# Arbor Networks APS

Непрерывная и Надёжная защита от DDoS-атак

## ОСНОВНЫЕ ФУНКЦИИ И ПРЕИМУЩЕСТВА

**Непрерывная защита от DDoS-атак**
Надёжная защита от всех типов DDoS-атак (объёмных, истощающих ресурсы и уровня приложений).

**Защита входящего и исходящего трафика**
Предотвращение входящих DDoS-атак и исходящей вредоносной активности от скомпрометированных внутренних хостов.

**Облачная сигнализация**
При необходимости, отправка сигнала к вышестоящему ISP (или Arbor Cloud) для подавления объёмных атак, с которыми не справится защита на площадке.

**ATLAS Intelligence Feed**
Защита, основанная на уникальных данных об угрозах от Arbor's Security & Engineering Response Teams (ASERT).

**Сервис управления APS (mAPS)**
Использование опыта и экспертизы лидера индустрии компании Arbor networks для управления и оптимизации вашей защиты от DDoS-атак.

**Дешифрация SSL**
Предотвращение DDoS-атак, скрытых в зашифрованном трафике.

**Поддержка IPV6**
Детектирование и противодействие IPv4 и IPv6 DDoS-атакам.

**Поддержка Виртуальных Сред**
Воспользуйтесь преимуществами виртуализации чтобы быстро задействовать защиту от DDoS-атак.
vAPS - это виртуальная версия устройства APS, которая поддерживает гипервизоры VMware vSphere, KVM hypervisors и VNF orchestration через Cloud-Init и OpenStack.

ARBOR NETWORKS
The Security Division of NETSCOUT

По мере увеличения зависимости от веб-приложений и сервисов, растёт риск возникновения распределённых атак в обслуживании (DDoS-атак). В последнем отчёте (*Worldwide Infrastructure Security Report)* от компании Arbor Networks, респонденты сообщили о возросшем количестве многовекторных атак — таких как ботнеты или вредоносное ПО в сочетании с DDoS-атаками. Также продолжает расти размер более традиционных объёмных DDoS-атак. Портфолио решений Arbor Networks позволяет справляться с этими продвинутыми угрозами, предоставляя полный обзор сетевой активности для быстрого исправления и блокировки атак на уровне экспертов.

Arbor Networks® APS помогает защитить непрерывность работы и доступность бизнеса от растущего спектра DDoS-атак и других продвинутых угроз. Данный продукт предоставляет самую передовую и современную технологию в мире по обнаружению и устранению атак на простой в развёртывании платформе, предназначенной для автоматической нейтрализации IPv4 и IPv6 атак, до того, как они смогут причинить ущерб критическим приложениям и сервисам.

Благодаря возможностям ATLAS® Intelligence Feed, обновления в реальном времени, содержащие информацию о DDoS-атаках и продвинутых угрозах, могут помочь в предотвращении проникновения зловредного трафика в вашу сеть.

Такие возможности как:

- DDoS защита от активных ботнетов
- DDoS защита от активных DDoS кампаний, основанных на репутации IP
- Продвинутый сервис поисковых роботов( web crawler service)
- Геолокация IP
- Репутация Доменов и IP для блокировки угроз

APS расширяет ваши возможности, используя Облачную Сигнализацию (Cloud Signaling™), чтобы связать вашу локальную защиту от DDoS-атак с сервисом от оператора связи (ISP). С Облачной Сигнализацией, APS автоматически оповещает вышестоящего сервисного оператора (ваш ISP или Arbor Cloud℠), если большие по объёму атаки угрожают доступности. Это позволяет сократить время для подавления атак.


*Полностью интегрированное решение 1) APS на площадке для непрерывной защиты от DDoS-атак уровня приложений; 2) Интеллектуальная Облачная Сигнализация 3) ISP или Arbor Cloud для подавления больших атак—с использованием глобального анализа угроз от ATLAS/ ASERT—предлагая наиболее эффективное решение по защите от DDoS-атак в отрасли.*

## Аппаратные платформы Arbor Networks APS

| Параметры | 2600 Серия | 2800 Серия |
|---|---|---|
| **Габариты** | **Шасси:** Высота 2U rack; **Высота:** 3.45 дюйма (8.67 cm); **Ширина:** 17.4 дюйма (43.53 cm) | |
| | **Глубина:** 20 дюймов (50.8 cm); **Вес:** 16.76 kg | |
| **Электропитание** | **БП постоянного тока:** 2 x DC с резервированием и возможностью горячей замены<br>**Номинальная мощность:** от -48 до -72 В, 30 А max.(на блок)<br>**БП переменного тока:** 2 x AC с резервированием и возможностью горячей замены<br>**Номинальная мощность:** от 100 до 240 Вольт, от 50 до 60 Hz, 12/6 А max (на блок) | |
| **Жесткие диски** | 2 x 120 ГБ SSD в RAID 1 | 2 x 240 ГБ SSD в RAID 1 |
| **Окружающая среда** | **Рабочий диапазон:** Температура -5º to 55ºC, Влажность 5 to 85% без конденсации<br>**Рабочий хранения:** Температура -40º to 70ºC, Влажность 95% без конденсации | |
| **Оперативная память** | 32 ГБ | 64 ГБ |
| **Процессор** | 2 x Intel Xeon (6 ядер) E52608L v3 | Dual Intel Xeon (12 ядер) E52648L v3 |
| **Операционная система** | ArbOS® Операционная система собственной разработки | |
| **Интерфейсы управления** | 2 x 10/100/1000 BaseT медь; RJ-45 последовательный консольный порт | 2 x 10/100/1000 BaseT медь; RJ-45 последовательный консольный порт |
| **Интерфейсы защиты (варианты компоновки)** | • 4 x 1GE, 8 x 1GE или 12 x 1GE (медь, оптика SX, оптика SX)<br>• 4 x 10 GE плюс 0 или 4 x 1GE или 8 x 1GE (медь, оптика SX, оптика LX) | • 4 x 10 GE (SR или LR оптика на выбор)<br>• 8 x 10 GE (SR или LR оптика на выбор)<br>• 8 x 10 GE (SR или LR оптика на выбор), плюс 4 x 1 GE (медь, SX оптика, LX оптика) |
| **Варианты Bypass** | Встроенный аппаратный bypass; Внутренний программный bypass для передачи трафика без инспекции | |
| **Задержка** | менее 80 микросекунд | |
| **Отказоустойчивость** | Аппаратный bypass, два источника электропитания, RAID массив из SSD дисков | |
| **Наработка на отказ** | 44 000 часов | |
| **Соответствие нормативам** | UL60950-1/CSA 60950-1 (США/Канада); EN60950-1 (Европа); IEC60950-1 (Международный), CB Сертификат и Отчет включающий все международные подразделения; GS Сертификат (Германия); Соответствие EAC-R (Россия); CE— Директива по слаботочным системам 73/23/EEE (Европа); BSMI CNS 13436 (Тайвань); KCC (Южная Корея); RoHS Директива 2002/95/EC (Европа) | |
| **Инспектируемая пропускная способность** | Лицензии на 100 Мбит/с, 500 Мбит/с, 1 Гбит/с, 2 Гбит/с, 5 Гбит/с, 10 Гбит/с, 15 Гбит/с, 20 Гб/с | Лицензии на 10 Гбит/с, 20 Гбит/с, 30 Гбит/с, 40 Гбит/с; программное наращивание мощности |
| **Максимальная скорость очистки от DDoS флуда** | До 15 Мпакетов/с | До 28.80 Мпакетов/с |
| **Количество одновременных соединений** | Не применимо, APS не отслеживает соединения | |
| **HTTP(s) Соединений/Сек** | 368 000 для рекомендуемого уровня защиты;<br>613 000 с использованием только списка фильтрации | 1 351 000 для рекомендуемого уровня защиты;<br>1 497 000 с использованием только списка фильтрации |
| **Возможности SSL Дешифрования** | **Инспектируемая полоса:** варианты на 750 Мбит/с и 5 Гбит/с<br>**HTTPS Соединений:** До 7 500<br>(750M HSM) или 45 000 (5G HSM)<br>**Параллельных сессий:** До 150 000 | **Инспектируемая полоса:** До 5 Гбит/с<br>**HTTPS Соединений:** До 45,000<br>**Параллельных сессий:** До 150,000 |
| | FIPS 140-2 Level 2 and 3 support; Separate “Trusted-Path” Administration for FIPS 140-2 Level 3; Secure tamper-proof enclosure; Keys cleared if enclosure breached; Power: <25 Watts; Operating Temperature: 0 to 50 C; Regulatory Compliance: CTUVus UL (USA/Canada), FCC / ICES Class A | |
| **Количество защищаемых объектов** | Не ограничено | |
| **Аутентификация** | На устройстве, RADIUS; TACACS | |
| **Протоколы управления** | SNMP-gets v1, v2c; SNMP-traps v1, v2c, v3; HTTPS; SSH, поддержка политик разграничения прав | |
| **Количество групп защиты** | 50 | |
| **Отчеты и аналитические данные** | Отчеты IPV4 и IPV6 о трафике в реальном времени и по архивным данным, максимально детализированные отчеты по группам защиты и заблокированным сетевым элементам, включая весь объем трафика (пропущенного и блокированного), наиболее часто использованные адреса URL, службы, домены, типы атак, блокированные источники, самые популярные источники с разбивкой по географии. Возможность анализировать пакеты в режиме реального времени. | |
| **Защита от DDoS атак** | Защита от атак типа TCP/UDP/HTTP(s)-флуд, ботнетов, хактивизма, поведенческая защита хостов, защита от подделки IP (спуфинга); настраиваемая фильтрация трафика по регулярным выражениям, включая содержимое пакетов, постоянные и обновляющиеся черные и белые списки, управление пропускной способностью, многоуровневая защита HTTP, DNS и SIP, ограничение TCP-соединений, защита от атак фрагментированными пакетами, защита от атак с установлением большого количества сессий. | |
| **Режимы работы** | Активный при установке в разрыв; Неактивный при установке в разрыв (создает отчеты, но не блокирует); мониторинг при подключении на SPAN-порт | |
| **Уведомления** | SNMP trap, syslog, email | |
| **Cloud Signaling** | Поддерживается протокол облачной сигнализации для подавления DDoS атак совместно с сервис провайдером (ISP) или Arbor Cloud | |
| **Web-Based GUI** | Многоязыковой пользовательский интерфейс (поддержка русского языка) | |
| **Поддерживаемые браузеры** | Internet Explorer v10-11, Firefox ESR v31, Firefox v40, Chrome v44, Safari v6 | |

### ВИРТУАЛЬНЫЙ APS (vAPS)

| Параметры | Гипервизоры | |
|---|---|---|
| **Hypervisor** | VMware vSphere 5.5+ | KVM kernel 3.19 QEMU 2.0 |
| **Минимальные требования** | **vCPUs:** 4; **NICs:** 1 to 10; **Память:** 12 GB; **Хранилище:** 100 GB | |
| **Полоса инспектирования** | 1 Гбит/с на экземпляр виртуальной машины | |
| **Максимальная скорость обработки DDoS флуда** | 910 Кпакетов/с на экземпляр виртуальной машины | 600 Кпакетов/с на экземпляр виртуальной машины |
| **Максимальная полоса пропускания на сервер** | 4 Гбит/с, 2.40 Мпакетов/с | |
| **Virtual Network Function (VNF) Orchestration** | Cloud-Init v0.7.6, Openstack Kilo и Mitaka | |

ARBOR NETWORKS
The Security Division of NETSCOUT

**Corporate Headquarters**
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

www.arbornetworks.com

**North America Sales**
Toll Free +1 855 773 9200

**Europe**
T +44 207 127 8147

**Asia Pacific**
T +65 68096226