

Таблица 1. Производительность различных моделей^A

Производительность	PA-7080 ^B	PA-7050 ^B	PA-5450 ^C	PA-5280	PA-5260	PA-5250	PA-5220
Режим анализа приложений App-ID (arpmix)	687 Гбит/с	416 Гбит/с	200 Гбит/с	60 Гбит/с	60 Гбит/с	37 Гбит/с	17 Гбит/с
Режим блокировки всех угроз (arpmix)	405 Гбит/с	243 Гбит/с	148 Гбит/с	33,8 Гбит/с	33,8 Гбит/с	23 Гбит/с	10 Гбит/с
Пропускная способность IPsec VPN	334 Гбит/с	200 Гбит/с	79 Гбит/с ^D	28 Гбит/с	28 Гбит/с	19 Гбит/с	10 Гбит/с
Новых L7 сессий в секунду	6 000 000	4 000 000	3 500 000 ^D	586 000	586 000	392 000	166 000
Максимум одновременных L7-сессий	416 000 000	245 000 000	100 000 000 ^D	64 000 000	32 000 000	8 000 000	4 000 000
Виртуальные системы (база/макс. ^E)	25/225			25/225			10/20
Характеристики	PA-7080	PA-7050	PA-5450	PA-5280	PA-5260	PA-5250	PA-5220
Интерфейсы ^F	10/100/1000 (до 120), SFP/ SFP+ (до 80), QSFP+/QSFP28 (до 40)	10/100/1000 (до 72), SFP/ SFP+ (до 48), QSFP+/QSFP28 (до 24)	100/1000/10G RJ45 (до 8), 1G/10G SFP/ SFP+(до 24), 40G/100G QSFP28 (до 4)	100/1000/10G RJ45 (4), 1G/10G SFP/SFP+ (16), 40G/100G QSFP28 (4)			100/1000/10G RJ45 (4), 1G/10G SFP/SFP+ (16), 40G QSFP+ (4)
Интерфейсы подсистемы управления	SFP/SFP+ MGT (2), SFP/SFP+ HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), консольный порт RJ45 (1), консольный порт Micro USB (1)		SFP/SFP+ MGT (2), SFP/ SFP+ HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), консольный порт RJ45 (1), консольный порт Micro USB (1)	10/100/1000 RJ45 (2), 10/100/1000 порт управления (1), консольный порт RJ45 (1)			(1) 40G QSFP+ HA
Габариты	19U, 19” стандартная стойка (84.38см. В x 62.64см. Г x 44.45см. Ш)	9U, 19” стандартная стойка (40см. В x 60.32см. Г x 44.45см. Ш) или 14U, 19” стандартная стойка с опциональным набором PAN-AIRDUCT (62.23см. В x 60.32см. Г x 44.45 см. Ш)	5U, 19” стандартная стойка (22.23см. В x 76.2см. Г x 44.2см. Ш)	3U, 19” стандартная стойка (13.33см. В x 52.07см. Г x 43.81см. Ш)			
Источник питания	2500 W AC (2400 W/2700 W) (4 с расширением до 8)	2500 W AC (2400 W/2700 W) (4)	2,200 W AC или DC (2 с расширением до 4)	1200 W AC или DC (1:1 с полным резервированием) (2)			
Резервное питание	Да			Да			
Дисковые накопители	Системный диск 240 ГБ SSD, RAID1 (2)		Система: 480 ГБ SSD, RAID1 Журналы:4 ТБ SSD (опционально)	Система: 240 ГБ SSD, RAID1 Журналы: 2 ТБ HDD, RAID1			
Горячая замена вентиляторов	Да			Да			
Производительность	PA-3260		PA-3250		PA-3220		
Режим анализа приложений App-ID (arpmix)	8,7 Гбит/с		5,8 Гбит/с		4,8 Гбит/с		
Режим блокировки всех угроз (arpmix)	4,7 Гбит/с		3,1 Гбит/с		2,6 Гбит/с		
Пропускная способность IPsec VPN	4,7 Гбит/с		2,9 Гбит/с		2,6 Гбит/с		
Новых L7 сессий в секунду	94 400		63 700		52 800		
Максимум одновременных L7-сессий	2 200 000		2 000 000		1 000 000		
Виртуальные системы (база/макс. ^B)			1/6				
Характеристики	PA-3260		PA-3250		PA-3220		
Поддерживаемые интерфейсы ^F	10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)		10/100/1000 (12), 1G/10G SFP/SFP+ (8)		10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)		
Интерфейсы подсистемы управления	10/100/1000 порт управления (1), 10/100/1000 HA (2), 10G SFP+ HA (1), консольный порт RJ45 (1), консольный порт Micro USB (1)						
Габариты			2U, 19” стандартная стойка (8.89см. В x 52.15см. Г x 44.04см. Ш)				
Источник питания			650 W AC или DC (180/240)				
Резервное питание			Да				
Дисковые накопители			240 Гбайт SSD				
Горячая замена вентиляторов			Да				

Таблица 1. Производительность различных моделей (продолжение)

Производительность	PA-850	PA-820	PA-460	PA-450	PA-440	PA-410	PA-220	PA-220R
Режим анализа приложений App-ID (arpmix)	2,1 Гбит/с	1,7 Гбит/с	4,7 Гбит/с	3,2 Гбит/с	2,4 Гбит/с	1,3 Гбит/с	560 Мбит/с	560 Мбит/с
Режим блокировки всех угроз (arpmix)	1,2 Гбит/с	900 Мбит/с	2,6 Гбит/с	1,7 Гбит/с	1,0 Гбит/с	600 Мбит/с	300 Мбит/с	300 Мбит/с
Пропускная способность IPsec VPN	1,7 Гбит/с	1,4 Гбит/с	3,1 Гбит/с	2,2 Гбит/с	1,6 Гбит/с	930 Мбит/с	570 Мбит/с	570 Мбит/с
Новых L7 сессий в секунду	13 100	8 100	74 000	52 000	39 000	13 000	4 200	4 200
Максимум одновременных L7-сессий	192 000	128 000	400 000	300 000	200 000	64 000	64 000	64 000
Виртуальные системы (база)	1	1	1	1	1	1	1	1
Характеристики	PA-850	PA-820	PA-460	PA-450	PA-440	PA-410	PA-220	PA-220R
Поддерживаемые интерфейсы ^F	10/100/1000 (4), 1G SFP (4), 1G/10G SFP/SFP+ (4)	10/100/1000 (4), SFP (8)	10/100/1000 RJ45 (8)			10/100/1000 RJ45 (7)	10/100/1000 RJ45 (8)	10/100/1000 (6), SFP (2)
Интерфейсы подсистемы управления	10/100/1000 внешнее управление (1), 10/100/1000 HA (2), консольный порт RJ45 (1), USB (1), консольный порт Micro USB (1)		10/100/1000 внешнее управление (1), консольный порт RJ45 (1), USB (2), консольный порт Micro USB (1)			10/100/1000 внешнее управление (1), консольный порт RJ45 (1), USB (2)	10/100/1000 внешнее управление (1), консольный порт RJ45 (1), USB (1), консольный порт Micro USB (1)	
Габариты	1U, 19" стандартная стойка (4.44см. В x 36.83см. Г x 43.49см. Ш)	1U, 19" стандартная стойка (4.44см. В x 35.56см. Г x 43.49см. Ш)	4.45см. В x 22.35см. Г x 20.3см. Ш			4.14см. В x 16.31см. Г x 24.21см. Ш	4.1см. В x 16см. Г x 20.5см. Ш	5.08см. В x 22см. Г x 23.5см. Ш
Источник питания	450 W AC (2; один резервный)	200 W	Двойной резервный 50 W			25 W	Двойной резервный 40 W	
Резервное питание	Да	Нет	Да (опционально)			Нет	Да (опционально)	
Дисковые накопители	240 Гбайт SSD		128 Гбайт eMMC			64 Гбайт eMMC	32 Гбайт eMMC	
Горячая замена вентиляторов	Нет					Без вентилятора		
Производительность	CN-Series	VM-50/VM-50 Lite	VM-100/VM-200	VM-300/VM-1000-HV		VM-500	VM-700	
Режим анализа приложений App-ID (arpmix)	500 Мбит/с	200 Мбит/с	2 Гбит/с	4 Гбит/с		8 Гбит/с	16 Гбит/с	
Режим блокировки всех угроз (arpmix)	250 Мбит/с	100 Мбит/с	1 Гбит/с	2 Гбит/с		4 Гбит/с	8 Гбит/с	
Пропускная способность IPsec VPN	Не применимо	100 Мбит/с	1 Гбит/с	1,8 Гбит/с		4 Гбит/с	6 Гбит/с	
Новых L7 сессий в секунду ^A	Не применимо	3 000	15 000	30 000		60 000	120 000	
Максимум сессий	20 000	64 000/50 000	250 000	819 200		2 000 000	10 000 000	
Поддерживается ЦП	2 (CN-MGMT) + 1 (CN-NGFW)	2 ^G	2	2, 4		2, 4, 8	2, 4, 8, 16	
Выделенная память (минимум)	2 Гбайт (CN-MGMT) + 2 Гбайт (CN-NGFW)	4,08/4,5 Гбайт	6,5 Гбайт	9 Гбайт		16 Гбайт	56 Гбайт	
Выделенная емкость диска (минимум)	50 Гбайт	32 Гбайт ^H	60 Гбайт	60 Гбайт		60 Гбайт	60 Гбайт	
Поддерживаемые среды	—	VM-50/VM-50 Lite	VM-100/VM-200	VM-300/VM-1000-HV		VM-500	VM-700	
Частное облако								
1. VMware NSX-V	—	Нет				Да	Нет	
2. VMware NSX-T	—	Нет				Да		
3. Cisco ACI	—				Да			
4. OpenStack	—				Да			
5. Nutanix AOS	—				Да			
Гипервизор								
1. VMware ESXi	—				Да			
2. KVM на CentOS/RHEL и Ubuntu LTS	—				Да			
3. Microsoft Hyper-V	—				Да			
Публичное облако								
1. Amazon Web Services (AWS)	—	Нет	BYOL ^I или VM-Series ELA	PAYG (VM-300), BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	
2. Microsoft Azure	—	Нет	BYOL или VM-Series ELA	PAYG (VM-300), BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	
3. Google Cloud Platform (GCP)	—	Нет	BYOL или VM-Series ELA	PAYG (VM-300), BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	
4. Oracle Cloud	—	Нет	BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	
5. Alibaba Cloud	—	Нет	BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	BYOL или VM-Series ELA	

(A) Производительность виртуальных NGFW VM-series зависит от инфраструктуры виртуализации (гипервизор/облако). Подробная информация о производительности и тестировании представлена в отдельных технических проспектах. (B) Каждый результат в этом столбце относится к оптимальному сочетанию заполненных карт PA-7000-DPC-A и PA-7000-100G-NPC-A во всех доступных разьемах. (C) Все тесты выполнены с использованием двух сетевых карт + 4 заполненных перфокарт, если не указано иное. (D) Этот тест выполнен с использованием 1 сетевой карты + 5 заполненных перфокарт. (E) Для добавления виртуальных систем к базовому количеству необходимо приобрести отдельную лицензию. (F) Оптические или медные трансиверы приобретаются отдельно. (G) Превышение лимита ЦП возможно при использовании до 5 экземпляров в двухпроцессорной конфигурации. (H) При первоначальной загрузке требуется 60 Гбайт. После активации лицензии VM-Series будет использовать 32 Гбайта. (I) Вариант развертывания с использованием имеющейся лицензии (Bring your own license). (J) Вариант развертывания с оплатой по мере использования (Pay as you go).

Таблица 2. Главные функции

Межсетевой экран нового поколения	Поддерживается во всех моделях
Глубокая инспекция и контроль тысяч приложений, возможности создавать пользовательские приложения и управлять неизвестными приложениями с помощью политик, оптимизатор политик.	✓
Идентификация и контроль пользователей: VPN, контроллеры WLAN, портал авторизации, прокси-серверы, Active Directory, eDirectory, Exchange, VDI, анализ системных журналов, XML API.	✓
Расшифрование и инспекция TLS/SSL (входящий и исходящий трафик); включает поддержку инспекции протоколов TLS 1.3 и HTTP/2; статистика и журналирование параметров SSL инспекции.	✓
Сеть: динамическая маршрутизация (RIP, OSPF, BGP, MultiProtocol-BGP), DHCP, DNS, NAT, перераспределение маршрутов, ECMP, LLDP, инспекция содержимого туннелей.	✓
Качество обслуживания QoS: управление полосой пропускания трафика с помощью политик (приоритеты, гарантированная скорость, максимум) для каждого приложения, пользователя, туннеля, на основе классификации DSCP.	✓
Виртуальные системы: логические отдельно управляемые экземпляры межсетевых экранов на базе одного физического межсетевого экрана, с разделением трафика и политик каждой виртуальной системы.	✓
Сегментация сети по зонам; защита от DoS атак.	✓
Предотвращение угроз (требуется подписка)	
Антивирус: встроенная защита от вредоносного ПО, обновляемая автоматически за счет ежедневно обновляемых сигнатур, разрабатываемых собственной исследовательской лабораторией.	✓
IPS: защита от эксплойтов и методик обхода с учетом уязвимостей на уровне сети и приложений, включая сканирование портов, переполнение буфера, фрагментацию пакетов и обфускацию.	✓
Anti-Spyware: блокировка командных центров бот-сетей для предотвращения кражи данных или доставки вредоносной полезной нагрузки; идентификация зараженных узлов с помощью DNS Sinkholing.	✓
Продвинутая фильтрация URL (требуется подписка)	
Автоматическое предотвращение веб-атак, включая фишинговые ссылки в электронных письмах и на фишинговых сайтах, командных центры на основе HTTP и страниц, содержащих эксплойты.	✓
Блокировка утечек учетных записей и паролей на фишинговых ресурсах.	✓
Настраиваемые категории URL, оповещения и страницы с уведомлениями.	✓
Определения категорий вредоносных веб-сайтов в режиме реального времени с использованием алгоритмов Машинного обучения, включая бессигнатурное определение вредоносных скриптов в реальном времени	✓
Безопасность Интернета вещей (требуется подписка)	
Точная идентификация и классификация всех устройств IoT в сети, включая ранее не известные, используется Машинное обучение	✓
Защита устройств путем обнаружения аномалий с помощью машинного обучения, оценки уязвимостей, рекомендованных политик с учетом риска и применения политик Device-ID (применение политик на уровне устройств недоступно для VM-50, VM-50 Lite или CN-Series).	✓
Для активации функции в межсетевых экранах нового поколения дополнительная инфраструктура не требуется.	✓
Защита от вредоносного ПО WildFire (требуется подписка)	
Обнаружение атак и эксплойтов нулевого дня с помощью техники многоуровневого анализа, встроенный механизм Machine Learning для обнаружения неизвестного вредоносного кода на лету.	✓
Автоматическое предотвращение большинства угроз за считанные секунды в сетях, на конечных устройствах и в облачных средах.	✓
Обмен найденными сигнатурами между клиентами для защиты (более 30 000 подписчиков).	✓
Аналитика угроз AutoFocus (требуется подписка)	
Контекстуализация и классификация атак, включая семейство вредоносного ПО, злоумышленника и вредоносную кампанию, для ускорения расследования и реагирования.	✓
Глубокий анализ угроз и сопоставление с глобальными данными, получаемыми от WildFire.	✓
Автоматическое предотвращение с использованием сторонних данных об угрозах.	✓
Безопасность DNS (требуется подписка)	
Автоматическая защита от десятков миллионов вредоносных доменов, выявленных с помощью анализа в режиме реального времени и постоянно растущей глобальной экосистемы аналитики угроз.	✓
Быстрое обнаружение атак C2 и утечек данных, при которых используется туннелирование DNS, DGA, FastFlux, DNS-rebinding и многое другое с помощью анализа на базе Машинного обучения	✓
Автоматический динамический поиск зараженных машин и быстрое реагирование с помощью политик.	✓
Фильтрация файлов и данных (для расширенных DLP функций требуется подписка)	
Двунаправленный контроль несанкционированной передачи файлов, номеров социальных и кредитных карт, а также нестандартных комбинаций данных.	✓
Функционал SD-WAN (требуется подписка)	
Сетевая защита конечных устройств с помощью клиентов GlobalProtect (требуется подписка для отдельного функционала)	
VPN для удаленного доступа (SSL, IPsec, без клиента); предотвращение мобильных угроз и применение корпоративных политик к мобильным устройствам с учетом приложений, пользователей, контента, устройств и их состояния.	✓
BYOD: VPN на уровне приложений для конфиденциальности данных пользователей	✓
Управление сетевой безопасностью с помощью Rapogata (для управления несколькими межсетевыми экранами требуется подписка)	
Интуитивно понятный контроль на базе политик, охватывающий приложения, пользователей, защиту от сложных угроз, контроль URL, типов файлов и комбинаций данных — всё в одной политике.	✓
Графическая аналитика трафика и угроз с помощью Application Command Center (ACC); полностью настраиваемые отчеты.	✓
Агрегирование журналов и корреляция событий.	✓
Согласованное масштабируемое управление аппаратными межсетевыми экранами (до 30 000 штук) и всеми межсетевыми экранами VM-Series; контроль доступа на базе ролей; логическая и иерархическая группировка устройств; шаблоны настроек.	✓
Графический интерфейс пользователя, интерфейс командной строки и REST API на базе XML.	✓

© Palo Alto Networks, Inc., 2021. (PAN-OS® 10.1) Только для сравнения. Актуальные сведения представлены в спецификации конкретного продукта.

