paloalto NETWORKS

the network security company™

Решения Palo Alto Networks для центров обработки данных: исключая компромиссы

Май 2011 г.

Краткий обзор

В принципе, гарантировать безопасность сетей в центрах обработки данных несложно — необходимо обеспечить предотвращение угроз, соответствие требованиям нормативных документов и корпоративным политикам и при этом не препятствовать осуществлению коммерческой деятельности. Но на практике вследствие постоянного роста требований к обеспечению доступности приложений и повышению их производительности, возникновения новых видов угроз и необходимости в полном представлении о работе приложений с точки зрения безопасности реализовать вроде бы простые требования к безопасности сетей в центрах обработки данных довольно сложно. Более того, большинство организаций вынуждены идти на значительные компромиссы, обеспечивая баланс между безопасностью, выполнением рабочих функций и видением производительности, простотой и эффективностью. Задача усложняется еще и тем, что не все центры обработки данных одинаковы. Задачи и требования к безопасности для внутренних корпоративных центров обработки данных значительно отличаются от требований к безопасности, предъявляемых центрам обработки данных с выходом в Интернет. Эти два типа центров обработки данных различаются характеристиками приложений и пользователей, нормативными требованиями и дополнительными уникальными аспектами обеспечения безопасности. Для корпоративных центров обработки данных критически важными, специфическими требованиями к инфраструктурам сетевой безопасности являются возможность интеграции средств безопасности сетей в разнообразные сетевые архитектуры, возможность сегментации сетей на основе обусловленных бизнесом условий (например, приложений и пользователей) и возможность поддержания контакта с разработчиками приложений. В отличие от этого перед руководителями центров обработки данных с выходом в Интернет стоят задачи повышения гибкости и возможности мониторинга, улучшения и упрощения интегрированных средств предотвращения угроз и при этом повышения надежности операций.

Решения компании Palo Alto Networks уникально обеспечивают соответствие требованиям к безопасности сетей для сред в обоих типах центров обработки данных. Основанные на инновационных технологиях (App-ID™, User-ID и Content-ID), встроенных в архитектуру, предназначенную для высокопроизводительных и надежных центров обработки данных, межсетевые экраны следующего поколения компании Palo Alto Networks предоставляют организациям решение по обеспечению безопасности сетей в центрах обработки данных. Это решение устраняет множество неприемлемых компромиссов, ранее присущих системам безопасности сетей в центрах обработки данных.

Сетевая безопасность в центрах обработки данных = предотвращение угроз, соответствие нормативам, высокая производительность

Как известно, на вопрос «Почему вы грабили банки?» известный американский грабитель банков Вилли Саттон ответил: «Потому что деньги именно там». Хотя, по словам Саттона, эта история выдумана, центры обработки данных привлекают злоумышленников по тем же причинам — там хранятся данные (а данные — это либо деньги, либо что-то равноценное). Теоретически, обеспечить сетевую безопасность в центрах обработки данных довольно просто. В ходе обсуждений с корпоративными клиентами выяснилось, что для обеспечения сетевой безопасности в современных центрах обработки данных необходимо решить три задачи:

- Предотвращение угроз.
- Соответствие нормативным документам и сегментация.
- Обеспечение производительности и доступности приложений.

Следует признать, что решать первую задачу, предотвращение угроз, за последние несколько лет стало значительно сложнее. Базовые атаки на инфраструктуру открыли путь для мультивекторных, порожденных приложениями изощренных атак, которые незаметны для пользователей, направлены на получение прибыли, непреднамеренно поддерживаются пользователями и во многих случаях являются полиморфными. Уровень организации, связанной с разработкой таких угроз, также является беспрецедентным. Решение второй задачи, обеспечение соответствия нормативным документам, по-прежнему оказывает большое влияние на архитектуры и сетевую безопасность центров обработки данных. Нормативные документы PCI, департамента здравоохранения США или европейское законодательство по обеспечению конфиденциальности предъявляют высокие требования по соблюдению правовых и нормативных документов, требующих большего уровня сегментации сетей на уровне организаций и особенно на уровне центров обработки данных. Наконец, задача обеспечения производительности и доступности — два требования, объединенные в одно. Как правило, одно из этих требований сводится к упрощению. Сложность обычно означает возникновение дополнительных проблем, повышение вероятности перебоев в работе и увеличение задержек. Очень важно не усложнять систему. Второе требование относится к скорости. Необходимо обеспечить быструю обработку, не вносящую задержек. Если решения по обеспечению безопасности невозможно обновлять, они не останутся надолго в центрах обработки данных.

Обеспечение сетевой безопасности в центрах обработки данных связано с неприемлемыми компромиссами.

Сетевая безопасность в центрах обработки данных традиционно отставала от обеспечения защиты периметра сети. Причина этого заключается в том, что доступности и производительности приложений отдается больший приоритет по сравнению с безопасностью. Если приложение, развернутое в центре обработки данных, недоступно или не отвечает на запросы пользователей, организация зачастую упускает возможности для увеличения доходов. Поэтому в организациях обычно «упрощаются» средства обеспечения сетевой безопасности, слишком часто вызывающие задержки и перебои в работе. Когда на предприятиях создавали инфраструктуру безопасности периметра сети с использованием потоковой проверки трафика, в центрах обработки данных для обеспечения сетевой безопасности использовали списки управления доступом на маршрутизаторах. Позднее, когда в инфраструктуре обеспечения безопасности периметра сети на предприятиях стали использовать системы предотвращения вторжений (IPS), прокси-серверы, DLP и другие устройства, в некоторых центрах обработки данных только начали внедрять технологию потоковой проверки трафика. Такая историческая перспектива наглядно демонстрирует компромиссы, присущие обеспечению сетевой безопасности в центрах обработки данных:

- Производительность ИЛИ безопасность.
- Простота ИЛИ функциональность.
- Эффективность ИЛИ доступность.

Зачастую эти компромиссы являются аппаратными. Например, организации с центром обработки данных с выходом в Интернет при выборе оборудования приходилось выбирать между производительностью и безопасностью. С одной стороны, межсетевой экран класса поставщика услуг с высокой производительностью, но со слабыми средствами обеспечения безопасности. С другой стороны, межсетевой экран класса сетевого периметра с широким выбором средств обеспечения безопасности, но отличающийся невысокой производительностью и не обеспечивающий требуемую надежность. Проблема заключается в том, что после выбора оборудования организации приходилось внедрять все новые разработки и продукты для изменения баланса между безопасностью и производительностью.

Не все центры обработки данных одинаковы

При рассмотрении центра обработки данных с развернутым приложением страховой компании по внутренней обработке страховых требований и центра обработки данных, на котором развернут веб-сайт с онлайн-магазином розничных продаж, можно легко выявить значительные различия. Эти различия относятся к типу и количеству приложений, классам и количеству пользователей и к приоритетам и функциональным возможностям некоторых средств обеспечения безопасности. Далее в настоящем документе обсуждаются различные атрибуты и требования, предъявляемые к сетевой безопасности, для двух основных типов центров обработки данных:

- Корпоративные/внутренние центры обработки данных.
- Центры обработки данных с выходом в Интернет.

Хотя межсетевые экраны следующего поколения компании Palo Alto Networks предоставляют организациям основные элементы обеспечения сетевой безопасности для обоих типов центров обработки данных, вследствие значительных различий инновационные технологии компании Palo Alto Networks (см. Приложение) реализованы различным образом.

Корпоративные/внутренние центры обработки данных

Собственно говоря, корпоративные центры обработки данных связаны с большим количеством приложений и с меньшим количеством пользователей. При этом могут использоваться готовые приложения, приложения собственной разработки или адаптированные приложения. Могут использоваться веб-приложения или приложения с архитектурой клиент/сервер. Приложения могут быть терминальными или виртуализированными. Что касается пользователей, они, как правило, известны. Это сотрудники, поставщики или партнеры. См. рис. 1.

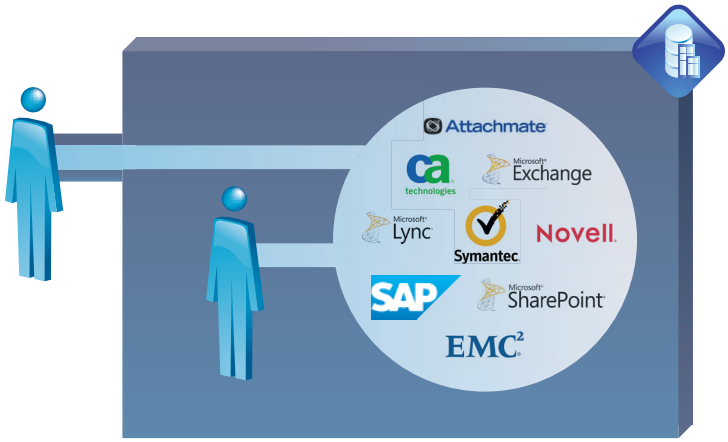

Рис. 1. Корпоративный центр обработки данных

Уникальные вопросы, связанные с обеспечением сетевой безопасности, с которыми сталкиваются корпоративные центры обработки данных, включают необходимость сегментации сети (обычно это связано с соблюдением нормативных требований), необходимость поддерживать связь с разработчиками приложений и требование по соответствию средств сетевой безопасности различным схемам центров обработки данных. Другая задача, решение которой приобретает все более важное значение в корпоративных центрах обработки данных, связана с увеличением количества неавторизованных приложений. Будь то неавторизованная установка SharePoint или использование администратором SSH на нестандартных портах, эти приложения необходимо идентифицировать и обеспечить управление по сетям центра обработки данных.

Решения Palo Alto Networks для корпоративных центров обработки данных

Как указано выше, сетевая безопасность в корпоративных центрах обработки данных зачастую связана с сегментацией сети. Хотя выполнить сегментацию сети можно с помощью любого межсетевого экрана, использовать сегментацию на основе портов и IP-адресов в центрах обработки данных не имеет смысла, так как центр находится в пределах периметра. То есть такая сегментация практически бесполезна перед комбинацией приложений и угроз, по большей части способных использовать любой открытый порт. Кроме того, контроль доступа по IP-адресу или пулу IP-адресов является также плохой аппроксимацией для пользователей. Неважно, необходимо ли обеспечить соответствие нормативным документам или другим внешним требованиям (например, PCI, Приложение F), предприятиям требуется обеспечить сегментацию сети по пользователям и приложениям. Например, в организации можно сегментировать серверы, на которых размещаются данные о владельцах кредитных карт, и обеспечить доступ к этому сегменту только для финансовых пользователей, использующих приложение для проведения платежей. Таким образом обеспечивается ограничение доступа и отслеживаемость отдельных пользователей. Такой уровень контроля и, что наиболее важно, возможность аудита, являются незаменимыми для многих крупных предприятий.

Другим основным атрибутом корпоративных центров обработки данных является разнородность архитектур. Частично это связано с тем, что в некоторых организациях центры обработки данных разбросаны по разным местам. Это означает, что стойки с маршрутизаторами, центральными коммутаторами, коммутаторами подключения и другим сетевым оборудованием могут различаться ввиду широкого применения виртуальных ЛВС и компонентов распределенных приложений. Другим преимуществом межсетевых экранов следующего поколения компании Palo Alto Networks является возможность их интеграции на уровнях L1 (виртуальное соединение), L2 и L3 даже при эксплуатации в смешанном режиме в устройстве с плотным размещением портов. Более того, способность объединять в магистрали виртуальные локальные сети, агрегировать порты и выполнять ролевое администрирование в зонах безопасности и виртуальных межсетевых экранах обеспечивает организациям возможность интегрировать межсетевые экраны в любую архитектуру и операционную модель. На рисунке 2 представлена схема «межсетевого экрана второго уровня» с использованием виртуальной ЛВС и интеграцией на уровне L2. Межсетевой экран остается встроенным, но гибкая интеграция позволяет корпоративным пользователям использовать необходимую сетевую архитектуру.

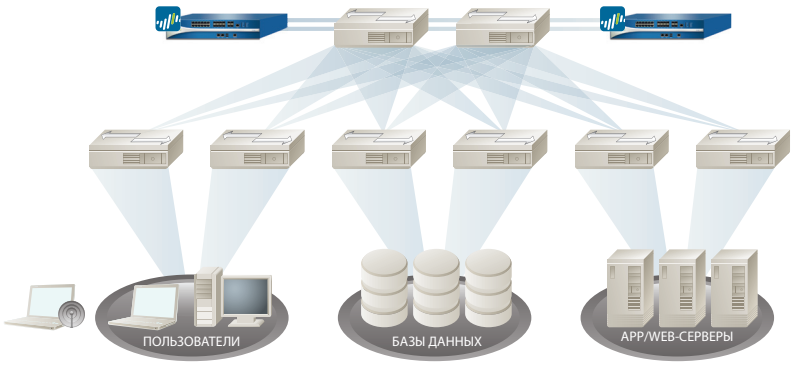

Рис. 2. Схема корпоративного центра обработки данных на уровне L2 с использованием виртуальных ЛВС с оборудованием компании Palo Alto Networks

Наконец, еще одним из основных преимуществ межсетевых экранов следующего поколения компании Palo Alto Networks для корпоративных центров обработки данных является управление неавторизованными приложениями. Неавторизованные несконфигурированные приложения SharePoint, неавторизованное использование SSH на нестандартных портах и даже системы обмена файлами P2P выявляются и контролируются с помощью приложений заказчика. Другой более реальный пример. Известно, что разработчики приложений реализуют компоненты баз данных и других приложений на любых удобных портах. Вместо контроля разработчиков приложений контролируйте приложения. Например, если MySQL является приложением, разрешенным между зонами безопасности, работа этого приложения разрешается независимо от используемого порта. Это значительно упрощает контакты с разработчиками и обеспечивает безопасную работу приложений, не увеличивая возможности для атак.

Центры обработки данных с выходом в Интернет

В центрах обработки данных с выходом в Интернет, как правило, используется относительно мало приложений. Обычно это веб-приложения (на базе браузера). Зачастую в этих приложениях используется один из стандартных «наборов» веб-инфраструктур (например, IBM, LAMP, Microsoft, Oracle). При этом пользователей много, причем часто это неизвестные пользователи или пользователи с неизвестными полномочиями. См. рис. 3.

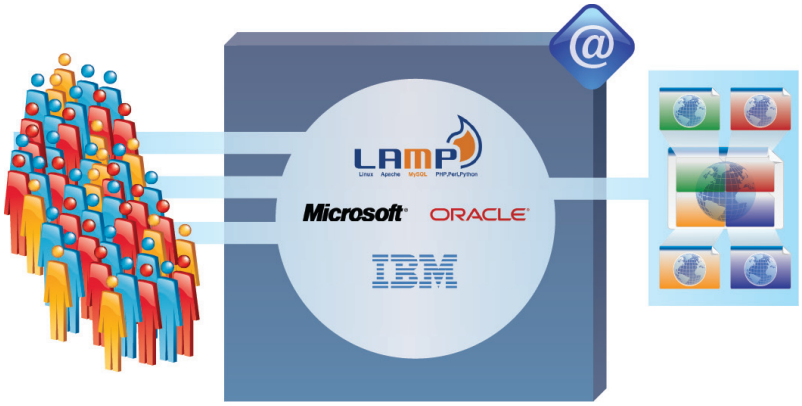

Рис. 3. Центр обработки данных с выходом в Интернет

Уникальность задач по обеспечению сетевой безопасности в центрах обработки данных с выходом в Интернет связана с конструкцией (например, встроенный межсетевой экран в отказоустойчивом развертывании с высокой пропускной способностью, но где размещать систему предотвращения вторжений (IPS) с учетом общих проблем, связанных с производительностью этой системы?), упомянутыми ранее аппаратными компромиссами и мониторингом (например, что используется, что подвергается атаке?).

Решения Palo Alto Networks для центров обработки данных с выходом в Интернет

В центрах обработки данных с выходом в Интернет межсетевые экраны следующего поколения компании Palo Alto Networks обеспечивают преимущества, связанные с гибкостью использования. Теперь на предприятиях могут выбрать инфраструктуру сетевой безопасности без учета производительности или безопасности. Изменение средств обеспечения безопасности представляет собой настройку политики — начиная от сканирования всего контента, политик межсетевых экранов для приложений и пользователей и заканчивая основными политиками для межсетевого экрана.

Дополнительным преимуществом такой гибкости является упрощение. См. рис. 4. Разработчикам сетей для центров обработки данных больше не требуется ломать голову над тем, как внедрить систему предотвращения вторжений (что обычно являлось узким местом при разработке). По результатам тестирования межсетевых экранов следующего поколения компании Palo Alto Networks на предмет предотвращения вторжений, проведенного компанией NSS, межсетевые экраны не только обеспечивают верхний уровень блокировки (93,4 % при 100 % устойчивости к вторжениям с использованием маскировки), но и превосходят заявленные характеристики (обеспечивая пропускную способность в 115 % от номинальной). Разработчики сетей для центров обработки данных могут упросить свои проекты.

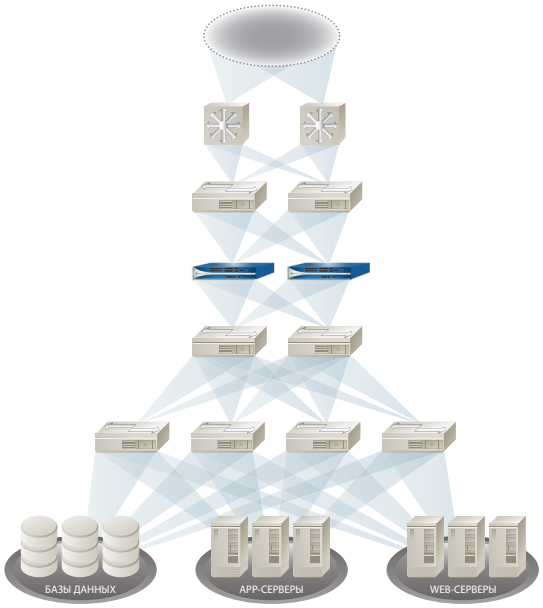

Рис. 4. Решения Palo Alto Networks для центров обработки данных с выходом в Интернет

Наконец, значительные преимущества обеспечивает возможность мониторинга из одной точки. Обычно «мониторинг» означает просмотр нескольких файлов журналов в поисках «иголки в стоге сена». Для пользователей в центрах обработки данных с решениями от компании Palo Alto Networks мониторинг приложений и трафика, а также журналы входящих URL-адресов и журналы угроз доступны с помощью одного пользовательского интерфейса. Это позволяет исключить необходимость выбора между возможностями мониторинга и эффективностью.

Межсетевые экраны следующего поколения дают вторую жизнь сетевой безопасности в центрах обработки данных

Благодаря инновационным технологиям (App-ID, User-ID и Content-ID и однопроходной архитектуре параллельной обработки — дополнительные сведения см. в Приложении) межсетевые экраны следующего поколения компании Palo Alto Networks позволяют исключить компромиссы, свойственные сетевой безопасности центров обработки данных. Впервые организации могут решить следующие задачи:

- Предотвращение угроз.
- Соответствие нормативным документам и сегментация.
- Обеспечение производительности и доступности приложений.

При этом не требуется искать компромиссы между производительностью, простотой, эффективностью и безопасностью, функциональностью и мониторингом.

Приложение

Уникальные технологии компании Palo Alto Networks

В компании Palo Alto Networks разработаны четыре уникальных технологии, помогающие клиентам обеспечить соответствие требованиям, предъявляемым к сетевой безопасности для обоих типов центров обработки данных, и устранить необходимость компромиссов между безопасностью, функциональностью, мониторингом и производительностью, простотой и эффективностью.

- App-ID.
- User-ID.
- Content-ID.
- Архитектура параллельной обработки за один проход.

App-ID — основной механизм классификации трафика

Средства точной классификации трафика — основной компонент любого межсетевого экрана, а результаты их применения — основа политики безопасности. Традиционные межсетевые экраны классифицируют трафик по портам и протоколам. В свое время такой подход был достаточным для надежной защиты центров обработки данных. Современные приложения и угрозы легко обходят межсетевые экраны, выполняющие фильтрацию трафика на основании портов. Это выполняется с помощью динамической смены портов, использования протоколов SSL и SSH, туннелирования своего трафика через порт 80 или использования нестандартных портов. Технология App-ID (подана заявка на патент) представляет собой уникальный механизм классификации трафика, разработанный в компании Palo Alto Networks, который снимает ограничения на классификацию трафика при мониторинге, которым подвержены традиционные межсетевые экраны. Это выполняется за счет использования нескольких механизмов классификации трафика на устройстве — будь то стандартное приложение, упакованное приложение или пользовательское приложение.

User-ID — технология интеграции пользователей и групп каталогов с политикой обеспечения безопасности сетей

В любом стандартном межсетевом экране компании Palo Alto Networks технология User-ID связывает IP-адреса с определенными идентификаторами пользователей. Благодаря этому появляется возможность осуществлять мониторинг сетевой активности на основе отдельных пользователей. Благодаря тесной интеграции с Microsoft Active Directory (AD) и другими каталогами LDAP агент идентификации пользователя, разработанный в компании Palo Alto Networks, обеспечивает выполнение этой задачи двумя способами. Во-первых, агент периодически проверяет и поддерживает связь между пользователями и IP-адресами, используя мониторинг входа в систему, опрос конечных станций и методы адаптивного портала. Затем агент связывается с контроллером домена AD и собирает соответствующую информацию о пользователях, например сведения о назначении ролей и групп пользователям. Затем эти данные используются при решении следующих задач:

- Мониторинг (и возможность аудита) пользователей, несущих ответственность за трафик всех приложений, контента и угроз в сети.
- Возможность использовать в политиках контроля доступа идентификаторов пользователей в качестве переменных.
- Поддержка поиска и устранения неисправностей/реагирования на события и использование соответствующих данных в отчетах.

Технология User-ID предоставляет ИТ-подразделениям еще один эффективный механизм интеллектуального контроля использования приложений. Например, приложение, в котором хранятся управляемые данные, можно сделать доступным для отдельных пользователей или групп, имеющих право на запросы к этому приложению, с одновременным сканированием для снижения рисков и регистрацией попыток доступа в соответствии с требованиями аудита и сохранения данных.

Content-ID — технология сканирования трафика для защиты от угроз

Технология Content-ID, как и другие подобные технологии, привносит в межсетевые экраны следующего поколения компании Palo Alto Networks возможности, ранее недоступные для корпоративных межсетевых экранов. В данном случае это отражение угроз в реальном времени, связанных с разрешенным трафиком приложений, подробный мониторинг использования веб-приложений, а также фильтрация файлов и данных.

Предотвращение угроз. В этом компоненте Content-ID несколько инновационных функций используются для предотвращения попыток взлома защиты сетей посредством атак вирусов, шпионского программного обеспечения и использования уязвимостей приложений от проникновения в сеть независимо от типа трафика приложений (старый или нового поколения), который используется в качестве транспорта.

- **Декодер приложения.** Технология Content-ID использует компонент App-ID для предварительной обработки потоков данных, которые затем проверяются на наличие определенных идентификаторов угроз.
- **Унифицированный формат сигнатур угроз.** Повышение производительности достигается за счет устранения необходимости в раздельных механизмах сканирования для каждого типа угроз. Выявление вирусов, шпионского программного обеспечения и эксплойтов уязвимостей выполняется за один проход.
- **Защита от атак, использующих уязвимости (IPS).** Надежные процедуры по нормализации и дефрагментации трафика объединены в механизмах выявления отклонений в протоколах, поведении и в механизмах эвристического анализа. Эти механизмы обеспечивают комплексную защиту от широкого диапазона известных и неизвестных угроз.
- **Встроенное ведение журналов URL-адресов.** Выявление используемых или подвергшихся атаке элементов веб-приложений в центре обработки данных.

Фильтрация файлов и данных. Этот набор функций использует преимущества подробного анализа приложений, выполняемого с помощью технологии App-ID, и позволяет использовать политики, снижающие риски, связанные с несанкционированной передачей файлов и данных. Набор функций включает возможность блокировать файлы по фактическому типу (то есть не на основе просто расширений файлов) и возможность контролировать передачу конфиденциальных шаблонов данных, например номеров кредитных карт и карт социального страхования.

Результат заключается в том, что с помощью технологии Content-ID ИТ-подразделения получают возможность предотвращать известные и неизвестные угрозы, повысить уровень мониторинга и гарантировать допустимое использование. И все это без снижения производительности, простоты или эффективности.

Архитектура параллельной обработки за один проход является основой высокопроизводительной платформы

В первую очередь, инфраструктура сетевой защиты в центрах обработки данных должна работать. Как уже сказано ранее, не следует устанавливать в центре обработки данных то, что не работает. Для создания настоящего межсетевого экрана следующего поколения в компании Palo Alto Networks пришлось разработать новую архитектуру, позволяющую выполнять функции с большим объемом вычислений (например, идентификация приложений) со скоростью передачи данных по кабелю.

В межсетевых экранах следующего поколения компании Palo Alto Networks архитектура параллельной обработки за один проход (SP3) используется для защиты сред центров обработки данных при скорости обмена данными до 20 Гбит/с.

Двумя основными элементами архитектуры SP3 являются однопроходная архитектура программного обеспечения и специализированная аппаратная платформа. Архитектура SP3, разработанная в компании Palo Alto Networks, представляет собой уникальный подход к интеграции аппаратных и программных средств, который позволяет упростить управление, процессы обработки и максимизировать производительность.

Программное обеспечение с однопроходной обработкой

Программное обеспечение с однопроходной обработкой компании Palo Alto Networks предназначено для выполнения двух основных функций межсетевых экранов следующего поколения, производимых компанией Palo Alto Networks. Во-первых, программное обеспечение с однопроходной обработкой выполняет операции один раз на один пакет. При обработке пакета сетевые функции, поиск политик, идентификация и декодирование приложений и сопоставление сигнатур любых угроз и контента выполняются всего один раз. Это значительно сокращает объем служебных операций при обработке, которые необходимы для выполнения нескольких функций в одном устройстве обеспечения безопасности.

Во-вторых, этап сканирования контента в программном обеспечении с однопроходной обработкой компании Palo Alto Networks выполняется на основе потоков, а для определения и блокировки угроз используется унифицированное сопоставление сигнатур. Вместо использования отдельных механизмов и наборов сигнатур (требующих многопроходного сканирования), а также вместо использования файловых прокси-серверов (требующих загружать файлы перед сканированием) программное обеспечение с однопроходной обработкой, установленное в межсетевых экранах следующего поколения, сканирует контент один раз на основе потоков, чтобы избежать внесения задержек.

Такая однопроходная обработка обеспечивает очень высокую пропускную способность и низкие задержки при активных функциях безопасности. Дополнительным преимуществом является использование одной полностью интегрированной политики, позволяющей упростить управление безопасностью корпоративной сети.

Аппаратура параллельной обработки

Другим важным аспектом архитектуры Palo Alto Networks SP3 является оборудование. В межсетевых экранах следующего поколения компании Palo Alto Networks используется несколько банков специализированных функций обработки, которые работают в параллельном режиме, обеспечивая максимальную эффективность программного обеспечения с однопроходной обработкой.

- **Сетевые функции.** Маршрутизация, поиск в потоках, статистические расчеты, преобразование сетевых адресов (NAT) и другие подобные функции выполняются с помощью специализированного сетевого процессора.
- **Безопасность.** Технологии User-ID, App-ID и процесс поиска политик выполняются с использованием многоядерного механизма обработки, предназначенного для обеспечения безопасности, обеспечивающего ускоренное шифрование, дешифровку и декомпрессию.
- **Предотвращение угроз.** Технология Content-ID для анализа контента на наличие вредоносного программного обеспечения любого типа использует специализированный процессор сканирования контента.
- **Управление.** Специализированный процессор управления выполняет задачи по управлению конфигурациями, ведению журнала и созданию отчетов без использования оборудования по обработке данных.

Заключительный элемент архитектуры относится к встроенным средствам отказоустойчивости, которая обеспечивается за счет физического разделения уровней данных и управления. Такое разделение означает, что интенсивное использование одного из уровней не будет негативно влиять на другой уровень. Например, администратор может создавать отчет, интенсивно использующий процессор. При этом возможность обработки пакетов будет полностью сохранена благодаря разделению уровней данных и управления.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Главный офис: +1.408.573.4000
Отдел продаж: +1.866.320.4788
Служба поддержки: +1.866.898.9087

www.paloaltonetworks.com