Fortinet
Защита периметра сети

Вячеслав Павлов
vpavlov@netwell.ru

FORTINET

Цифровая трансформация значительно расширяет поверхность атак

Решения компании Fortinet

FortiNAC	FortiAP	FortiGate	FortiGate VM	FortiWeb	FortiClient	FortiAnalyzer	FortiManager
FortiClient Fabric Agent	FortiSwitch		FortiCWP	FortiMail	FortiEDR	FortiSIEM	FortiCloud
FortiAuthenticator				FortiCASB	FortiInsight	FortiSandbox	
				FortiADC		FortiSOAR	

FortiGuard Services

Netwell: контакты

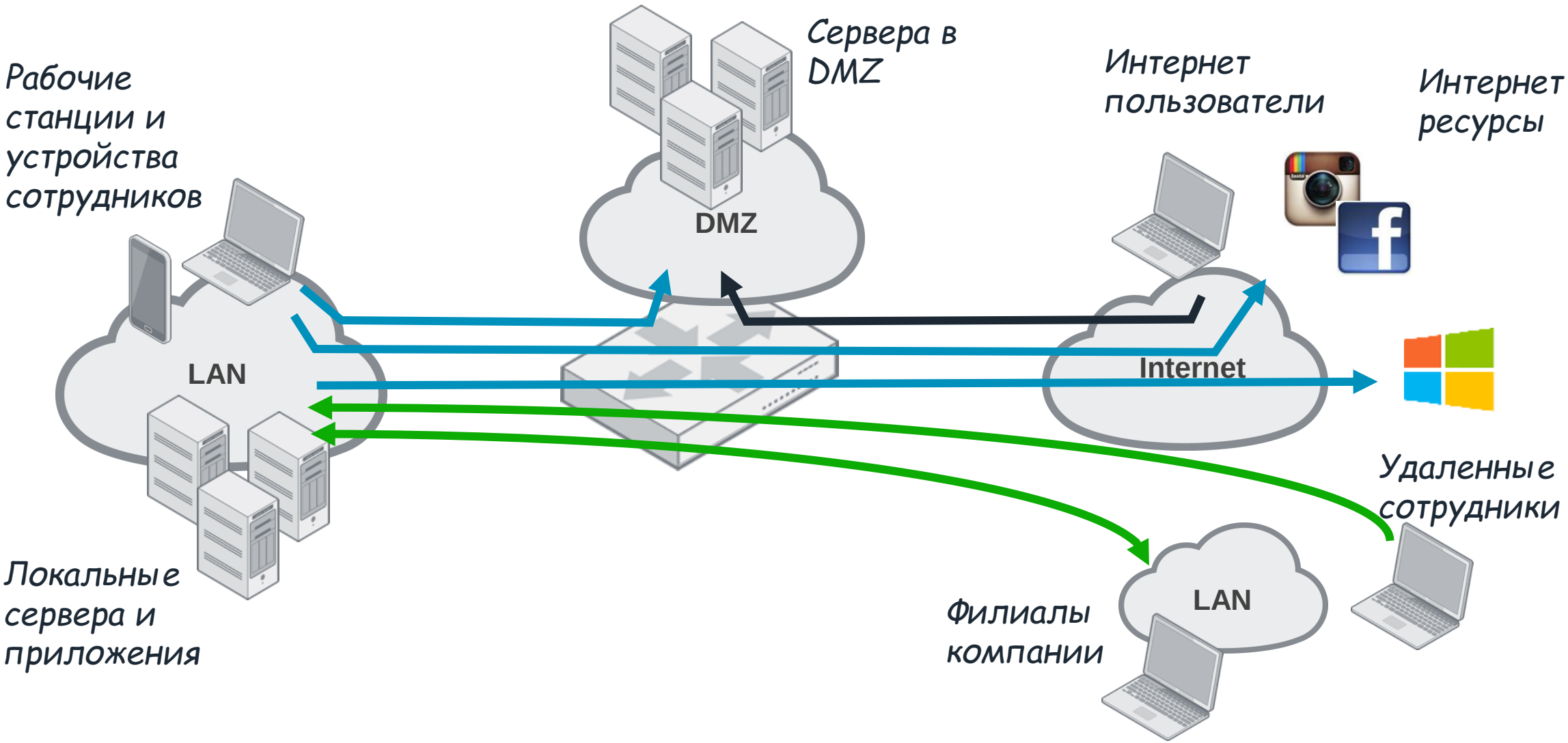
Сайт http://netwell.ru

E-mail: *fortinet@netwell.ru*

Защита периметра сети

- Теория и спектр задач
- Обзор NGFW FortiGate
- Практика применения

Периметр сети



Задачи

A Контролируемый и безопасный доступ в интернет

B Публикация и защита приложений

C Управление трафиком приложений и SLA

D Безопасный удаленный доступ

E Распределенная филиальная сеть

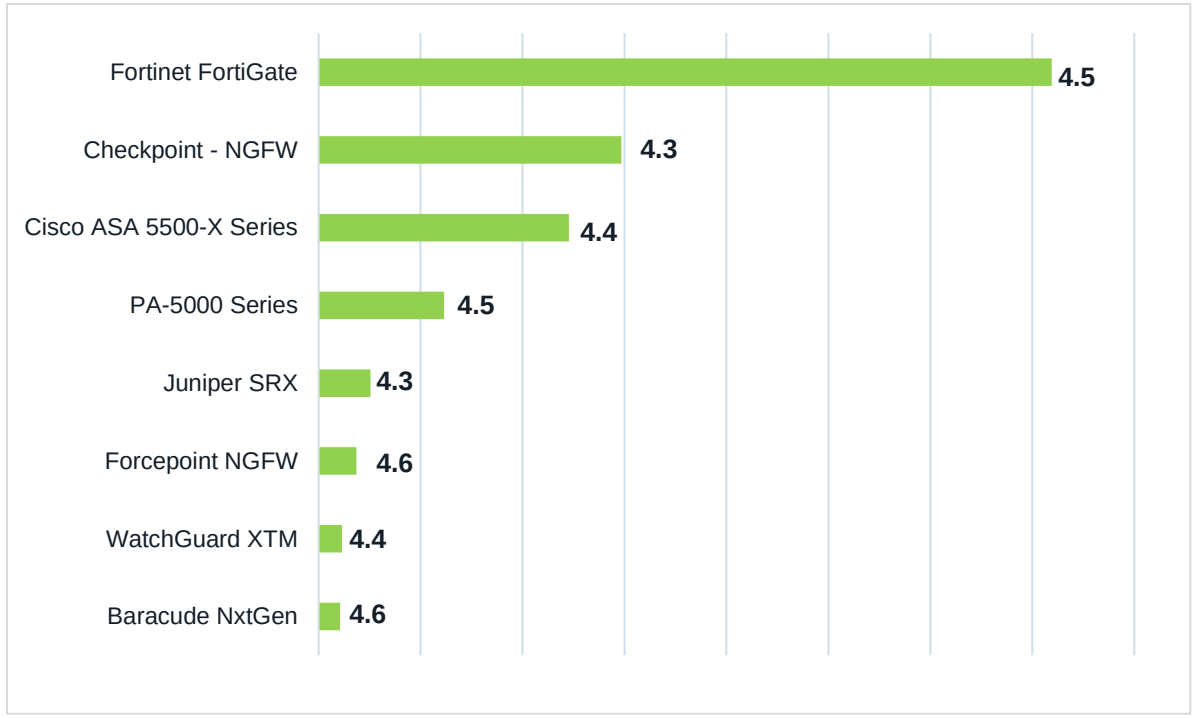
F Видимость, контроль и автоматизация

Квадрант Гартнера для межсетевых экранов 2019

Figure 1. Magic Quadrant for Network Firewalls

Source: Gartner (September 2019)

Gartner peerinsights™



As of 09/10/19

FortiGate – набор функций

- Accelerated Firewall
- IPS & IDS
- Dynamic Web Filtering
- Anti-Virus & Anti-Botnet
- Application Control & DLP
- Cloud / on-premise Sandboxing
- Mobile Security & Endpoint Control

- Advanced HA
- Virtual Domains & vClustering
- SSL & IPSec VPN (+ADVPN)
- QoS & Traffic shaping
- Identity & Device Awareness
- Advanced SD WAN
- Wan Optimization
  (cache, explicit proxy, wanop)

Служба FortiGuard Labs

FortiGuard Labs delivers services and intelligence that protects and defends against the evolving threat landscape

Powered by AI

Enterprise Protection

Enterprise Protection	
CASB	
Industrial Security	
Security Rating	
Web Filtering	
Advanced Malware Protection*	
IPS	
Antispam	
FortiCare + App Control	

Advanced Malware Protection (AMP) includes:
Antivirus, FortiSandbox Cloud, Mobile, Botnet, Virus Outbreak Protection and Content Disarm & Reconstruct

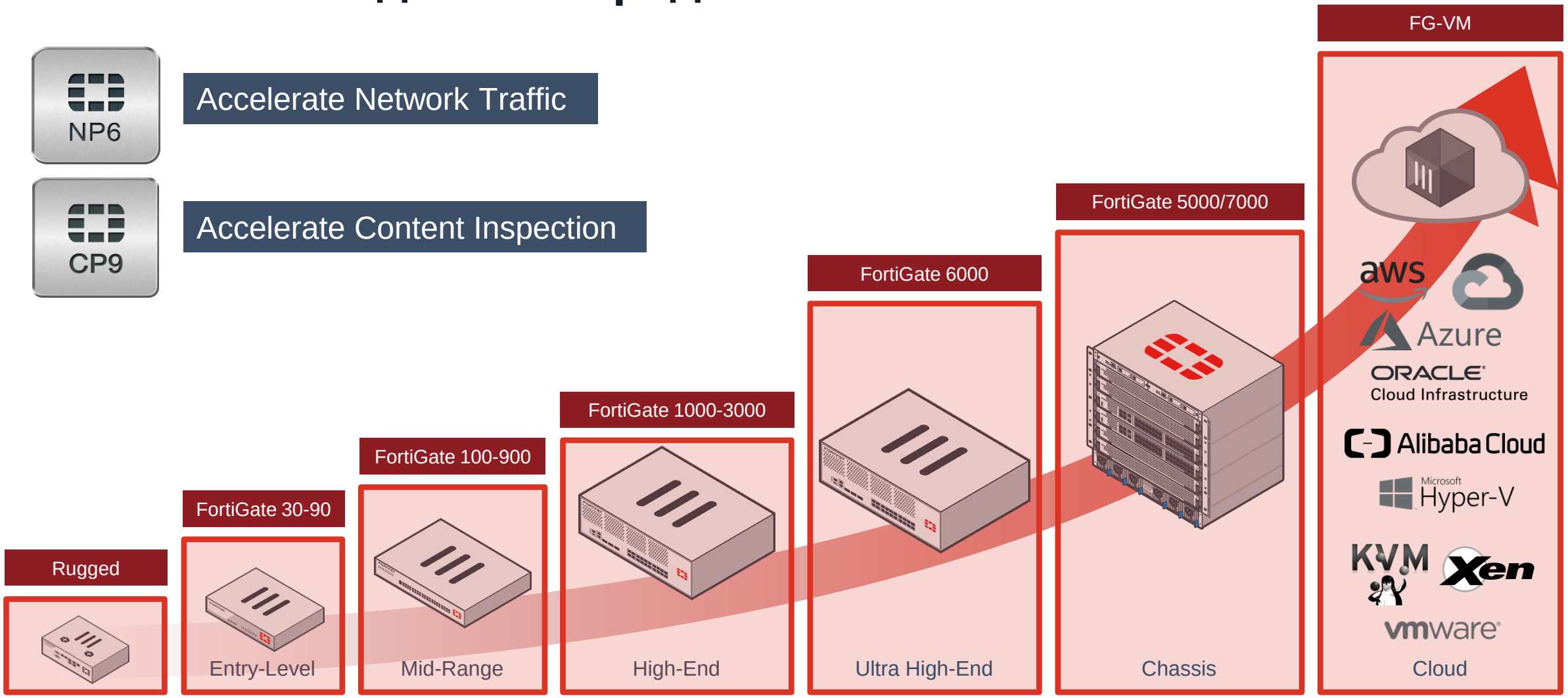
FortiGate – модельный ряд

NP6

Accelerate Network Traffic

CP9

Accelerate Content Inspection

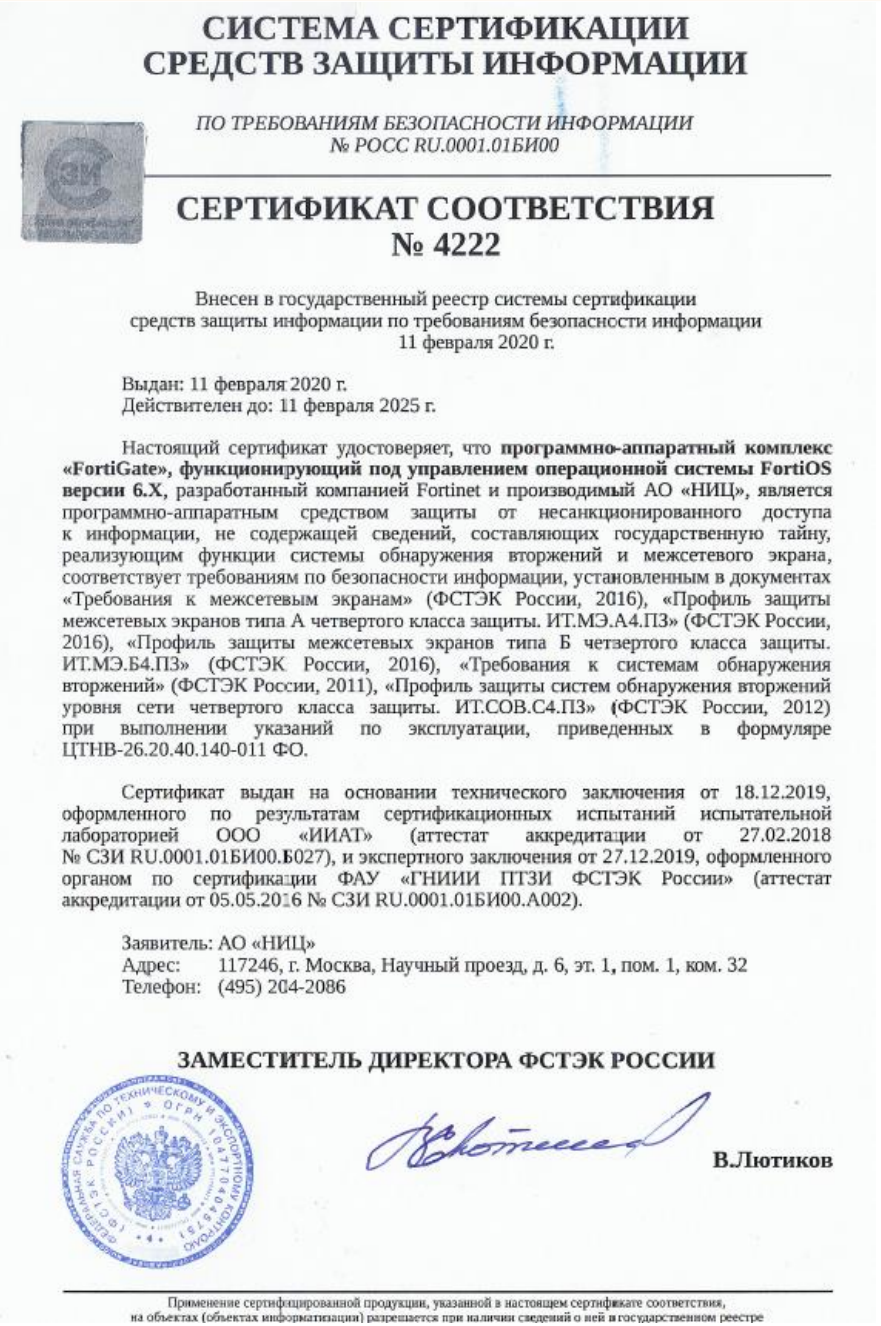


Сертификация ФСТЭК

Сертификат действителен до 11 февраля 2025 г.

На соответствие чему сертифицировано?

- Требования к межсетевым экранам ” ФСТЭК России 2016”
- Профиль защиты межсетевых экранов типа А четвёртого класса защиты (ФСТЭК России 2016)
- Профиль защиты межсетевых экранов типа Б четвёртого класса защиты (ФСТЭК России 2016)
- Профиль защиты систем систем обнаружения вторжений уровня сети четвертого класса защиты (ФСТЭК России 2012)
- Требования к системам обнаружения вторжений (ФСТЭК России 2011)



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4222

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
11 февраля 2020 г.

Выдан: 11 февраля 2020 г.
Действителен до: 11 февраля 2025 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс «FortiGate», функционирующий под управлением операционной системы FortiOS версии 6.X**, разработанный компанией Fortinet и производимый АО «НИЦ», является программно-аппаратным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции системы обнаружения вторжений и межсетевого экрана, соответствует требованиям по безопасности информации, установленным в документах «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре ЦТНВ-26.20.40.140-011 ФО.

Сертификат выдан на основании технического заключения от 18.12.2019, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ИИАТ» (аттестат аккредитации от 27.02.2018 № СЗИ RU.0001.01БИ00.Б027), и экспертного заключения от 27.12.2019, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «НИЦ»
Адрес: 117246, г. Москва, Научный проезд, д. 6, эт. 1, пом. 1, ком. 32
Телефон: (495) 264-2086

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре

Метрики производительности

FortiGate® Network Security Platform - ***Top Selling** Models Matrix

FORTINET®

Product Matrix

April 2020

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG/FWF-30E	FG-40F	FG/FWF-50E	FG/FWF-60E	FG-60F
Firewall Throughput (1518/512/64 byte UDP)	0.95 Gbps ****	5 / 5 / 5 Gbps	2.5 Gbps ****	3 / 3 / 3 Gbps	10/10/6 Gbps
IPsec VPN Throughput (512 byte) [1]	75 Mbps	4.4 Gbps	90 Mbps	2 Gbps	6.5 Gbps
IPS Throughput (Enterprise Mix) [2]	300 Mbps	1 Gbps	350 Mbps	400 Mbps	1.4 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	200 Mbps	800 Mbps	220 Mbps	250 Mbps	1 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	150 Mbps	600 Mbps	160 Mbps	200 Mbps	700 Mbps
SSL VPN Throughput	35 Mbps	490 Mbps	100 Mps	150 Mbps	900 Mbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	100	200	200	200	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	125 Mbps	310 Mbps	150 Mbps	135 Mbps	750 Mbps
Application Control Throughput (HTTP 64K) [2]	400 Mbps	990 Mbps	450 Mbps	650 Mbps	1.8 Gbps

Функциональные отличия и кол-во объектов?

FortiOS Feature/Platform Matrix

https://docs.fortinet.com/document/fortigate/6.2.3/fortios-feature-platform-matrix

FortiOS Maximum Values Table

https://docs.fortinet.com/document/fortigate/6.2.0/fortios-maximum-values-table

Документация

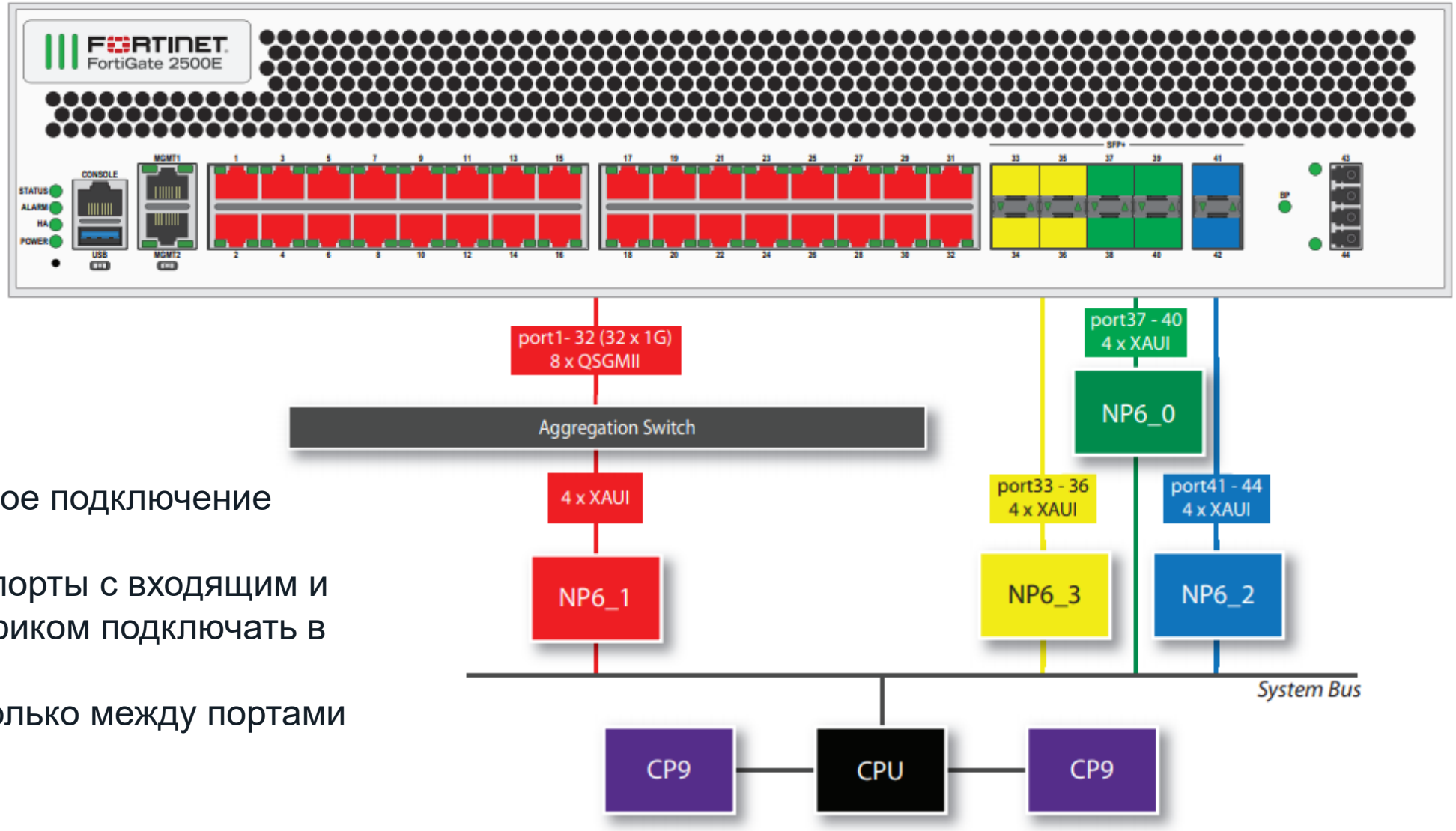
https://docs.fortinet.com/

Чем отличаются аппаратные модели FortiGate?

- Все модели работают под управлением операционной системы FortiOS
- Аппаратные отличия (компоненты ➡ производительность ➡ цена):
  - » Физические интерфейсы
  - » Жесткий диск
  - » CPU и RAM
  - » Сопроцессоры FortiASIC
  - » Блоки питания
  - » Места в стойке
  - » POE порты
  - » WiFi точка доступа

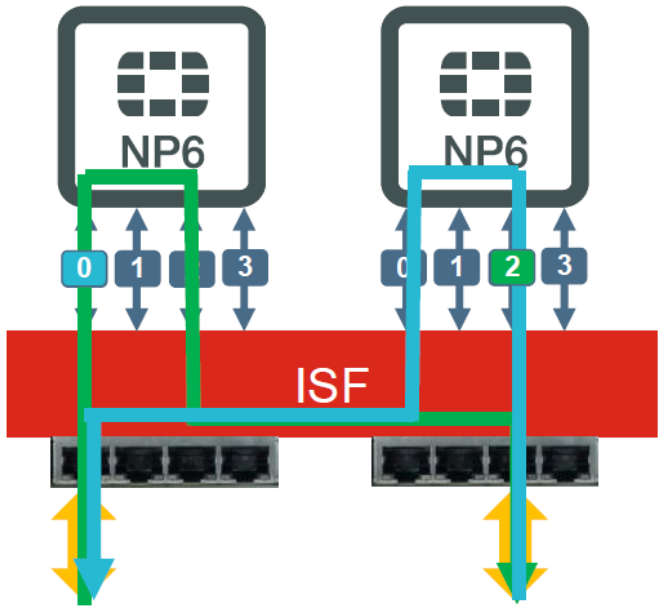
Подробное описание технических характеристик и данных по производительности указаны в даташитах

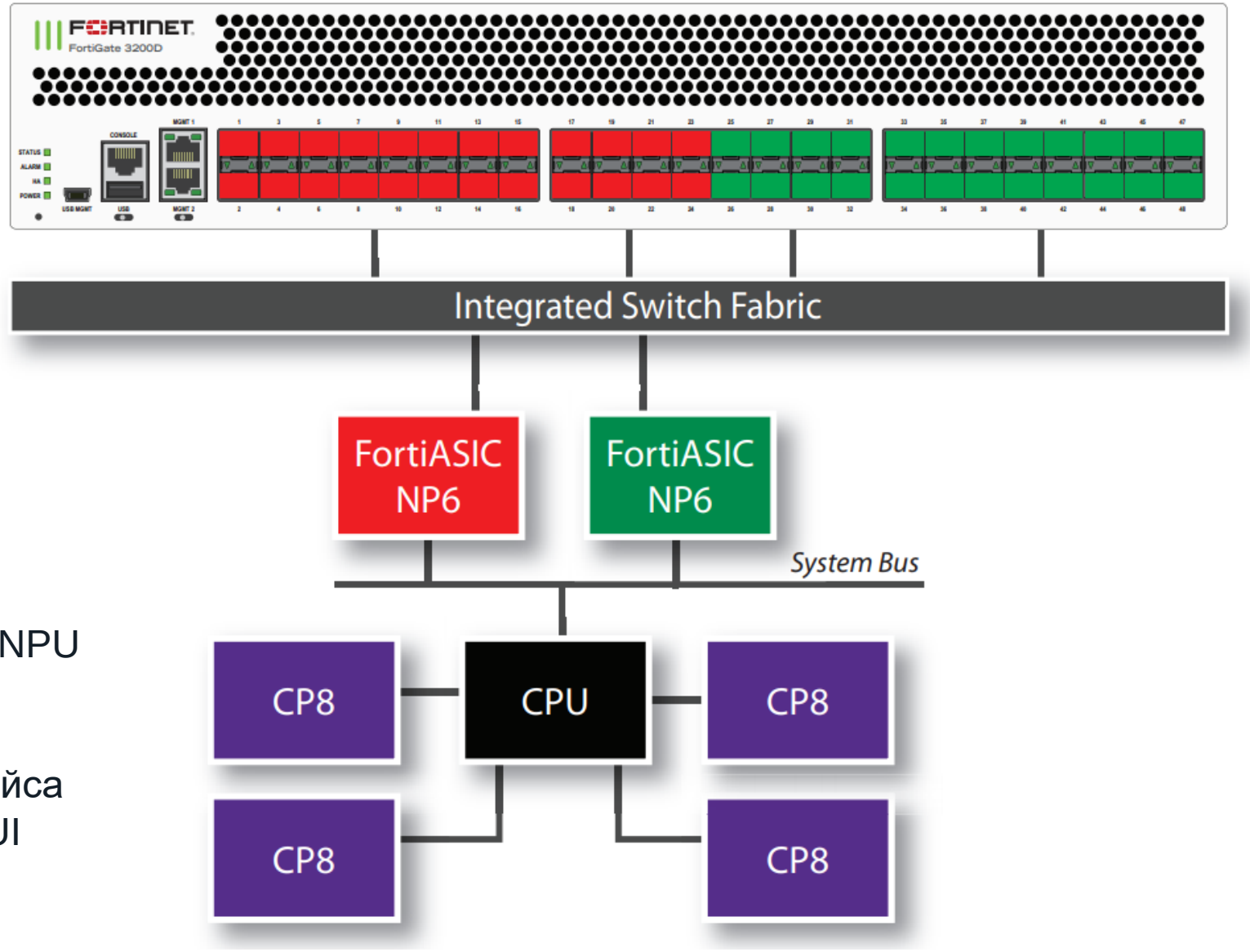
Пример внутренней архитектуры #1



- NP Direct – прямое подключение портов в ASIC
- Рекомендуется порты с входящим и исходящим трафиком подключать в один NPU
- LAG доступен только между портами одного NPU

Пример внутренней архитектуры #2





- Распределите трафик по разным NPU
- Разгрузите внутреннюю шину. Номер исходящего XAUI интерфейса от NPU совпадает с номером XAUI интерфейса физического порта

Как добиться максимальной производительности?

- Используйте UTM функции рационально (для разных сегментов сети, для разных типов трафика нужны разные функции безопасности)
- Пересылайте логи во внешние коллекторы (FortiAnalyzer), логирование на локальный жесткий диск – дополнительная нагрузка на CPU и RAM
- Используйте FortiASIC эффективно

Жизненный цикл ПО и оборудования

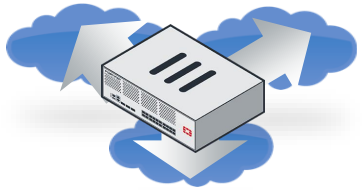
- Политика и сроки жизненного цикла (Life Cycle)

https://support.fortinet.com/Information/ProductLifeCycle.aspx

- Выбор версии ПО (апрель 2020)
  - Самая новая, новые функции: FortiOS 6.4
  - Рекомендованная в общем случае «-1»: FortiOS 6.2.x
  - Рекомендованная для критичной инфраструктуры «-2»: 6.0.x

Режимы работы FortiGate

NAT/Route

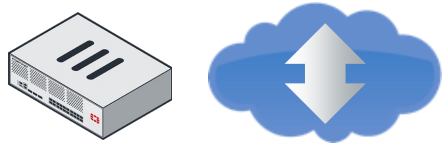


- Контроль трафика между подсетями
- Статическая, динамическая и policy-based маршрутизация, NAT и SD-WAN
- Внедряется как роутер

Transparent/Bridge

- Прозрачный контроль трафика в сети
- Поддержка протоколов L2 коммутации
- Внедряется как свитч

Sniffer



- Мониторинг трафика в режиме оффлайн
- Не влияет на работу сети
- Внедряется как sniffer

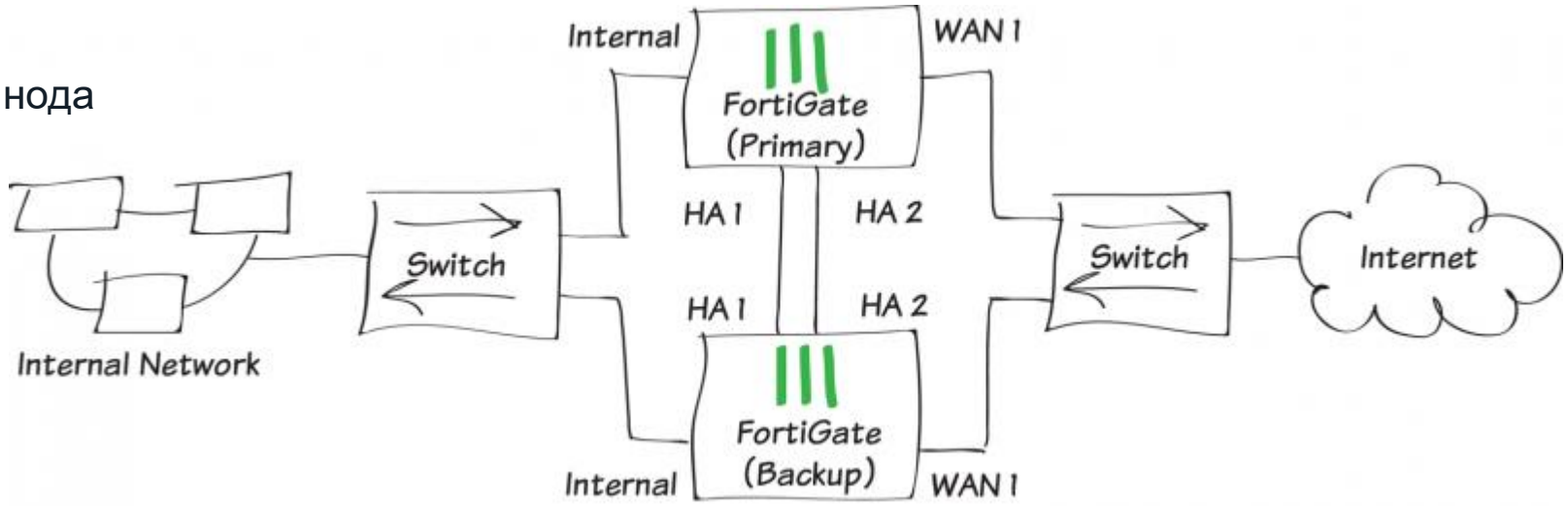
FortiOS позволяет использовать комбинации режимов при помощи VDOM

Отказоустойчивость

- **Требования к кластеризации**
  - 2-4 FortiGate одинаковой:
    - Модели
    - Версии FortiOS
    - Режим работы
  - Как минимум 1 heartbeat линк (рекомендуется несколько)
  - Порты для трафика подключаются в L2 домен

- **Выбор Мастер ноды**
  - Override disabled (режим по умолчанию)
    - Статус интерфейсов, uptime, приоритет, серийный номер
    - ‘diagnose sys ha reset-uptime’
  - Override enabled
    - Мастер – нода с самым высоким приоритетом
    - Смена приоритета приводит в «перевыборам»

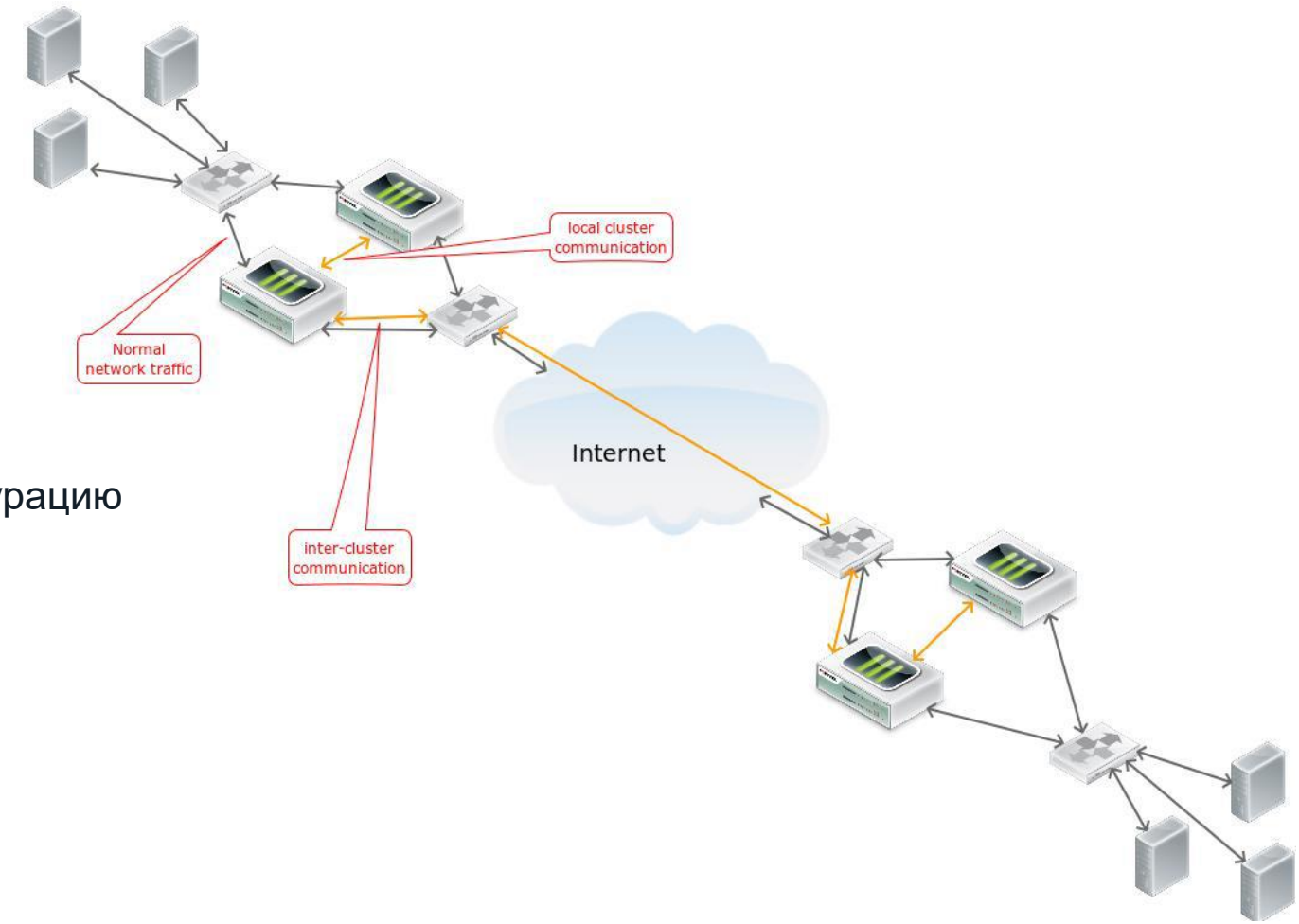
- **Режимы работы кластера**
  - Active-Passive – только Master нода обрабатывает трафик
  - Active-Active – все ноды обрабатывают трафик, мастер распределяет трафик



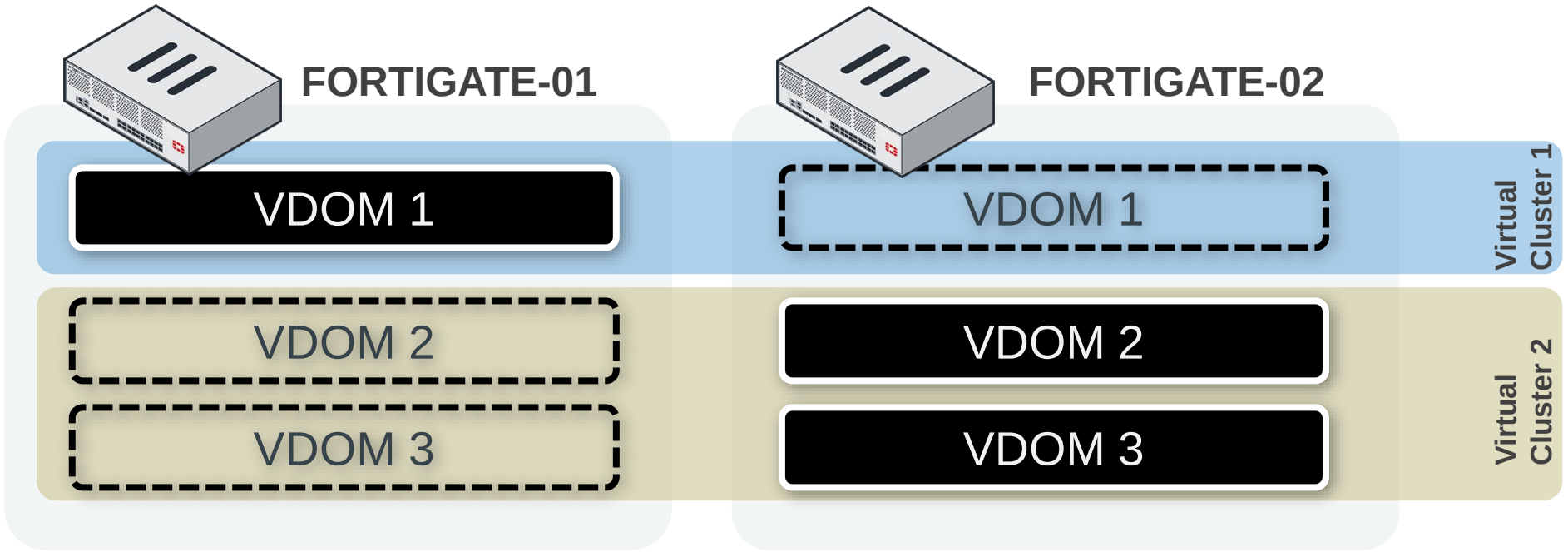
«Кластер» синхронизаций сессий FGSP

- **FortiGate Session Life Support Protocol (FGSP)**
  - Синхронизирует сессии до 16 устройств.
  - Настраивается per-VDOM
  - Проще топология
  - Выполняет синхронизацию TCP сессий (по умолчанию).

    Можно включить для UDP, ICMP, IPsec
  - Может частично синхронизировать конфигурацию (кроме management IP, interfaces, routing)
  - Начиная с FortiOS 6.0 поддерживается синхронизация между кластерами и отдельными устройствами



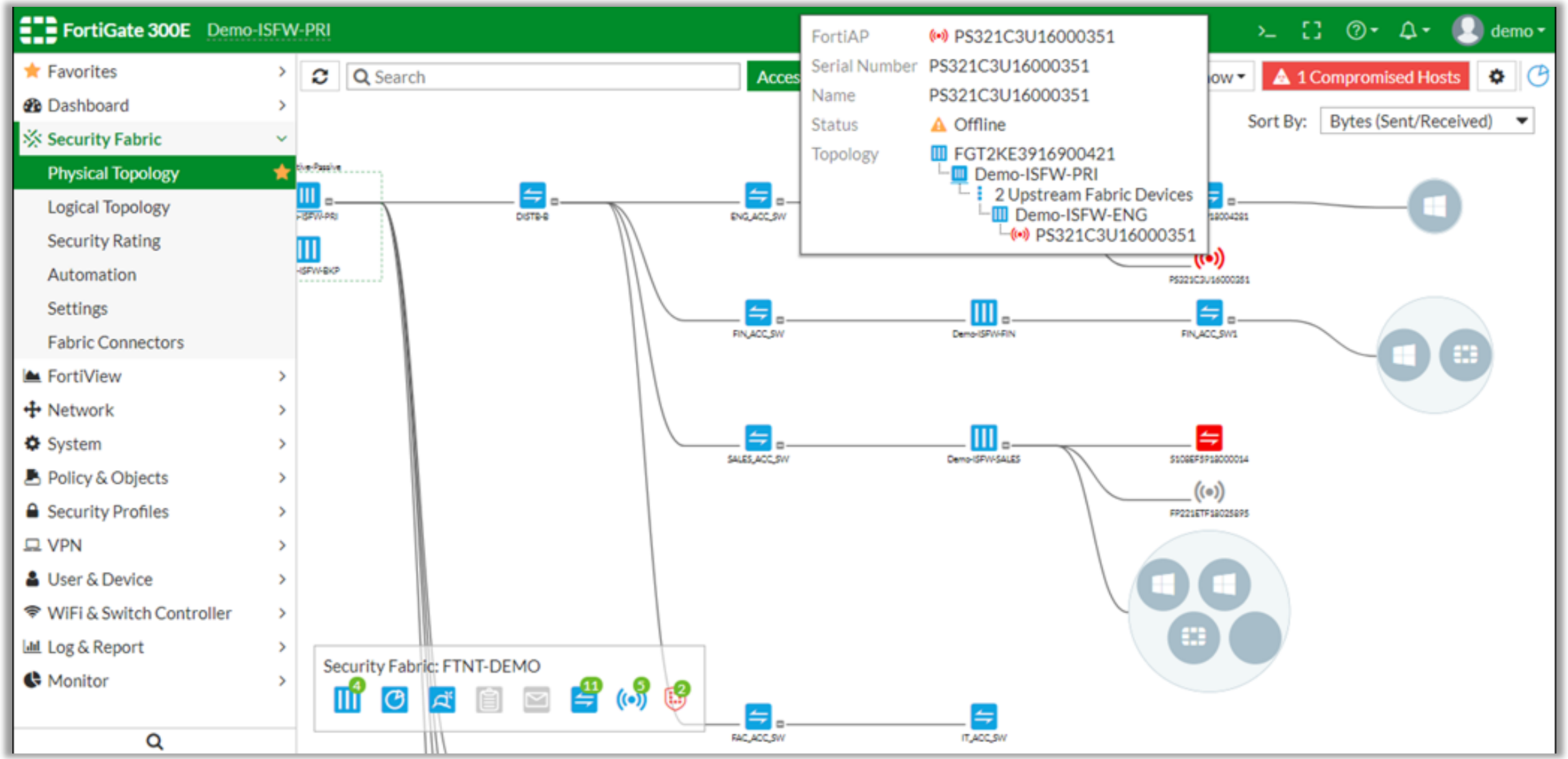
VDOM и кластеризация



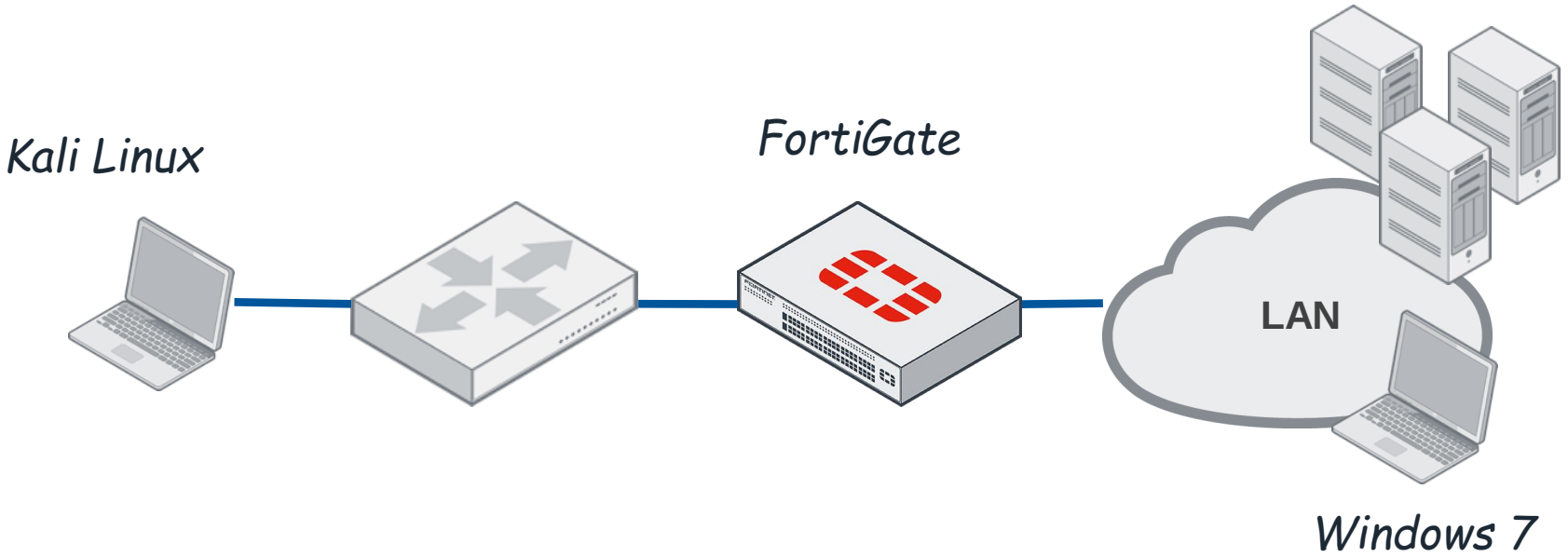
ВИРТУАЛЬНЫЙ КЛАСТЕР

- Поддерживается A-A и A-P режим
- Доступен при использовании VDOM
- Позволяет реализовать балансировку
- Виртуальный кластер может иметь несколько VDOM
- Inter-VDOM линки создаются для одного VDOM

Топология «Фабрики безопасности»



Тестовый стенд



Спасибо

Вопросы?

Вячеслав Павлов
vpavlov@netwell.ru

FORTINET