Серия VM

Основные особенности межсетевого экрана нового поколения серии VM:

КЛАССИФИКАЦИЯ ВСЕХ ПРИЛОЖЕНИЙ, НА ВСЕХ ПОРТАХ, В ЛЮБОЕ ВРЕМЯ С ПОМОЩЬЮ ТЕХНОЛОГИИ 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 App-ID или захвата пакетов для дальнейшего исследования.

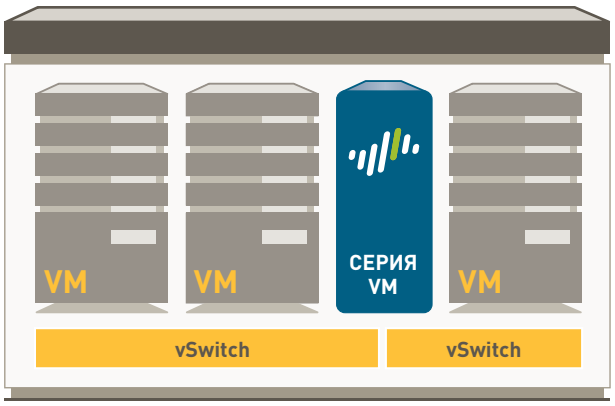
ВОЗМОЖНОСТЬ РАСПРОСТРАНЕНИЯ ПРАВИЛ БЕЗОПАСНОГО РАЗРЕШЕНИЯ ДОСТУПА ПРИЛОЖЕНИЯМ НА ЛЮБОГО ПОЛЬЗОВАТЕЛЯ И ЛЮБОЕ МЕСТО С ПОМОЩЬЮ USER-ID™ И GLOBALPROTECT™.

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

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 защиты при очередном обновлении.

paloalto NETWORKS
the network security company™



Виртуальный межсетевой экран серии VM

VM-Series от Palo Alto Networks™ расширяет сферу применения безопасного разрешения доступа приложениям в виртуализированные среды, решая ключевые проблемы обеспечения безопасности в условиях виртуализации: применение правил безопасности на виртуальных машинах, в которых используются объекты с динамическими адресами, и интеграция с системами взаимодействия с применением мощного интерфейса API управления на основе XML.

VM-Series состоит из трех высокопроизводительных моделей, VM-100 и VM-200 и VM-300, каждая из которых использует однопроходную программную архитектуру, позволяющую повысить скорость обработки данных в условиях центров обработки данных. Панели для данных и управления разделены, что позволяет пользователям устанавливать отдельные процессоры для каждой панели, тем самым гарантируя непрерывную возможность осуществления управления, независимо от интенсивности трафика. Межсетевой экран серии VM работает на основе PAN-OS™, операционной системы для систем безопасности, которая позволяет безопасно разрешать доступ приложениям с помощью App-ID, User-ID, Content-ID, GlobalProtect и WildFire.

ОБЩАЯ ПРОПУСКНАЯ СПОСОБНОСТЬ[1]	VM-300	VM-200	VM-100
Макс. кол-во сеансов	250 000	100 000	50 000
Число IPSec VPN туннелей/туннельных интерфейсов	2 000	500	25
Число одновременных пользователей GlobalProtect (SSL VPN)	500	200	25
Число сеансов расшифровки SSL	1024	1024	1024
Число входящих сертификатов SSL	25	25	25
Число виртуальных маршрутизаторов	3	3	3
Число зон безопасности	40	20	10
Макс. кол-во политик	5 000	2 000	250
Адресные объекты	10 000	4 000	2 500
ПРОИЗВОДИТЕЛЬНОСТЬ[1]			
Пропускная способность межсетевого экрана (при включенном App-ID)	1 Гбит/с		
Пропускная способность при предотвращении угроз	600 Мбит/с		
Пропускная способность IPSec VPN	250 Мбит/с		
Число новых сеансов в секунду	8000		

[1] Производительность и пропускная способность измеряются в идеальных условиях тестирования с использованием PAN-OS 5.0 и 4-ядерного процессора.

ВИРТУАЛИЗАЦИЯ	VM-300 VM-200 VM-100
HyperVisor	VMware ESXi 4.1 и ESXi 5.0
Сетевой драйвер	VMXNet3
Число ядер процессоров	2, 4 или 8
Память (мин.)	4 Гайт
Емкость диска (мин./макс.)	40 Гбайт/2 Тбайт

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): 1000/1000
- Переадресация на основе политик
- Многоадресная рассылка: PIM-SM, PIM-SSM, IGMP v1, v2 и v3

ВЫСОКАЯ ГОТОВНОСТЬ

- Режимы: активный/пассивный режим без синхронизации сеанса
- 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: 2000 (VM-300), 500 (VM-200), 100 (VM-100)

NAT/PAT

- Макс. кол-во правил NAT: 1 000 (VM-300), 1 000 (VM-200), 125 (VM-100)
- Макс. кол-во правил NAT (DIPP): 200 (VM-300), 200 (VM-200), 125 (VM-100)
- Динамический пул IP-адресов и портов: 254
- Динамический пул IP-адресов: 32,000
- 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): 2 (VM-300), 1(VM-200), 1 (VM-100)
- NAT64

ВИРТУАЛЬНЫЙ ПРОВОД

- Макс. кол-во виртуальных проводов: 1000 (VM-300), 250 (VM-200), 50 (VM-100)
- Типы интерфейсов, закрепленные за виртуальными проводами: физические и субинтерфейсы

ПЕРЕАДРЕСАЦИЯ ВТОРОГО УРОВНЯ

- Размер таблицы ARP на устройство: 2500 (VM-300), 500 (VM-200), 500 (VM-100)
- Размер таблицы MAC на устройство: 2500 (VM-300), 500 (VM-200), 500 (VM-100)
- Размер таблицы соседних элементов IPv6: 1 000 (VM-300), 500 (VM-200), 500 (VM-100)

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 1 000 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: 6 (VM-300, VM-200), 4(VM-100)

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

Полное описание характеристик межсетевого экрана нового поколения серии VM 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