

Palo Alto Networks

Межсетевые экраны нового поколения

Ваш межсетевой экран устарел

Традиционные межсетевые экраны (файрволы) классифицируют трафик по порту и протоколу. Такая классификация была эффективна много лет назад, когда каждому приложению соответствовал свой порт и протокол.

Однако все изменилось с появлением нового поколения Интернет-приложений, использующих для своей работы порты 80 и 443, а также динамические порты.

Некоторые из этих приложений необходимы для ведения бизнеса, другие принадлежат пользователям и могут нести опасность бизнес-процессам компании.

Традиционные файрволы не могут отличить первые приложения от вторых, поэтому не могут помочь администраторам эффективно контролировать безопасность ИТ-инфраструктуры.

Технология Palo Alto

Компания Palo Alto Networks была основана в 2005 году Ниром Зуком, изобретателем технологии Stateful Inspection, и группой опытных инженеров из лидирующих компаний Кремниевой долины в сфере сетевой безопасности (Check Point, Cisco, Juniper Networks и других).

Palo Alto Networks сконцентрировала свои усилия на разработке файрволов нового поколения, позволяющих решить указанную проблему и контролировать работу приложений и пользователей в корпоративных сетях.

Преодолев ограничение классификации трафика по порту и протоколу, Palo Alto Networks выпустила семейство файрволов

нового поколения, которые применяют свои политики к конкретным приложениям, пользователям Active Directory и данным, передаваемым по сети.

Прозрачный контроль сетевой активности достигается при помощи идентификации сетевых приложений вне зависимости от порта, через который они работают, а сигнатурный и эвристический анализ позволяют идентифицировать даже приложения, использующие тактику подмены и динамического изменения портов.

Дополнительно к функциям файрвола на платформе реализован функционал защиты от уязвимостей, вирусов, вредоносного ПО, а также фильтрация URL.

Межсетевые экраны нового поколения Palo Alto позволяют ИТ-департаментам и службам информационной безопасности более эффективно контролировать риски, связанные с работой современных сетевых приложений.

Корпоративное решение

Позволяя защищать даже наиболее критичные сегменты сети, межсетевые экраны Palo Alto работают в режиме реального времени, сканируя трафик на скоростях до 20 Гбит/с.

По оценкам Gartner, компания Palo Alto Networks стала одним из лидеров отрасли в короткие сроки именно благодаря своей инновационной технологии, а клиентами компании сегодня являются крупнейшие организации сфер производства, здравоохранения, образования, ИТ-индустрии и финансовых услуг.

Возможности и преимущества

Настройка правил для конкретных пользователей, а не IP-адресов

Настройка правил для приложений, а не портов

Пропускная способность до 20 Гбит/с

Работа в реальном режиме времени

Графическое управление политиками

Защита мобильных пользователей и сотрудников, работающих из дома



Межсетевой экран Palo Alto PA-4020

Серия Palo Alto PA-5000

Серия PA-5000 разработана для защиты центров обработки данных (ЦОД), сетей крупнейших организаций и Интернет-провайдеров, где сетевая нагрузка требует предсказуемой надежности и пропускной способности межсетевого экрана и сканера угроз.

Надежная защита каналов с пропускной способностью до 20 Гбит/с обеспечивается

Серия Palo Alto PA-4000

Межсетевые экраны нового поколения Palo Alto серии PA-4000 предназначены для использования в качестве Интернет-шлюзов в крупных и средних организациях, обеспечивая защиту от угроз и сетевую безопасность.

Серия PA-4000 управляет сетевыми потоками на скорости до 10 Гбит/с с помощью

Серия Palo Alto PA-2000

Межсетевые экраны нового поколения Palo Alto серии PA-2000 включают две модели PA-2020 и PA-2050, которые специально разработаны для использования в качестве Интернет-шлюзов крупных региональных офисов и средних организаций.

Устройства обеспечивают сетевую безопасность и защиту от угроз благодаря

Серия Palo Alto PA-500

Межсетевой экран Palo Alto серии PA-500 разработан для использования в качестве Интернет-шлюза в средних региональных офисах, а также в малых и средних организациях.

Устройство обеспечивает оптимальную производительность и поддерживает

40 процессорами, распределенными между четырьмя функциональными областями: сеть, безопасность, инспекция данных и управление.

Высокая доступность обеспечивается использованием пар активный/активный и активный/пассивный, физическим разделением управляющей логики и данных, а также дублированием критичных узлов.

выделенных сетевого сопроцессора и памяти, поддерживая сетевой доступ, безопасность, нейтрализацию угроз, а также URL-фильтрацию и управление.

Физическое разнесение логики управления устройствами и обработки трафика делают устройства доступными даже при исключительно высоких сетевых нагрузках.

управлению сетевыми потоками и фильтрацию URL-адресов, пакетов и обнаружению нештатных ситуаций.

Разделение логики обработки сетевого трафика и управления устройством позволяет обеспечить дополнительную защиту и доступность консоли управления даже при высоких сетевых нагрузках.

большинство технологий, доступных в более старших моделях, в том числе фильтрация URL-адресов, разбор пакетов и идентификацию пользователей и приложений.

Технические характеристики

Пропускная способность

- Файервол: 20 Гбит/сек
- Предотвращение угроз: 10 Гбит/сек
- 4 000 000 одновременных сессий
- 120 000 новых сессий в секунду

IPsec VPN

- Пропускная способность 4 Гбит/сек
- 8 000 IPsec-туннелей
- 20 000 SSL-пользователей
- 900 зон безопасности

Маршрутизация

- OSPF, RIP, BGP, статика
- До 64 000 правил
- Поддержка политик
- PPPoE
- Jumbo Frames

VLAN

- До 4 094 тэгов 802.1q
- 4 096 интерфейсов
- Агрегация 802.3ad

Технологии

- Идентификация приложений App-ID
- Идентификация пользователей User-ID
- Идентификация содержимого Content-ID
- Перехват SSL и SSH

Интерфейсы

- 12 x 10/100/1000
- 8 x Gigabit SFP
- 4 x 10 Gigabit SFP+



Тайгер Оптикс

125040, Россия, Москва
Нижняя улица, дом 9
Тел./факс: +7 (499) 504-16-70
info@tiger-optics.ru • www.tiger-optics.ru



Palo Alto Networks

3300 Olcott Street
Santa Clara, CA, 95054
The United States
www.paloaltonetworks.com