Обзор межсетевых экранов Palo Alto Networks нового поколения

В результате фундаментальных изменений используемых приложений и существующих угроз, поведения пользователей и инфраструктуры сетей традиционные межсетевые экраны, основанные на работе с портами, уже не обеспечивают достаточную безопасность. Очень часто для решения поставленных задач пользователи осуществляют доступ к приложениям различных типов с использованием устройств различных типов. В то же время расширение центров обработки данных, виртуализация, мобильные решения и использование облачных технологий заставляют задуматься над тем, как обеспечить доступ приложениям и при этом сохранить защиту сети.

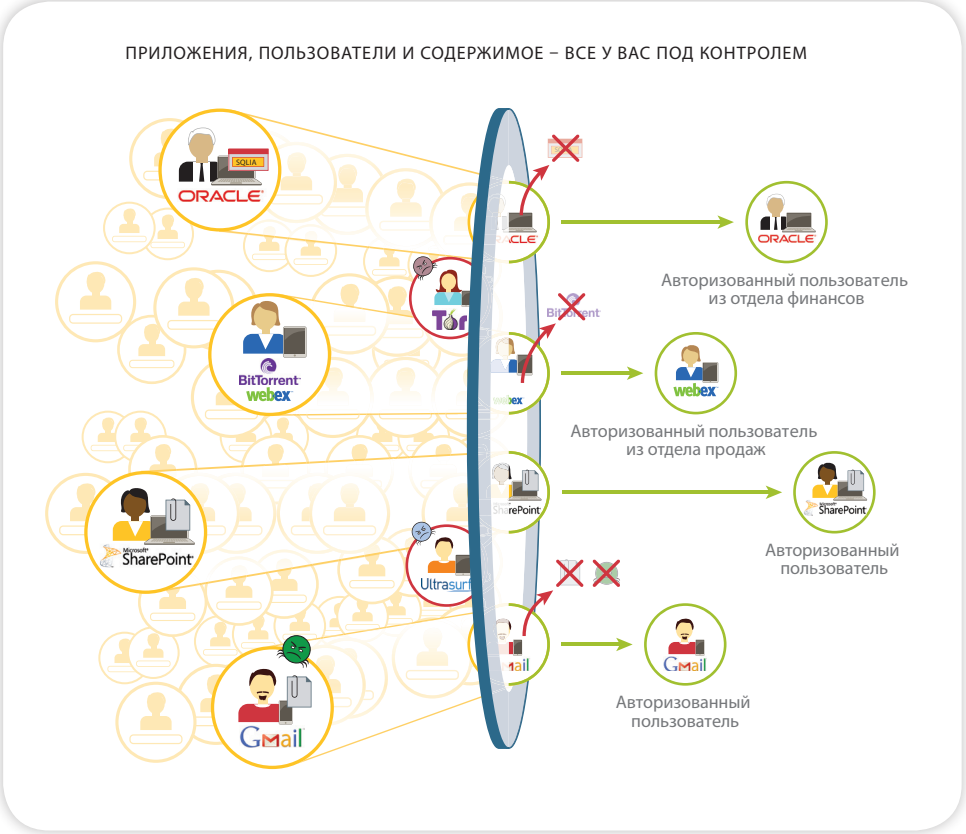
Традиционные способы решения этой задачи предполагают блокировку всего трафика приложений с помощью постоянно растущего списка точечных технологий, используемых в дополнение к межсетевым экранам, что может усложнить работу предприятия, или же разрешение доступа всем приложениям, что в равной степени неприемлемо в свете роста угроз для бизнеса и безопасности. Проблема состоит в том, что традиционный межсетевой экран, работающий на основе портов, даже с дополнительной функцией блокировки приложений не может использоваться в качестве альтернативы ни для одного из отмеченных подходов. Чтобы найти баланс между «разрешением всего» и «запрещением всего», необходимо обеспечить безопасное разрешение доступа приложениям, используя в качестве основных критериев политики безопасности межсетевого экрана такие элементы, как удостоверение приложений, пользователь приложения и тип контента, в зависимости от потребностей предприятия.

Основные требования по обеспечению безопасного доступа:

- **Идентификация приложений, а не портов.** Классификация трафика в момент прохождения через межсетевой экран позволяет идентифицировать приложение независимо от используемых протоколов, средств шифрования и тактики обхода средств анализа трафика. Результаты идентификации затем становятся основой для всех политик безопасности.
- **Привязка использования приложений не к IP-адресу, а к конкретным пользователям, независимо от их местоположения или используемого устройства.** Применение информации о пользователях и группах из служб каталогов предприятия и других хранилищ данных о пользователях для внедрения согласованной политики разрешения доступа для всех пользователей, независимо от их местоположения или используемого устройства.
- **Защита от всех угроз – как известных, так и неизвестных.** Блокирование известных угроз, включая вторжения, вредоносное и шпионское ПО, опасные URL-адреса, а также анализ трафика и обеспечения автоматической защиты от целенаправленного и ранее неизвестного вредоносного ПО.
- **Упрощение управления политиками.** Обеспечение безопасной работы приложений и сокращение времени на администрирование с помощью удобных графических интерфейсов, редактора унифицированной политики безопасности, шаблонов и групп устройств.

Политики безопасного доступа к приложениям помогут усовершенствовать систему безопасности, независимо от места внедрения. Вы можете защититься от внешних угроз путем блокирования на границе сети широкого спектра нежелательных приложений с последующей проверкой разрешенных приложений на наличие угроз – как известных, так и неизвестных. В центре обработки данных, традиционном или виртуализированном, для безопасной работы приложений необходимо обеспечить: использование приложений центра обработки данных только уполномоченными пользователями, защиту контента от угроз и решение проблем в сфере безопасности, связанных с динамичным изменением виртуальной инфраструктуры. Для защиты филиалов и удаленных пользователей можно использовать тот же набор политик безопасного доступа, который применяется в штаб-квартире, что обеспечивает согласованность применяемых политик.

paloalto NETWORKS
the network security company™



Безопасная работа приложений как необходимое условие успешного развития бизнеса

Безопасная работа приложений, обеспечиваемая с помощью сетевых экранов Palo Alto Networks нового поколения, помогает решить проблемы безопасности бизнеса, связанные с растущим числом используемых в сети приложений. Обеспечение безопасного доступа к приложениям для отдельных пользователей или групп пользователей – локальных, мобильных и удаленных – и защита трафика от известных и неизвестных угроз позволяет усилить безопасность и одновременно поддержать рост бизнеса.

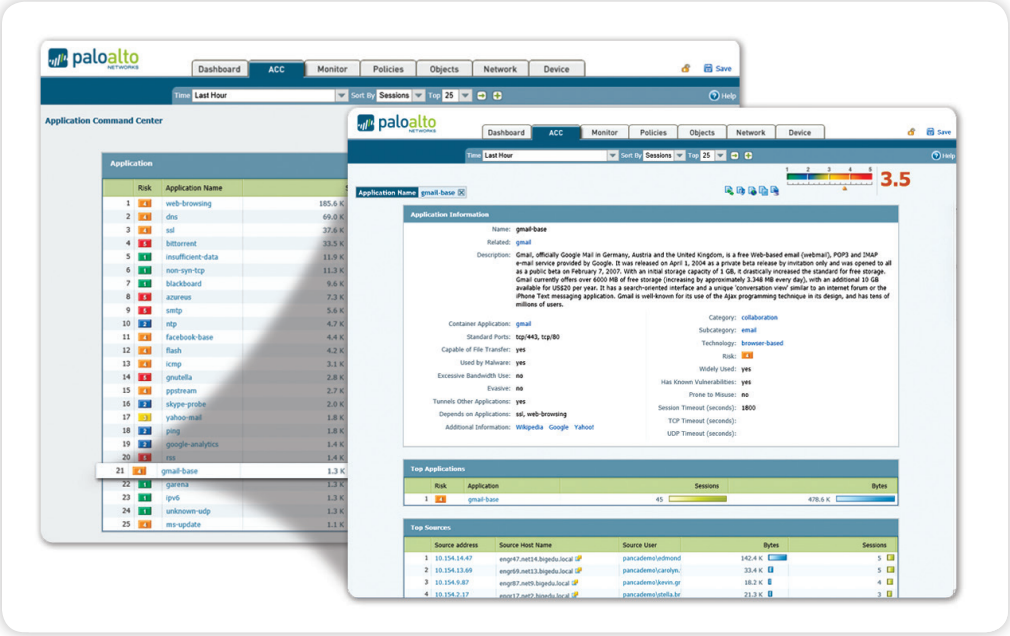
- **Классификация всех приложений, на всех портах, в любое время.** Средства точной классификации трафика – основной компонент любого межсетевого экрана, а результаты их работы становятся основой политики безопасности. Современные приложения легко обходят межсетевые экраны, выполняющие фильтрацию трафика на основе портов, путем динамической смены портов, использования протоколов SSL и SSH, туннелирования своего трафика через порт 80 или использования нестандартных портов. Технология App-ID снимает ограничения традиционных межсетевых экранов, связанных с видимостью классификации трафика, за счет использования нескольких механизмов классификации трафика, проходящего через межсетевой экран, и делает возможной точную идентификацию приложений в сети, независимо от порта, шифрования (SSL или SSH) и используемой техники маскировки. Информация о том, какое именно приложение получает доступ к сети, а не только порта и протокола, становится основой для всех решений в сфере безопасности. Неидентифицированные приложения, которые, как правило, генерируют небольшой процент трафика, но создают высокий потенциальный риск, автоматически классифицируются для систематического управления, которое может включать контроль соблюдения политик, исследование угроз, создание пользовательских сигнатур или захват пакетов для разработки сигнатур приложений Palo Alto Networks.

- **Включение в политику безопасности не только IP-адресов, но также пользователей и устройств**. Создание и управление политиками безопасности на основе приложений и идентификации пользователей, независимо от устройства или местоположения, является более эффективным средством защиты вашей сети, чем решение, основанное исключительно на портах и IP-адресах. Интеграция с различными корпоративными каталогов пользователей позволяет идентифицировать пользователей Microsoft Windows, Mac OS X, Linux, Android или iOS, которые осуществляют доступ к приложениям. Пользователи, которые находятся в командировке или работают удаленно, защищены с помощью тех же согласованных политик безопасности, которые действуют в локальной или корпоративной сети. Сочетание возможностей мониторинга и контроля использования приложений пользователями означает, что можно обеспечить безопасное использование Oracle, BitTorrent, Gmail или любого используемого в сети приложения, независимо от того, где и какой пользователь осуществляет доступ к нему.

- **Предотвращение всех угроз – как известных, так и неизвестных.** Чтобы обеспечить безопасность современной сети, необходимо найти устранить известные уязвимые места, обеспечить защиту от вредоносного и шпионского ПО, а также совершенно неизвестных и целенаправленных угроз. Этот процесс начинается с сокращения возможностей для сетевых атак путем разрешения доступа конкретным приложениям и запрета доступа всем остальным приложениям: либо с помощью неявной стратегии «запрещать все остальные», либо с помощью задаваемых в явном виде политик. Координированные меры по предотвращению угроз могут примяться ко всему разрешенному трафику, за один проход блокируя известные опасные сайты, уязвимости, вирусы, программы-шпионы и запросы злоумышленников к DNS-серверам. Активный анализ и идентификация неизвестных вредоносных программ осуществляется путем прямого запуска неопознанных файлов в виртуальной среде «песочница» и проверки на предмет более 100 видов вредоносного поведения. При обнаружении новых вредоносных программ автоматически генерируются и предоставляются сигнатуры зараженных файлов и связанного с ними вредоносного трафика. Анализ, связанный с предотвращением угроз, осуществляется с учетом контекста приложений и протоколов связи, гарантируя неизбежное выявление даже тех угроз, которые пытаются скрыться от систем безопасности в туннелях, сжатой информации или нестандартных портах.

Гибкость внедрения и управления

Функции обеспечения безопасной работы приложений могут быть внедрены либо на основе специально созданной аппаратной платформы, либо на виртуализированном решении. При развертывании нескольких межсетевых экранов Palo Alto Networks в виде аппаратной или виртуализированной платформы можно использовать дополнительное средство централизованного управления Panorama, позволяющее централизованно осуществлять мониторинг шаблонов трафика, внедрять политики безопасности, формировать отчеты и выполнять обновления.



Мониторинг приложений: Отображение действий приложений в простом и понятном виде. Возможность добавления и удаления фильтров, позволяющих узнать подробности о приложении, его функциях и пользователях.

Обеспечение безопасной работы приложений: комплексный подход

Обеспечение безопасной работы приложений требует комплексного подхода к защите сети и росту вашего бизнеса. Этот подход начинается с подробного изучения приложений, работающих в сети, и пользователях, независимо от используемой ими платформы или их расположения, а также информации, которую может пересылать приложение. Чем больше вы обладаете знаниями о сетевой активности, тем более эффективные вы сможете создавать политики безопасности с учетом особенностей приложений, пользователей и информации и в контексте специфики деятельности вашего предприятия. Местонахождение пользователей, используемая ими платформа и место внедрения политики (периметр, традиционные или виртуализированные центры обработки данных, филиалы или удаленные пользователи) практически не влияют на принцип создания политики. Теперь вы можете обеспечить безопасную работу любого приложения и любого пользователя с любой информацией.

Чем полнее знания, тем более надежная политика безопасности

Как показывает успешный опыт в области безопасности, чем больше вы обладаете знанием того, что происходит в вашей сети, тем более надежные удастся создать политики безопасности. Например, обладая точными знаниями о приложениях, осуществляющих доступ к сети, администраторы могут специально разрешать доступ приложениям, которые используются на вашем предприятии, и заблокировать нежелательные приложения, вместо того чтобы фильтровать трафик по отдельным портам. Знание того, кем является пользователь, а не только его IP-адреса, является еще одним критерием политики безопасности, позволяющим более точно формулировать правила политик.

- Благодаря мощному набору графических инструментов визуализации ваши администраторы могут получать более полное представление о работе приложениях и их потенциальном влиянии на безопасность, что позволяет принимать более обоснованные решение в сфере политики безопасности. По мере изменения состояния приложений происходит их непрерывная классификация и динамическое обновление их краткого графического представления в простои и удобном веб-интерфейсе.
- Новые или незнакомые приложения можно быстро анализировать, отобразив описание, ключевые особенности, поведенческие характеристики и пользователей приложения одним щелчком мыши.
- Дополнительный мониторинг категорий URL-адресов, угроз и шаблонов данных позволяет сформировать полное и четкое представление о ситуации в сети.
- Неизвестные приложения, которые, как правило, генерируют небольшой процент трафика, но представляют высокий потенциальный риск, автоматически классифицируются для анализа с целью определения того, являются ли они внутренними приложениями (например, коммерческими приложениями, которые еще не были идентифицированы) или представляют угрозу.

Обеспечение работы приложений и снижение риска

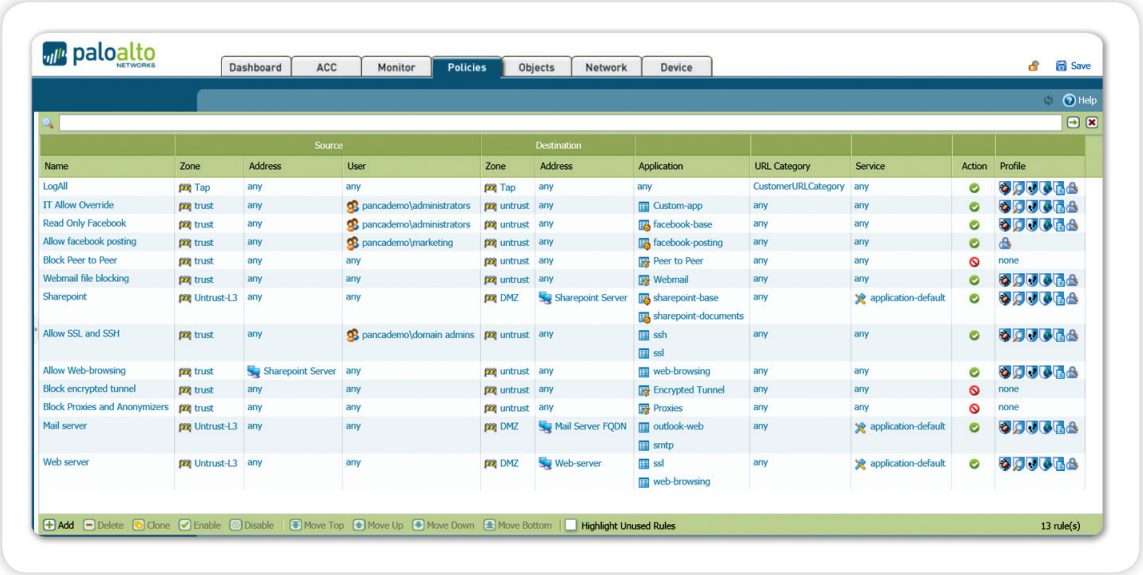
Критерии правил безопасного разрешения доступа приложениям включают приложения или функции приложений, пользователей и группы, а также контент и позволяют найти баланс между «запрещением всех приложений» и рискованной альтернативой в виде «разрешения всех приложений».

Политики обеспечения доступа, применяемые по периметру сети, включая филиалы, мобильных и удаленных пользователей, нацелены на идентификацию всего трафика и выборочное разрешение прохождения трафика на основе идентификации пользователей с последующим сканированием трафика на наличие угроз. Примеры политик включают:

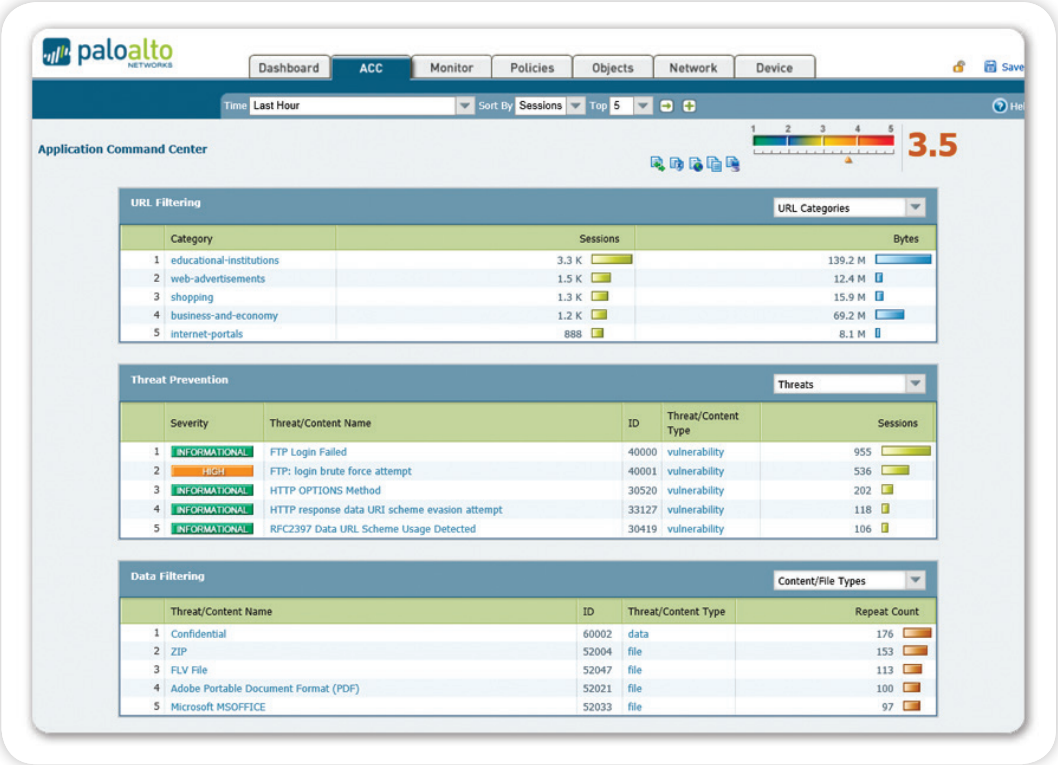
- Ограничение числа используемых почтовых веб-служб и служб обмена мгновенными сообщениями всего до нескольких возможных вариантов: расшифровка тех из них, которые используют SSL, проверка трафика на предмет вторжений и загрузка неизвестных файлов на WildFire для анализа и разработки сигнатур.
- Разрешение приложений и веб-сайтов, использующих потоковые мультимедиа, но с применением системы обеспечения качества обслуживания и защиты от вредоносных программ, чтобы минимизировать влияние на VoIP-приложения и защитить сеть.
- Контроль использования Facebook: пользователям разрешается просматривать страницы, но все игры и подключаемые модули социальной сети становятся заблокированными, а публикации в сети Facebook разрешены только для отдела маркетинга. Сканирование всего трафика Facebook на предмет вредоносных программ и вторжений.
- Контроль пользования Интернетом путем сканирования трафика и разрешения доступа к веб-сайтам, связанным с выполнением служебных обязанностей, и блокирования доступа к веб-сайтам, очевидно не связанным с работой. «обучение» доступу к сомнительным сайтам через настраиваемые страницы блокировки.
- Применение согласованных правил безопасности путем использования одинаковых политик для всех пользователей (локальных, мобильных или удаленных) с помощью GlobalProtect.
- Использование неявной стратегии «запрещать все остальные» или целенаправленное блокирование нежелательных приложений, например использующих прямое соединение «точка-точка» или пытающихся обойти средства защиты, а также трафика из определенных стран для сокращения потенциально опасного для бизнеса и безопасности трафика приложений.

Примеры использования правил разрешения доступа в центрах обработки данных (традиционных, виртуализированных или их комбинации) включают подтверждение приложений, поиск вредоносных приложений и защиту данных.

- Изоляция хранилища номеров кредитных карт Oracle в отдельной зоне безопасности, контроль доступа групп финансового подразделения путем направления трафика через стандартные порты и его проверки на предмет уязвимостей приложений.
- Разрешение доступа к центру обработки данных с использованием фиксированного набора удаленных приложений управления, например SSH, RDP, Telnet, через их стандартные порты только для группы ИТ-подразделения.
- Разрешение администрирования Microsoft SharePoint только группе администраторов и разрешение доступа к документам Microsoft SharePoint всем остальным пользователям.



Универсальный редактор политик: Привычный интерфейс и набора функций позволяет быстро создавать и внедрять политики контроля приложений, пользователей и информации.



Мониторинг информации и угроз: Просмотр URL-адресов, угроз и перемещения файлов/данных в простом и понятном формате. Добавление и удаление фильтров для получения дополнительной информации об отдельных элементах.

Защита разрешенных приложений

Безопасная работа приложений означает разрешение доступа к определенным приложениям и применение определенных политик в целях блокировки известных уязвимостей, известного или неизвестного вредоносного и шпионского ПО, контроль передачи файлов и данных, а также пользования Интернетом. Наиболее распространенные тактики маскировки угроз, включая переключение между портами и туннелирование, нейтрализуются путем реализации политики предупреждения угроз с использованием контекста приложений и протоколов, который генерируется декодерами в App-ID. Решения, основанные на концепции унифицированного управления защитой от угроз (UTM), напротив, используют разрозненный подход к предотвращению угроз, в рамках которого отдельные функции, межсетевые экраны, системы предотвращения вторжений, антивирусы, фильтры URL-адресов и сканеры трафика работают без обмена контекстом, что делает их более уязвимыми перед попытками обхода защиты.

- **Блокирование известных угроз: Системы предотвращения вторжений и сетевые антивирусы/средства защиты от шпионского ПО.** Единый формат сигнатур и система потокового сканирования позволяют защитить вашу сеть от широкого спектра угроз. Система предотвращения вторжений (IPS) нейтрализует угрозы, связанные с блокированием сети и использованием уязвимостей на уровне приложений, переполнением буфера, DoS-атаками и сканированием портов. Антивирус / средство защиты от шпионского ПО блокирует миллионы вариантов вредоносных программ, а также генерируемый вредоносными программами трафик команд и контроля, вирусы в PDF-файлах и вредоносные программы, скрытые в сжатых файлах или веб-трафике (сжатый HTTP/HTTPS). Реализуемая на основе политик безопасности расшифровка SSL для всех приложений и портов обеспечивает защиту от вредоносных программ, осуществляющих доступ через приложения, использующие защищенный протокол SSL.
- **Блокирование неизвестного и целенаправленного вредоносного ПО: Wildfire™.** WildFire выявляет и анализирует неизвестное или целенаправленное вредоносное ПО путем прямого запуска неопознанных файлов в виртуальной облачной среде «песочница». WildFire осуществляет мониторинг на предмет более 100 видов вредоносного поведения, а результаты немедленно доводятся до сведения администратора в форме экстренных уведомлений. Предлагающаяся отдельно подписка на WildFire обеспечивает усиленную защиту, ведение журналов и формирование отчетов. Как подписчик, вы получаете защиту в течение часа после обнаружения новой вредоносной программы в любой точке мира, что позволяет эффективно блокировать распространение новых вредоносных программ, прежде чем они нанесут вам вред. Как подписчик, вы также получаете доступ к интегрированным в WildFire инструментам ведения журналов и формирования отчетности, а также программному интерфейсу для отправки образцов в облако WildFire для анализа.

- **Идентификация хостов, зараженных ботами.** App-ID классифицирует все приложения на всех портах, включая весь неизвестный трафик, который зачастую может представлять собой опасность сбоев или угроз для вашей сети. Отчет о признаках ботнет-поведения анализирует неизвестный трафик, подозрительные запросы к DNS и URL-адресов, а также различное необычное поведение в сети в целях выявления устройств, которые могут быть заражены вредоносными программами. Результаты анализа отображаются в виде списка потенциально зараженных хостов, которые могут являться участниками ботнета.
- **Ограничение несанкционированной передачи файлов и данных.** Функции фильтрации данных позволяют администраторам реализовывать политики, которые снизят риски, связанные с несанкционированной передачей файлов и данных. Операции передачи файлов контролируются путем анализа содержимого файла (в отличие от анализа только расширения файла). По результатам анализа принимается решение, следует ли разрешать передачу файла. При этом может блокироваться загрузка исполняемых файлов (которые обычно загружаются с использованием различных средств маскировки), что позволяет защитить сеть от скрытого распространения вредоносных программ. Функции фильтрации данных позволяют обнаруживать содержимое, соответствующее шаблонам конфиденциальных данных (номеров кредитных карт и социального страхования), и управлять его передачей.
- **Контроль пользования интернетом.** Полностью интегрированная настраиваемая система фильтрации по URL-адресам позволяет администраторам применять точечные политики в отношении использования веб-ресурсов, дополняющие политики мониторинга трафика приложений и управления им, а также защищающие организацию от всех возможных рисков нарушения требований законодательства, несоблюдения нормативных требований и снижения производительности. Кроме того, в политику безопасности могут быть интегрированы категории URL-адресов, что позволяет точнее управлять расшифровкой SSL, качеством обслуживания или другими правилами.

Непрерывное управление и анализ

Оптимальные методики обеспечения безопасности требуют от администраторов нахождения компромисса между упреждающим управлением межсетевым экраном, защищающим одно устройство или несколько сот устройств, и реагированием на возникающие угрозы, проведением расследований, анализом и формированием отчетов об инцидентах в сфере информационной безопасности.

- **Управление:** Каждой платформой Palo Alto Networks можно управлять индивидуально через интерфейс командной строки (CLI) и полнофункциональный веб-интерфейс. При широкомасштабном развертывании систем безопасности можно приобрести лицензию и внедрить Panorama как централизованное решение для управления, позволяющее найти баланс между глобальным централизованным управлением и необходимостью обеспечения гибкости политики на локальном уровне с помощью таких функций, как шаблоны и общая политика. Дополнительная поддержка для инструментов, основанных на стандартах, например SNMP и API-интерфейсов на базе REST, позволяет, осуществлять интеграцию с инструментами управления от сторонних поставщиков. Независимо от того, какой интерфейс вы используете, веб-интерфейс устройства или интерфейс Panorama, он выглядит и работает одинаково, что избавляет от необходимости обучения при переключении между интерфейсами. Ваши администраторы могут в любое время использовать любой из доступных интерфейсов для внесения изменений, не беспокоясь о проблемах синхронизации. Для всех сред управления поддерживается администрирование на основе ролей, что позволяет назначать полномочия и функции конкретным лицам.
- **Формирование отчетов:** Предопределенные отчеты можно использовать без изменений, их можно доработать, а также сгруппировать в один отчет в соответствии с определенными требованиями. Для всех отчетов поддерживается экспорт в формат CSV или PDF, а также создание отчетов и их отправка по электронной почте по расписанию.
- **Ведение журналов:** Средства фильтрации журналов в режиме реального времени ускоряют анализ сеансов сетевого взаимодействия при проведении расследования инцидентов в сфере информационной безопасности. Результаты фильтрации журналов можно экспортировать в CSV-файл или отправить на сервер syslog для архивирования на внешнем носителе или проведения дополнительного анализа.

Специально спроектированные аппаратные средства или виртуализированные платформы

Palo Alto Networks предлагает полный спектр специально спроектированных аппаратных платформ: от PA-200 для удаленных офисов до PA-5060 для высокоскоростных центров обработки данных. В платформах используется однопроходная архитектура программного обеспечения и специфические методы обработки для каждой функции: организации работы сети, обеспечения безопасности, предотвращения угроз и осуществления управления, что позволяет получить предсказуемый уровень производительности. Все функции межсетевого экрана, реализованные в аппаратных платформах, также доступны в виртуальных межсетевых экранах серии VM, что позволяет вам обеспечить безопасность виртуальных и облачных вычислительных сред, используя те же самые политики для межсетевых экранов как для периметра, так и для удаленного офиса.

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