PRISMA
BY PALO ALTO NETWORKS

Виртуальные межсетевые экраны нового поколения серии VM

Виртуальные межсетевые экраны нового поколения серии VM

Защищайте приложения и данные в публичных облаках, средах виртуализации и NFV.

- Идентифицируйте и контролируйте приложения, предоставляйте доступ конкретным пользователям и предотвращайте известные и неизвестные угрозы.
- Сегментируйте критически важные приложения и данные по принципу нулевого доверия для совершенствования защиты и выполнения требований регуляторов.
- Централизованно управляйте политиками как физических, так и виртуальных межсетевых экранов, чтобы обеспечить целостную защиту.
- Эффективнее автоматизируйте рабочие процессы, чтобы системы безопасности успевали за изменениями в вашем облаке.

Организации во всем мире проходят цифровую трансформацию и в результате получают более быстрые и эффективные сетевые архитектуры, включающие в себя несколько публичных облаков, локальные виртуальные ЦОДы и (в некоторых случаях) защиту как компонент виртуализации сетевых функций (NFV).

Преимущества облаков, технологий виртуализации и NFV хорошо известны, но по-прежнему остается риск утечки данных и сопутствующих бизнес-проблем. Для защиты виртуальных рабочих нагрузок и данных вашей организации требуется облачная система безопасности, которая:

- Использует удостоверения приложений для включения сегментации и составления белого списка;
- Контролирует доступ к ресурсам на основе потребностей и идентификатора пользователя;
- Блокирует вредоносному ПО доступ и боковое перемещение от одной рабочей нагрузки к другой;
- Упрощает управление и может быть полностью автоматизирована, чтобы минимизировать несогласованность действий и быстро адаптировать политики безопасности при изменении виртуальных рабочих нагрузок.

Виртуальные межсетевые экраны нового поколения серии VM от компании Palo Alto Networks поддерживают те же функции безопасности нового поколения и предотвращения современных угроз, что и наши аппаратные межсетевые экраны, что позволяет защищать приложения и данные и в сети, и в облаке.

Серия VM – защита любого облака

Организации быстро берут на вооружение мультиоблачные архитектуры, чтобы распределить риски и воспользоваться ключевыми компетенциями разных вендоров облачных технологий. Для защиты приложений и данных в публичных облаках, виртуальных центрах обработки данных и развернутых средах NFV была разработана серия VM, состоящая из 5 моделей межсетевых экранов с поддержкой App-ID и производительностью до 16 Гбит/с:

• **VM-50/VM-50 Lite** потребляют минимум ресурсов, поддерживают переподписку CPU, имеют производительность до 200 Мбит/с с поддержкой App-ID и пригодны для решения широкого спектра задач от оборудования виртуального офиса / локальной площадки заказчика до построения многопользовательских сред высокой плотности.

• **VM-100 и VM-300** оптимизированы для использования в гибридных облаках, для сегментации и в качестве интернет-шлюзов и имеют производительность 2 Гбит/с и 4 Гбит/с с поддержкой App-ID соответственно.

• **VM-500 и VM-700** имеют лучшую в отрасли производительность – 8 Гбит/с и 16 Гбит/с с поддержкой App-ID соответственно и могут развертываться как компоненты безопасности NFV в полностью виртуальном ЦОДе и инфраструктуре поставщиков услуг.

Ключевые особенности и возможности серии VM

Межсетевые экраны серии VM защищают приложения и данные с помощью функций безопасности нового поколения, которые обеспечивают превосходную визуализацию и точный контроль, а также предотвращают угрозы на уровне приложений. Функции автоматизации и централизованное управление позволяют встраивать средства защиты в процесс разработки приложений, гарантируя, что система безопасности будет развиваться теми же темпами, что и облако.

• **Визуализация приложений для принятия обоснованных решений:** Межсетевые экраны серии VM визуализируют приложения на всех портах, а значит, вы получаете гораздо более актуальную информацию об облачной среде, чтобы принимать быстрые и обоснованные решения о политиках.

• **Использование сегментации / белых списков приложений для обеспечения безопасности и соблюдения требований регуляторов:** Современные киберугрозы, как правило, сначала компрометируют отдельную рабочую станцию или пользователя, а затем выполняют боковое перемещение по сети, подвергая риску критически важные приложения и данные, где бы они ни находились. Использование политик сегментации и белых списков позволяет контролировать приложения, взаимодействующие через разные подсети, чтобы блокировать боковое перемещение угроз и соблюсти требования регуляторов.

• **Предотвращение новейших атак внутри разрешенных взаимодействий приложений:** Атаки, как и многие приложения, могут использовать любой порт, делая традиционные механизмы предотвращения неэффективными. Серия VM позволяет использовать решения Threat Prevention, DNS Security и WildFire® от Palo Alto Networks, чтобы применять к конкретным приложениям конкретные политики блокирования эксплойтов, вредоносных программ и ранее неизвестных угроз, стремящихся попасть в облако.

• **Контроль доступа к приложениям, основанный на политиках в отношении пользователей:** Интеграция с разными репозиториями пользователей, такими как Microsoft Exchange, Active Directory® и LDAP, дополняет белый список приложений, идентифицируя пользователя в качестве дополнительного элемента политики, который контролирует доступ к приложениям и данным. Если межсетевой экран серии VM развертывается вместе с Palo Alto Networks GlobalProtect™ для обеспечения сетевой безопасности на оконечном устройстве, то это позволяет распространять корпоративные политики безопасности на мобильные устройства и пользователей, независимо от их местоположения.

• **Единообразие политик благодаря централизованному управлению:** Panorama™ обеспечивает централизованное управление сетевой безопасностью для межсетевых экранов серии VM, развернутых в нескольких облачных средах, и для физических устройств безопасности, гарантируя целостность и согласованность политик. Богатые возможности централизованного журналирования и отчетности дают полную картину виртуализированных приложений, пользователей и контента.

• **Защита контейнеров для управляемых сред Kubernetes:** Межсетевые экраны серии VM защищают контейнеры, работающие в Google Kubernetes® Engine и Azure® Kubernetes Service, обеспечивая те же возможности визуализации и предотвращения угроз, которые могут защитить критически важные для бизнеса рабочие нагрузки в GCP® и Microsoft Azure. Визуализация контейнеров позволяет ИБ-специалистам принимать обоснованные решения и быстрее реагировать на возможные инциденты. Политики Threat Prevention, WildFire и URL Filtering можно использовать для защиты кластеров Kubernetes от известных и неизвестных угроз. Panorama позволяет автоматизировать обновления политик при добавлении или удалении служб Kubernetes, гарантируя постоянную защиту непрерывно меняющимся управляемым средам Kubernetes.

• **Автоматическое развертывание систем безопасности и обновление политик:** Межсетевые экраны серии VM имеют ряд функций управления, позволяющих встроить средства защиты в процессы разработки приложений.

◦ Используйте начальную загрузку, чтобы автоматически предоставить межсетевому экрану серии VM рабочую конфигурацию вместе с лицензиями, подписками и возможностью подключения к Panorama для централизованного управления.

◦ Автоматизируйте обновления политик при изменении рабочих нагрузок, используя полностью документированный API-интерфейс и динамические группы адресов (Dynamic Address Groups), чтобы межсетевые экраны серии VM могли использовать внешние данные в форме тегов, которые могут :

◦ Используйте собственные шаблоны и сервисы поставщика облачных услуг вместе со сторонними инструментами, такими как Terraform® и Ansible®, чтобы полностью автоматизировать развертывание межсетевых экранов серии VM и обновление политик безопасности.

• **Свойственная облаку масштабируемость и доступность:** В средах виртуализации или облачных средах для выполнения требований к масштабируемости и доступности можно использовать традиционный подход с двумя устройствами или облачный подход. Чтобы обеспечить масштабируемость и доступность в публичных облачных средах, мы рекомендуем использовать облачные сервисы, такие как шлюзы приложений, балансировщики нагрузки и автоматизацию.

Гибкость развертывания

Чтобы узнать больше о публичном облаке и средах виртуализации, поддерживаемых межсетевыми экранами серии VM, посетите следующие веб-страницы:

Публичное облако
- Серия VM в Microsoft Azure/AzureStack
- Серия VM в Amazon Web Services
- Серия VM в Google Cloud Platform/GKE
- Серия VM в Oracle Cloud
- Серия VM в Alibaba Cloud
- Серия VM в VMware vCloud Air

Гибридное облако
- Серия VM в VMware Cloud (VMC) в AWS

Виртуализированный ЦОД / частное облако
- Серия VM в VMware NSX for vSphere
- Серия VM в VMware ESXi
- Серия VM в Cisco ACI
- Серия VM в Microsoft Hyper-V
- Серия VM в KVM/Nutanix/OpenStack

PRISMA BY PALO ALTO NETWORKS

3000 Tannery Way Santa Clara, CA 95054
Основной номер: +1.408.753.4000
Отдел продаж: +1.866.320.4788
Служба поддержки: +1.866.898.9087
www.paloaltonetworks.com

vm-series-summary-specsheet-ds-072919