Серия PA-4000

Основные особенности межсетевого экрана нового поколения серии PA-4000:

КЛАССИФИКАЦИЯ ВСЕХ ПРИЛОЖЕНИЙ, НА ВСЕХ ПОРТАХ, В ЛЮБОЕ ВРЕМЯ С ПОМОЩЬЮ APP-ID™.

- Идентификация приложения независимо от порта, шифрования (SSL или SSH) и используемой техники маскировки.
- Принятие всех решений в области безопасности на основе данных о приложении, а не порта: разрешение, запрет, планирование, проверка, формирование трафика.
- Классификация неидентифицированных приложений в целях контроля соблюдения правил, исследования угроз, создания пользовательских сигнатур или захвата пакетов для разработки сигнатур.

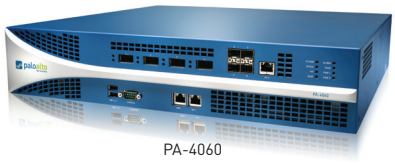
ВОЗМОЖНОСТЬ РАСПРОСТРАНЕНИЯ ПРАВИЛ БЕЗОПАСНОГО РАЗРЕШЕНИЯ ДОСТУПА ПРИЛОЖЕНИЯМ НА ЛЮБОГО ПОЛЬЗОВАТЕЛЯ И ЛЮБОЕ МЕСТО С ПОМОЩЬЮ USER-ID™ И GLOBALPROTECT™.

- Безагентская интеграция с Active Directory, LDAP, eDirectory Citrix и службами терминалов Microsoft.
- Интеграция с NAC, беспроводным 802.1X и другими нестандартными пользовательскими репозиториями с помощью XML API.
- Применение согласованных правил для локальных и удаленных пользователей, работающих на платформах Microsoft Windows, Mac OS X, Linux, Android или iOS.

ЗАЩИТА ОТ ВСЕХ УГРОЗ – КАК ИЗВЕСТНЫХ, ТАК И НЕИЗВЕСТНЫХ – С ПОМОЩЬЮ CONTENT-ID™ И WILDFIRE™.

- Блокирование широкого спектра известных угроз, включая вторжения, вредоносное и шпионское ПО, на всех портах, независимо от общей применяемой тактики маскировки угроз.
- Ограничение несанкционированной передачи файлов и конфиденциальных данных и контроль пользования Интернетом в целях, не связанных с работой.
- Идентификация неизвестных вредоносных программ, анализ с целью выявления более чем 100 типов вредоносного поведения, автоматическое создание и добавление сигнатур при очередном обновлении.

paloalto NETWORKS
the network security company™


PA-4060


PA-4050


PA-4020

Решение серии PA-4000 от Palo Alto Networks™ состоит из трех высокопроизводительных платформ, PA-4060 и PA-4050, каждая из которых ориентирована на использование в высокоскоростных центрах обработки данных и интернет-шлюзах. Система серии PA-4000 имеет пропускную способность до 10 Гбит/с благодаря использованию выделенных вычислительных ресурсов и памяти для организации работы сети, обеспечения безопасности, предотвращения угроз и осуществления управления.

Высокоскоростная панель физически разделена на отдельные панели для данных и управления, тем самым гарантируя непрерывную возможность осуществления управления, независимо от интенсивности трафика. Система серии PA-4000 на основе PAN-OS™, операционной системы для обеспечения безопасности, которая позволяет безопасно разрешать доступ приложениям с помощью App-ID, User-ID, Content-ID, GlobalProtect и WildFire.

ПРОИЗВОДИТЕЛЬНОСТЬ И ПРОПУСКНАЯ СПОСОБНОСТЬ[1]	PA-4060	PA-4050	PA-4020
Пропускная способность межсетевого экрана (при включенном App-ID)	10 Гбит/с	10 Гбит/с	2 Гбит/с
Пропускная способность при предотвращении угроз	5 Гбит/с	5 Гбит/с	2 Гбит/с
Пропускная способность IPSec VPN	2 Гбит/с	2 Гбит/с	1 Гбит/с
Число новых сеансов в секунду	60 000	60 000	60 000
Макс. кол-во сеансов	2 000 000	2 000 000	500 000
Число IPSec VPN туннелей/туннельных интерфейсов	4 000	4 000	2 000
Число одновременных пользователей GlobalProtect (SSL VPN)	10 000	10 000	5 000
Число сеансов расшифровки SSL	23 000	23 000	7 500
Число входящих сертификатов SSL	300	300	25
Число виртуальных маршрутизаторов	125	125	20
Число виртуальных систем (базовый вариант/макс.[2])	25/125	25/125	10/20
Число зон безопасности	500	500	80
Макс. кол-во политик	20 000	20 000	10 000

[1] Производительность и пропускная способность измеряются в идеальных условиях тестирования с использованием PAN-OS 5.0.

[2] Для добавления к базовому варианту дополнительных виртуальных систем необходимо купить отдельную лицензию.

Полное описание характеристик межсетевого экрана нового поколения серии PA-4000 можно найти по адресу: www.paloaltonetworks.com/literature.

СПЕЦИФИКАЦИИ ОБОРУДОВАНИЯ

ИНТЕРФЕЙСЫ

- PA-4060: (4) 10-гигабитный XFP-модуль, (4) Гигабитный SFP-модуль
- PA-4050/PA-4020: (16) 10/100/1000, (8) Гигабитный SFP-модуль

ИНТЕРФЕЙСЫ СИСТЕМЫ УПРАВЛЕНИЯ

- (2) 10/100/1000 высокой готовности, (1) 10/100/1000 управление по вспомогательному каналу, (1) порт консоли DB9

ЕМКОСТЬ

- Жесткий диск емкостью 160 Гбайт

ПИТАНИЕ (СРЕДНЯЯ/МАКСИМАЛЬНАЯ ПОТРЕБЛЯЕМАЯ МОЩНОСТЬ)

- 400 Вт переменного тока с резервированием (175 Вт/200 Вт)

МАКС. ТЕПЛОВЫДЕЛЕНИЕ (БТЕ/Ч)

- 682

ВХОДНОЕ НАПРЯЖЕНИЕ (ЧАСТОТА ВХОДНОГО СИГНАЛА)

- 100-240 В переменного тока (50-60 Гц)

МАКСИМАЛЬНЫЙ ПОТРЕБЛЯЕМЫЙ ТОК

- 2,5 А при 100 В переменного тока

НАРАБОТКА НА ОТКАЗ

- 7,18 лет

МАКС. ПУСКОВОЙ ТОК

- 50 А при 230 В переменного тока; 30 А при 120 В переменного тока

ВОЗМОЖНОСТЬ УСТАНОВКИ В СТОЙКУ (ГАБАРИТЫ)

- 2U, стандартная 19-дюймовая стойка (3,5 (В) x 16,5 (Г) x 17,5 (Ш) дюйма)

ВЕС (РАСПАКОВАННОЕ/УПАКОВАННОЕ)

- 14,97 кг/18,14 кг

БЕЗОПАСНОСТЬ

- UL, CUL, CB

ЭЛЕКТРОМАГНИТНЫЕ ПОМЕХИ

- FCC класса A, CE класса A, VCCI класса A

СЕРТИФИКАЦИЯ

- FIPS 140 уровня 2, общие критерии EAL2, ICSA, UCAPL

УСЛОВИЯ ЭКСПЛУАТАЦИИ

- Возможная температура окружающей среды при эксплуатации: от 0 до 50 °C
- Возможная температура окружающей среды при хранении: от -20 до 70 °C

СЕТЕВЫЕ ПАРАМЕТРЫ

ИНТЕРФЕЙСНЫЕ РЕЖИМЫ

- Второго уровня, третьего уровня, Tap, виртуальный провод (прозрачный режим)

МАРШРУТИЗАЦИЯ

- Режимы: OSPF, RIP, BGP, статический
- Размер таблицы переадресации (элементов на устройство/на VR): 20 000/20 000 (PA-4060, PA-4050), 10 000/10 000 (PA-4020)
- Переадресация на основе политик
- Протокол точка-точка через Ethernet (PPPoE)
- Jumbo-кадры: максимальный размер кадра 9 210 байтов
- Многоадресная рассылка: PIM-SM, PIM-SSM, IGMP v1, v2 и v3

ВЫСОКАЯ ГОТОВНОСТЬ

- Режимы: активный/активный, активный/пассивный
- Обнаружение сбоев: мониторинг пути, мониторинг интерфейса

НАЗНАЧЕНИЕ АДРЕСОВ

- Назначение адреса для устройства: DHCP-клиент/PPPoE/статический
- Назначение адреса для пользователей: DHCP-сервер/DHCP-реле/статический

IPV6

- Второго уровня, третьего уровня, Tap, виртуальный провод (прозрачный режим)
- Функции: App-ID, User-ID, Content-ID, WildFire и расшифровка SSL

VLAN

- VLAN-тегов 802.1q на устройство/на интерфейс: 4,094/4,094
- Макс. кол-во интерфейсов: 4 096 (PA-4060, PA-4050), 2 048 (PA-4020)
- Объединенные интерфейсы (802.3ad)

NAT/PAT

- Макс. кол-во правил NAT: 4 000 (PA-4060, PA-4050), 1 000 (PA-4020)
- Макс. кол-во правил NAT (DIPP): 250 (PA-4060, PA-4050), 200 (PA-4020)
- Динамический пул IP-адресов и портов: 254
- Динамический пул IP-адресов: 16,234
- Режимы NAT: 1:1 NAT, n:n NAT, m:n NAT
- Превышение лимита подписки DIPP (уникальных IP-адресов пункта назначения в расчете на порт-источник и IP): 8 (PA-4060, PA-4050), 4 (PA-4020)
- NAT64

ВИРТУАЛЬНЫЙ ПРОВОД

- Макс. кол-во виртуальных проводов: 2048 (PA-4060, PA-4050, 1024 (PA-4020)
- Типы интерфейсов, закрепленные за виртуальными проводами: физические и субинтерфейсы

ПЕРЕАДРЕСАЦИЯ ВТОРОГО УРОВНЯ

- Размер таблицы ARP на устройство: 20 000 (PA-4060, PA-4050), 10 000 (PA-4020)
- Размер таблицы MAC на устройство: 20 000 (PA-4060, PA-4050), 10 000 (PA-4020)
- Размер таблицы соседних элементов IPv6: 5 000 (PA-4060, PA-4050), 2 000 (PA-4020)

БЕЗОПАСНОСТЬ

МЕЖСЕТЕВОЙ ЭКРАН

- Управление приложениями, пользователями и контентом на основе политик
- Защита фрагментированных пакетов
- Защита от шпионского сканирования
- Защита от атак, связанных с отказом в обслуживании (DoS)/распределенных атак, связанных с отказом в обслуживании (DDoS)
- Дешифровка: SSL (входящий и исходящий трафик), SSH

WILDFIRE

- Идентификация и анализ известных и неизвестных файлы на предмет более чем 100 видов вредоносного поведения
- Создание и автоматическая установка защиты от недавно обнаруженных вредоносных программ через обновление сигнатур
- Обновление сигнатур менее чем в течение 1 часа, интегрированное создание/отправка отчетов; доступ к WildFire API для программной отправки до 100 образцов и до 250 отчетов с помощью хэша файлов в день (требуется подписка)

ФИЛЬТРАЦИЯ ФАЙЛОВ И ДАННЫХ

- Передача файлов: двунаправленный контроль более чем 60 уникальных типов файлов
- Передача данных: двунаправленный контроль несанкционированной передачи номеров кредитных карт и номеров социального страхования
- Защита от скрытой загрузки

ПОЛЬЗОВАТЕЛЬСКАЯ ИНТЕГРАЦИЯ (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One и другие службы каталогов на основе LDAP
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Службы терминалов Microsoft, Citrix XenApp
- Использование интерфейса API XML для интеграции с нестандартными пользовательскими репозиториями

IPSEC VPN (САЙТ-САЙТ)

- Обмен ключами: ручной ключ, IKE v1
- Шифрование: 3DES, AES (128-битное, 192-битное, 256-битное)
- Аутентификация: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Создание динамических VPN-туннелей (GlobalProtect)

ПРЕДОТВРАЩЕНИЕ УГРОЗ (ТРЕБУЕТСЯ ПОДПИСКА)

- Защита от уязвимостей приложений, операционной системы
- Защита от вирусов на основе потоков (в том числе от вирусов, встроенных в HTML, Javascript, PDF и вирусов в сжатых файлах), программ-шпионов, червей

ФИЛЬТРАЦИЯ URL-АДРЕСОВ (ТРЕБУЕТСЯ ПОДПИСКА)

- Предопределенные и пользовательские категории URL-адресов
- Кэш в устройстве для недавно открывавшихся URL-адресов
- Категория URL-адресов как часть критериев сопоставления при обеспечении безопасности
- Информация о времени доступа к страницам

КАЧЕСТВО ОБСЛУЖИВАНИЯ (QOS)

- Формирование трафика на основе политик, учитывающих такие критерии, как пользователь, источник, назначение, интерфейс, VPN-туннель IPSec и др.
- 8 классов трафика с гарантированными, максимальными и приоритетными параметрами пропускной способности
- Средство мониторинга пропускной способности в реальном времени
- Маркировка приоритизированных служб на основе политик
- Кол-во поддерживаемых физических интерфейсов для качества обслуживания: 12

SSL VPN/УДАЛЕННЫЙ ДОСТУП (GLOBALPROTECT)

- Шлюз GlobalProtect
- Портал GlobalProtect
- Передача данных: IPSec с резервным режимом SSL
- Аутентификация: LDAP, SecurID или локальная БД
- Клиентская ОС: Mac OS X 10.6, 10.7 (32/64-разрядная), 10.8 (32/64-разрядная), Windows XP, Windows Vista (32/64-разрядная), Windows 7 (32/64-разрядная)
- Поддержка сторонних клиентов: Apple iOS, Android 4.0 и последующих версий, VPNC IPSec для Linux

УПРАВЛЕНИЕ, СОЗДАНИЕ ОТЧЕТОВ, ИНСТРУМЕНТЫ ОБЗОРА

- Интегрированный веб-интерфейс, интерфейс командной строки или централизованное управление (Panorama)
- Многоязычный пользовательский интерфейс
- Syslog, Netflow v9 и SNMP v2/v3
- REST API на основе XML
- Графическое представление сводных данных по приложениям, URL-категориям, угрозам и данным (ACC)
- Просмотр, фильтрация и экспорт журналов фильтрации трафика, угроз, WildFire, URL и данных
- Полностью настраиваемые отчеты

Дополнительную информацию о характеристиках межсетевого экрана нового поколения серии PA-4000 можно найти по адресу: www.paloaltonetworks.com/literature.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com