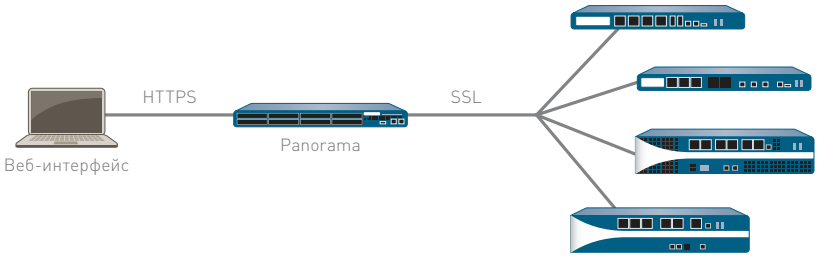
PANORAMA

Panorama обеспечивает централизованное администрирование и управление политиками безопасности межсетевых экранов следующего поколения от Palo Alto Networks.

- Просмотр графического представления сводных данных о приложениях в сети, соответствующих пользователях и потенциальных угрозах для безопасности.
- Централизованное применение политик безопасности. Обеспечение гибкости конфигурации с возможностью применения локальных политик безопасности.
- Делегирование соответствующих уровней административного контроля на уровне устройств или с помощью глобального управления на основе ролей.
- Централизованный анализ с возможностью создания отчетов о сетевом трафике, событий сетевой безопасности и изменениях конфигурации.



Как правило, большие организации в своих ЛВС используют множество межсетевых экранов, и зачастую процесс управления и контроля МЭ становится громоздким из-за сложности и несогласованности работы между отдельными устройствами. В результате приходится тратить больше усилий на администрирование, что в свою очередь увеличивает издержки.

Panorama обеспечивает централизованное управление и мониторинг для межсетевых экранов следующего поколения от Palo Alto Networks. Администраторы получают возможность централизованно отслеживать приложения, пользователей и содержимое, проходящее через межсетевой экран. Знание того, что происходит в сети, в сочетании с политиками безопасного доступа приложений позволяет усилить защиту, повысить управляемость и при этом затрачивать меньше усилий на администрирование. Администраторы могут проводить централизованный анализ, создавать отчеты и исследовать агрегированные данные за определенные промежутки времени, а также данные, хранящиеся локально на межсетевом экране.

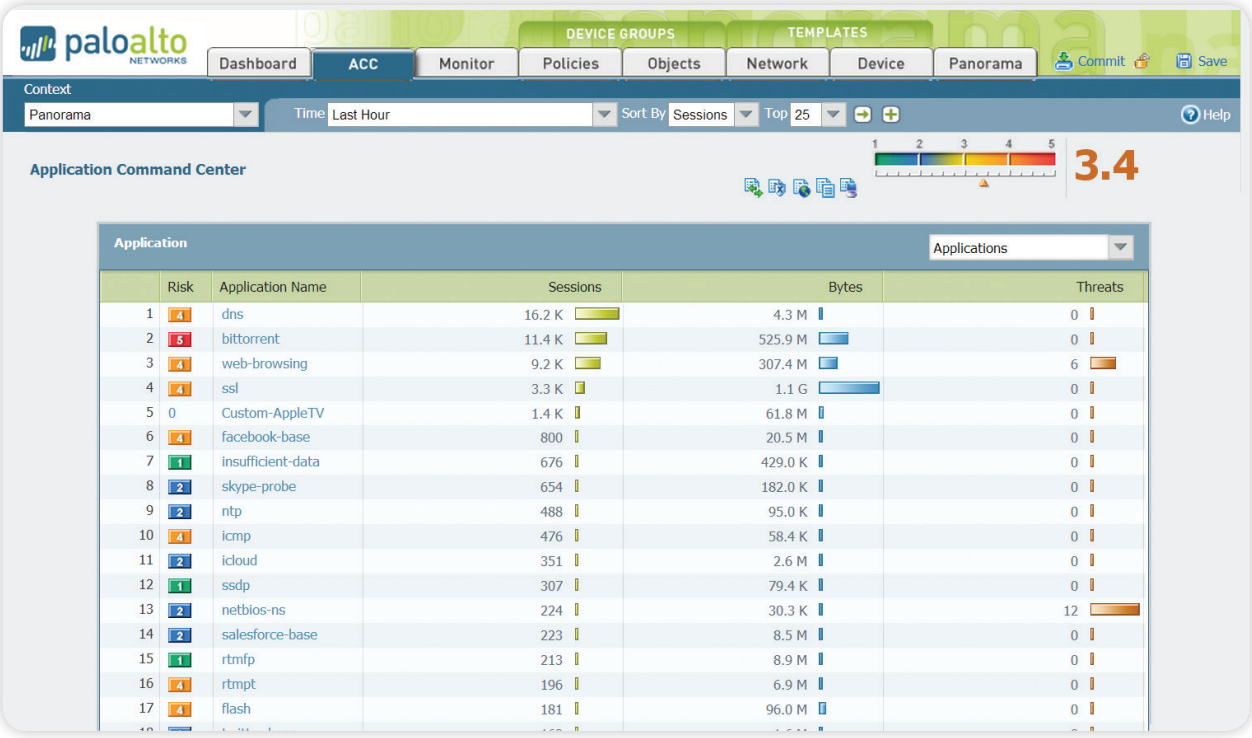
Panorama использует тот же веб-интерфейс, что и на отдельных устройствах, что сокращает необходимость в обучении и задержки в выполнении задач. Palo Alto Networks придерживается философии управления на основе согласованного подхода, что обеспечивает существенное преимущество по сравнению с предложениями конкурентов.

Централизованный мониторинг: Application Command Center

Благодаря Application Command and Control (ACC) администратор Panorama получает графическое представление всех приложений, URL-адресов, угроз и данных (файлов и шаблонов поведения), проходящих через все устройства, управляемых с помощью Panorama. ACC в динамическом режиме получает данные от каждого устройства Palo Alto Networks, обеспечивая администраторам возможность своевременного мониторинга информации о приложениях в сети, их пользователей, а также связанных с ними потенциальных угрозах. Администраторы могут анализировать новые или незнакомые приложения одним щелчком мыши, имея возможность просмотреть описание приложения, его ключевые особенности, поведенческие характеристики, а также пользователей данного приложения.

Дополнительные данные о категориях URL-адресов и угроз позволяют сформировать полное и четкое представление о ситуации в сети. Мониторинг с использованием ACC позволяет администраторам принимать взвешенные решения по определению политик и быстро реагировать на потенциальные угрозы безопасности.

paloalto NETWORKS
the network security company™



Application Command Center предоставляет возможность глобального и локального просмотра трафика приложений с подробным анализом текущих сессий.

Глобальное управление политиками: обеспечение безопасной работы приложений

Обеспечение безопасной работы приложений заключается в применении специальных политик предотвращения угроз, а также политик фильтрации файлов, данных и URL-адресов. Panorama обеспечивает безопасную работу приложений во всей сети межсетевых экранов, позволяя администраторам централизованно настраивать правила безопасности.

Применение общих политик безопасности с помощью Panorama позволяют гарантировать выполнение внутренних или законодательных требований, а локальные политики безопасности для МЭ обеспечивают гибкость в управлении. Сочетание централизованного и локального административного контроля над политиками и объектами помогает найти баланс между надежным обеспечением безопасности на глобальном уровне и гибкостью на локальном уровне.

МЭ Palo Alto Networks позволяют администраторам создавать политики безопасности для конкретных пользователей или групп пользователей, интегрируясь при этом со службами каталогов. Возможность установить единую политику безопасного доступа приложениям на основе пользователей, а не IP-адресов, позволяет значительно сократить количество время конфигурации и администрирования. Дополнительным преимуществом интеграции со службами каталогов является резкое сокращение административных расходов, связанных с добавлением, перемещением и изменением информации о сотрудниках – действий, которые могут выполняться ежедневно, – благодаря тому, что при перемещении сотрудников между группами политики безопасности остаются неизменными.

Мониторинг трафика: анализ, формирование отчетов и расследование инцидентов в сфере информационной безопасности

Panorama использует тот же набор мощных инструментов мониторинга и формирования отчетов, как и на локальном уровне управления отдельным межсетевым экраном PaloAlto Networks, при этом есть возможность визуализации, которая обеспечивает общее представление по всем операциям. Когда администраторы создают отчеты на основе журналов событий информационной безопасности, Panorama динамически извлекает самые актуальные данные из межсетевых экранов, находящихся под непосредственным управлением. Доступ к самой актуальной информации для всех устройств позволяет администратору реагировать на события информационной безопасности, а также применять профилактические меры по защите корпоративных ресурсов.

- **Средство просмотра журналов:** С помощью Panorama администраторы могут быстро просматривать события в журнале событий, как для отдельного устройства, так и для всех устройств, с использованием функций динамической фильтрации журнала, нажав на значение в ячейке и/или определив критерии сортировки с помощью функции построения выражений. Результаты можно сохранять или экспортировать для дальнейшего анализа
- **Настройка отчетов:** Преднастроенные отчеты можно использовать без изменений, либо отредактировать, а также сгруппировать в один отчет интересующие отчеты в соответствии с определенными требованиями.
- **Отчеты о действиях пользователей:** При помощи Panorama можно создавать отчеты о действиях пользователей, в которых будет содержаться информация об используемых приложениях, категориях посещенных URL-адресов, список посещенных веб-сайтов за определенный период времени для отдельных пользователей. Panorama формирует отчеты на основе сводного представления действий пользователей, независимо от межсетевого экрана, которым они защищены, а также типа устройств или IP-адреса.

Архитектура управления Panorama

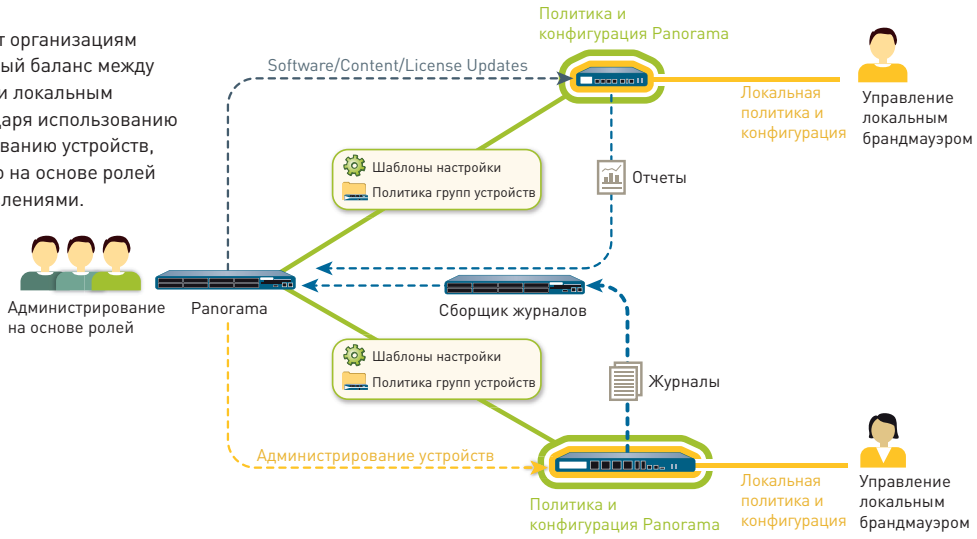
Panorama позволяет управлять межсетевыми экранами Palo Alto Networks на основе модели, обеспечивающей как централизованный контроль, так и локальное управление. Panorama предлагает ряд инструментов для централизованного администрирования:

- **Шаблоны:** Panorama управляет общей конфигурацией устройств с помощью шаблонов. Шаблоны могут использоваться для централизованного управления конфигурацией и последующего применения изменений на всех находящихся под управлением межсетевых экранах. Такой подход избавляет от необходимости многократно изменять одни и те же настройки межсетевых экранов на большом количестве устройств. Одним из примеров такого использования является применение общих настроек DNS и NTP серверов для сотен межсетевых экранов без необходимости выполнять одни и те же изменения для каждого отдельного устройства.
- **Группы устройств:** Panorama осуществляет управление общими правилами и объектами на основе групп устройств. Группы устройств используются для централизованного управления базами правил для большого количества устройств с общими требованиями. Устройства могут объединяться в группы, например по географическим (например, Европа и Северная Америка) или функциональным (например, периметр или центр обработки данных). В группах устройств виртуальные системы рассматриваются как отдельные физические межсетевые экраны. Это позволяет использовать общие базы правил для различных виртуальных систем на одном устройстве.

  При помощи Panorama можно использовать общие политики для централизованного управления, при этом обеспечивая возможность внесения специфических корректив с учетом локальных требований. На уровне групп устройств администраторы могут создавать общие политики, которые определяются как первый набор правил (предварительные правила) и последний набор правил (пост-правила), для которых производится оценка по критериям соответствия. Предварительные и пост-правила можно просматривать на находящемся под управлением межсетевом экране, но редактировать их можно только в Panorama в рамках предварительно определенных административных ролей. Локальные правила для устройств (занимающие место между предварительными и пост-правилами) могут редактироваться либо локальным администратором, либо администратором Panorama, переключившимся на локальный контекст межсетевого экрана. Кроме того, есть возможность использовать общие объекты, заданные администратором Panorama, на которые могут ссылаться правила для устройств, управляемых локально.
- **Администрирование на основе ролей:** администрирование межсетевых экранов Palo Alto Networks может осуществляться на основе ролей для делегирования различным сотрудникам административного доступа на уровне функций (включен, только просмотр или отключен и скрыт от просмотра). Администраторам может быть предоставлен соответствующий уровень доступа к определенным функциям, при этомостальные функции будут недоступны. В качестве примера можно привести определение различных ролей для персонала, отвечающего за выполнение разных задач, например «администраторов систем безопасности» и «сетевых администраторов». Все изменения, сделанные администратором, фиксируются в журнале с указанием времени изменений, имени администратора, использованного интерфейса управления (веб-интерфейс, интерфейс командной строки, Panorama), команды или действия.
- **Управление обновлением программного обеспечения, контента и лицензий:** По мере увеличения масштабов многие организации хотят организовать и унифицировать процесс обновлений на всех уровнях. Например, специалисты по безопасности могут предпочесть централизованно подготовить обновление программного обеспечения, а затем отправить его через систему управления сразу на все межсетевые экраны. Благодаря Panorama можно централизованно управлять процессом обновления программного обеспечения, контента (обновления приложений, сигнатур антивирусов, сигнатур угроз, баз данных фильтрации URL-адресов и т.д.) и лицензий.

С помощью шаблонов, групп устройств, администрирования на основе ролей и управления обновлениями администраторы могут предоставлять надлежащий доступ ко всем управленческим функциям: инструментам визуализации, созданию политик, формированию отчетов и ведению журналов, как на глобальном, так и на локальном уровнях.

Panorama позволяет организациям находить оптимальный баланс между централизованным и локальным управлением благодаря использованию шаблонов, группированию устройств, администрированию на основе ролей и управлению обновлениями.



Гибкость при развертывании

Организации могут развертывать Panorama в виде аппаратного или виртуального устройства.

Аппаратное устройство

Для организаций, которые предпочитают развертывать системы управления на высокопроизводительных специализированных платформах или хотят разделить в Panorama функции управления и отчетности для журналов с большими объемами данных, есть возможность использовать специализированное аппаратное устройство M-100. Существуют следующие варианты внедрения Panorama на M-100:

- **Централизованный:** В этом случае все функции Panorama, связанные с управлением и ведением журналов, объединены в одном устройстве (с дополнительной возможностью обеспечения высокой доступности).
- **Распределенный:** При такой конфигурации функции распределены между устройствами, занимающимися управлением и ведением журналов отчетности. В этой конфигурации функции распределены между устройствами, занимающимися управлением и ведением журналов.
  - **Средство управления Panorama:** Отвечает за задачи, связанные с настройкой политик и конфигурацией для всех управляемых устройств. Средство управления не хранит данные журналов на локальном диске, а использует для этого отдельные средства ведения журналов. Средство управления осуществляет централизованное формирование отчетности на основе анализа данных, хранящихся в средствах ведения журналов.
  - **Средство ведения журналов Panorama:** Организации с большими объемами данных, фиксируемых в журналах, и повышенными требованиями к длительности их хранения могут внедрить отдельное средство ведения журналов Panorama, которое будет объединять информацию, получаемую от нескольких управляемых межсетевых экранов.

Разделение функций управления и ведения журналов позволяет организациям оптимизировать процессы внедрения, а также соблюсти требования к масштабируемости.

Виртуальное устройство

Panorama имеет возможность внедрения в виде виртуальной машины на VMware ESX(i). Существует два варианта внедрения:

- **Централизованный:** Все функции Panorama, связанные с управлением и ведением журналов, объединены в одном виртуальном устройстве (с дополнительной возможностью обеспечения высокой доступности).
- **Распределенный:** При распределенном ведении журналов можно использовать сочетание аппаратных и виртуальных устройств.
  - **Средство управления Panorama:** При этом виртуальное устройство используется как средство управления и отвечает за задачи, связанные с настройкой политик и конфигурации для всех управляемых устройств.
  - **Средство ведения журналов Panorama:** Средства ведения журналов Panorama используются для выполнения задач, связанных со сбором и обработкой больших объемов данных имеет возможность реализации с использованием аппаратной M-100. Виртуальное устройство не может использоваться в качестве средства ведения журналов Panorama.

Возможность выбрать аппаратную или виртуализированную платформу, а также группировать или разделять функции Panorama обеспечивает максимальную гибкость при управлении межсетевыми экранами Palo Alto Networks в распределенных сетях.

СПЕЦИФИКАЦИЯ PANORAMA

Количество поддерживаемых устройств	До 1 000
Отказоустойчивость	Active/Stanby
Аутентификация администратора	Локальная БД RADIUS

СПЕЦИФИКАЦИИ УСТРОЙСТВА УПРАВЛЕНИЯ M-100

ИНТЕРФЕЙСЫ

- (1) 10/100/1000, (3) 10/100/1000 (для будущего использования), (1) последовательный порт консоли DB9

НАКОПИТЕЛИ (2 ВАРИАНТА)

- M-100 1TB RAID: 2 x 1TB RAID Certified HDD for 1TB of RAID Storage
- M-100 4TB RAID: 8 x 1TB RAID Certified HDD for 4TB of RAID Storage

ПИТАНИЕ/МАКСИМАЛЬНАЯ ПОТРЕБЛЯЕМАЯ МОЩНОСТЬ

- 500 Вт/500 Вт

МАКС. ТЕПЛОВЫДЕЛЕНИЕ (БТЕ/Ч)

- 1705 БТЕ/ч

ВХОДНОЕ НАПРЯЖЕНИЕ (ЧАСТОТА ВХОДНОГО СИГНАЛА)

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

МАКСИМАЛЬНЫЙ ПОТРЕБЛЯЕМЫЙ ТОК

- 10 А при 100 В переменного тока

СРЕДНЕЕ ВРЕМЯ НАРАБОТКИ НА ОТКАЗ)

- 14,5 лет

ВОЗМОЖНОСТЬ УСТАНОВКИ В СТОЙКУ (ГАБАРИТЫ)

- 1U, стандартная 19-дюймовая стойка (1,75 (В) x 23 (Г) x 17,2 (Ш) дюйма)

ВЕС (РАСПАКОВАННОЕ/УПАКОВАННОЕ)

- 53,4 кг/70 кг

СЕРТИФИКАТЫ БЕЗОПАСНОСТИ

- UL, CUL, CB

EMI

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

ВОЗМОЖНАЯ ТЕМПЕРАТУРА ОКРУЖАЮЩЕЙ СРЕДЫ

- Возможная температура окружающей среды при эксплуатации: от 5 до 40 °C
- Температура хранения: от -40 до 65 °C

СПЕЦИФИКАЦИИ ВИРТУАЛЬНОГО УСТРОЙСТВА

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ К СЕРВЕРУ

- Жесткий диск 80 Гбайт
- Процессор с частотой 2 ГГц
- Оперативная память 2 Гбайт

ПОДДЕРЖКА VMWARE

- VMware ESX 3.5, 4.0, 4.1, 5.0

ПОДДЕРЖКА БРАУЗЕРОВ

- IE версии 7 или новее
- Firefox версии 3.6 или новее
- Safari версии 5.0 или новее
- Chrome версии 11.0 или новее

ХРАНЕНИЕ ЖУРНАЛОВ

- Виртуальный диск VMware: макс. 2 Тбайт
- NFS

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