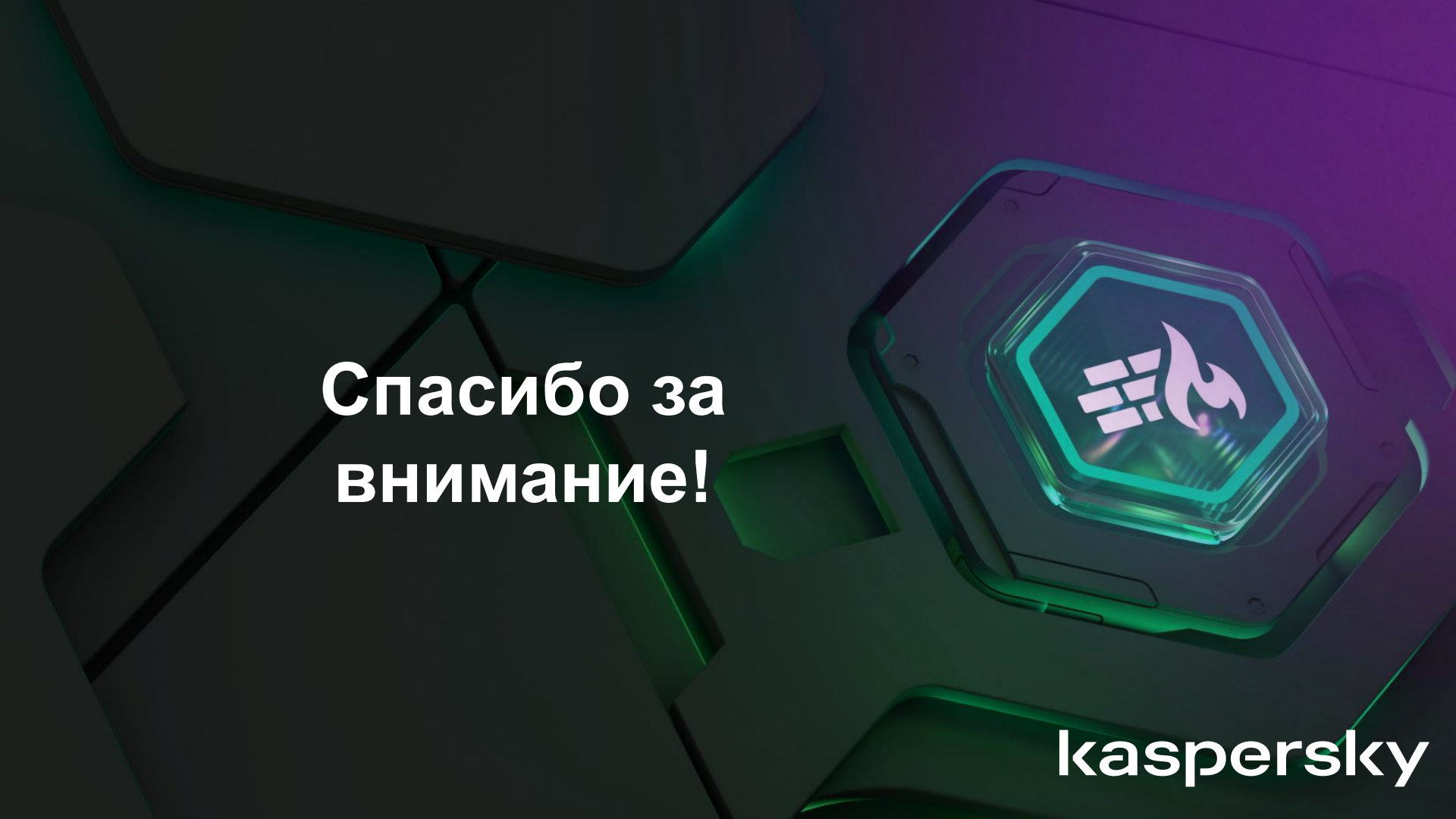
Кратко о главном

Выбирайте NGFW в зависимости от сценария использования, а не путем сравнения всех функций доступных NGFW.

«Один в поле не воин»: NGFW должен поддерживать интеграцию со смежными решениями: комплексное решение, аналитика, расследование, автоматизация.

Планируйте реальную загрузку NGFW, оптимизируйте производительность. Требуйте от вендора обучение по чтению Datasheet.

Спасибо за внимание!



kaspersky