Отказоустойчивая безопасность

Рассматриваются современные схемы реализации отказоустойчивости ряда ключевых компонент систем безопасности распределенных информационных систем (ИС), позволяющие добиться максимальных показателей надежности, использования оборудования и каналов связи при общей оптимизации затрат.

Введение

Информационные технологии серьезно влияют на течение современного бизнеса. Еще несколько лет назад всерьез обсуждались проблемы внедрения компьютеров в организации и мучительно рассчитывались выгоды от установки компьютеров на рабочие места: насколько замедлит компьютер бизнес-процессы, считая компьютерные технологии еще одной параллельной системой учета, которую также надо содержать (заполнять необходимые формы, документы и др.). Современная компания немыслима без систем электронного документооборота и других технологий, где все делается при помощи информационных систем. Соответственно, и объемы информации, обрабатываемые системами, возросли на несколько порядков, и системы обработки информации и ее хранения преобразовались в мощные дата-центры с резервированием не только в локальном месте, но и в распределенные дата-центры, которые сейчас набирают все большую популярность и способны обеспечить непрерывность работы системы даже в случае полного разрушения одного или даже нескольких из них.

Однако при всей мощной системе резервирования часто возникают проблемы другого рода, которые могут свести решение задачи сохранения информации и непрерывности работы на нет.

Простой пример: известное отключение электроэнергии в Москве показало, насколько многие компании не готовы к обеспечению непрерывности бизнеса. У них были резервированы центры обработки данных, и все переключилось на резервный. Но что такое ЦОД без пользователей, которые должны работать с информацией?

Оказалось, у некоторых не было возможности обеспечить пользователей бесперебойным питанием и каналами связи до ЦОД (они тоже отключились), у других начались проблемы с системами безопасности: пользователи, присоединяющиеся непонятно откуда с другими приложениями и др. – понятно, что системы безопасности начинают блокировать такую работу. Можно вспомнить немало примеров, когда для экстренной работы обеспечивали доступ по упрощенным схемам различного рода сотрудникам, когда системы безопасности начинали работать в нештатном режиме и именно в эти моменты происходили кражи информации (например, базы данных).

Вместе с обеспечением процессов непрерывности бизнеса, необходимо рассматривать и процессы обеспечения непрерывной защиты информации в организации, особенно в чрезвычайных обстоятельствах. Соответственно, и системы безопасности должны также быть тщательно спроектированы для обеспечения непрерывности бизнеса.

Тенденции бизнеса

Ввиду быстрого развития информационных технологий и повышения скорости и динамичности ведения бизнеса современных организаций, в системах безопасности происходят также изменения, которые влияют на их построение.

Если посмотреть на отчет CSI/FBI за 2006 г., где показаны потери от разного рода атак (рис. 1), то видно, что в "пятерке лучших" находятся вирусы, несанкционированный доступ к информации, воровство информации и атаки DoS (специально не делаем акцент на воровстве ноутбуков из-за того, что у нас, люди, ворующие ноутбуки, редко интересуются бизнесом компании).

Все эти атаки как раз в плане построения отказоустойчивых корпоративных систем, способных работать непрерывно, становятся наиболее актуальными.

Почему информационная безопасность является одной из важных составляющих обеспечения непрерывности бизнеса?

Проблемы, возникающие в системе безопасности современной организации и особенно ее дата-центра, часто недооцениваются персоналом. Нестабильная работа систем безопасности может приводить к более серьезным проблемам, нежели явный перерыв в работоспособности сервера.

Во-первых, часто неочевидно для пользователей и администраторов: что происходят какие-то несанкционированные действия; трудно распознать, когда именно началась вредоносная активность и что произошло с системой. *Во-вторых*, об атаке, чаще всего, узнают в последний момент, когда все уже произошло и виден уже плачевный результат. При этом резервирование данных может не спасти – ошибка или искаженные данные будут распространяться и в системах резервирования, нередко делая невозможным их восстановление.

Как правило, процесс восстановления после таких атак достаточно длителен, устранение последствий нападения, уязвимостей или действий враждебного ПО может занять несколько дней.

В-третьих, вредоносные атаки могут приводить к повторяющимся остановам в работе при не полностью устраненных последствиях предыдущих атак или Backdoors, которые оставляют злоумышленники.

Другая сторона вопроса кроется в том, что в последнее время все чаще компании задумываются о непрерывности бизнеса и создают системы распределенных

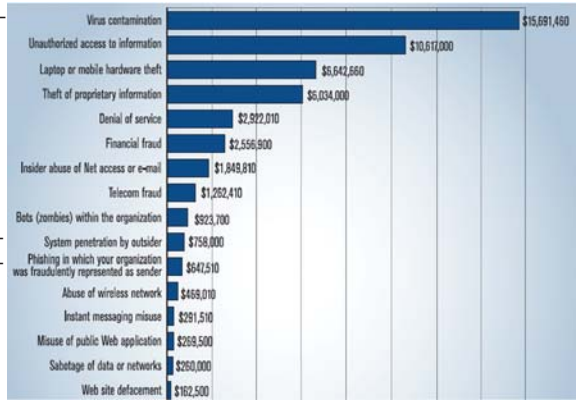

Рис. 1. Потери от разного рода атак по результатам исследования CSI/FBI за 2006 г.

дата-центров, находящихся на достаточно большом расстоянии друг от друга. Чтобы успешно участвовать в конкурентной борьбе, компании зачастую ускоряют внедрение сложных бизнес-приложений, забывая при этом о создании соответствующей IT-инфраструктуры и инфраструктуры безопасности, поддерживающей такие приложения. Во многих случаях это ведет к ухудшению производительности и надежности системы. Поэтому важно уже при начальном проектировании предусмотреть возможности масштабирования. Все это приводит к изменению технологий ведения бизнеса, хранения данных и передачи информации. Точно так же это и приводит и к изменению средств безопасности, которые должны теперь отвечать новым реалиям. В противном случае, средства безопасности могут стать тем "бутылочным горлышком", часто не позволяющим выполнять в срок поставленные бизнес-задачи.

Классическая схема обеспечения отказоустойчивости систем безопасности современных ИС

Итак, что нужно для успешной работы современной организации и ее центров обработки информации?

Рассмотрим классическую схему дата-центра. Типичная схема его построения – дублированная архитектура на уровне L2 (рис. 2). Это означает, что серверы включаются двумя сетевыми адаптерами в разные сетевые коммутаторы (switch), один из которых работает в резервном режиме, подключаясь в случае выхода из строя основного. Точно также дублируются и маршрутизаторы, и каналы связи (при этом возможно одновременное использование каналов связи). У каждого коммутатора устанавливается межсетевой экран для обеспечения высокой надежности – дублированный. Кроме того, применяются системы IPS/IDS, шифрование каналов связи.

Разделение дата-центра на зоны безопасности (как правило, на несколько DMZ-зон, зоны баз данных и др.) на самих серверах часто используются хостовые системы предотвращения вторжений (HIPS) и другие системы безопасности, например, системы анализа уязвимостей, или системы мониторинга и корреляции (отказоустойчивость данных систем – тема отдельной статьи).

Вроде бы все нормально, однако достаточно ли этого для современного дата-центра?

Рассмотрим потоки информации в дата-центре. Потоки информации могут быть разными: например, в канале связи между клиентом и дата-центром и между сервером приложений и базой данных. Причем, объем потоков может различаться в несколько раз: между клиентом и сервером приложений – мегабиты, а между сервером и базой – гигабиты. Это требует наличия очень мощного межсетевого экрана. Когда мощности не хватает, приходится разбивать систему на сегменты и ставить свои экраны для обеспечения надежности. Дополнительные экраны дублируют инфраструктуру – часто до четырех крат! Системы IPS, обладающие, как правило, невысокой пропускной способностью (обычно до 1 Гбит/с), также требуют кластеризации.

Таким образом, получается, с одной стороны, большой расход оборудования, с другой – недостаточная пропускная способность устройств в сравнении с требованиями, предъявляемыми в современных дата-центрах. Кроме того, информация между системами хранения должна постоянно реплицироваться по защищенным каналам связи и, как правило, это те же каналы связи, что и для связи с клиентами, что вносит дополнительные требования к каналам связи по надежности, приоретизации потоков и др. Таким образом, обычных схем резервирования, защищенных VPN-соединениями между клиентами и дата-центром и основным дата-центром и резервным, уже недостаточно, когда при пропадании связи они возобновляются по резервным каналам связи.

Последний момент, который хотелось бы отметить – управление. Когда основной центр выходит из строя и надо перевести всех пользователей на резервный, возникает большой объем проблем по правильной авторизации пользователей в новом дата-центре (всем ли туда есть доступ и есть ли актуальная информация о пользователях в резервном дата-центре?).

Что же необходимо?

1. Максимальное использование имеющегося оборудования, 50% которого простаивает в режиме ожидания, а производительности средств безопасности нередко не хватает для обеспечения полноценной защиты.

2. Полноценное резервирование всех систем.

3. Полноценное, по возможности, резервирование каналов связи.

4. Возможность резервирования системы управления и централизованное управление устройствами безопасности.

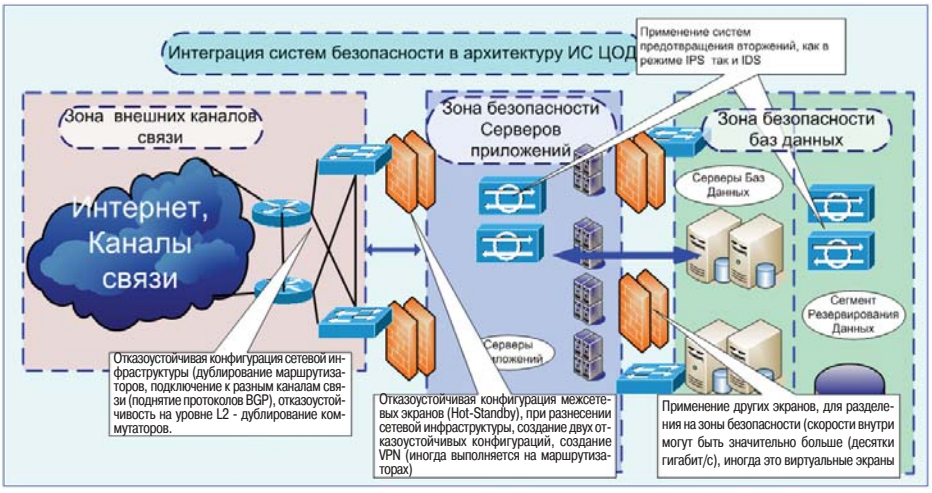

Рис. 2. Архитектура "классической" системы безопасности центров обработки данных.

Современные схемы реализации отказоустойчивости отдельных компонент систем безопасности ИС

Что предлагается в настоящее время различными вендорами? У каждой компании свои стратегии, многие из которых, в общих чертах похожи. Рассмотрим особенности современных схем реализации ряда ключевых компонент систем безопасности ИС.

Кластер кластеру рознь. Что лучше, Hot-standby или кластер?

Одна из последних тенденций при построении современных систем безопасности – использование различных схем кластеризации при реализации межсетевых экранов (МЭ).

В концепции фирмы Juniper предлагается использование межсетевых экранов, как в режиме Hot-Standby, так и в режиме Active/Active (я бы назвал это "псевдокластер").

Сущность подхода заключается в том, что каждый межсетевой экран является основным для своей зоны и резервным

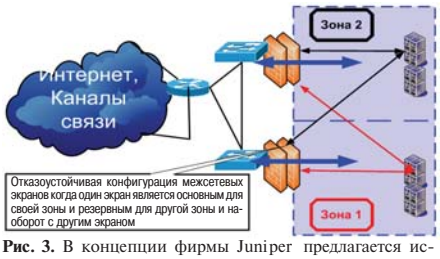

Рис. 3. В концепции фирмы Juniper предлагается использование межсетевых экранов как в режиме Hot-Standby и в режиме Active/Active.

– для другой зоны, которая работает через другой МЭ, а другой экран – зеркально для данной зоны (рис. 3).

Таким образом, предполагается, что оборудование не простаивает, и все оборудование задействовано и используется для нужд защиты информации дата-центра.

Cisco Systems предлагает также 2 варианта резервирования оборудования. Они идентичны и подозрительно похожи на то, что предлагает Juniper, поскольку в Juniper такие типы обеспечения резервирования работают давно (рис. 4).

Так же, как и в Juniper, для работы системы в таком же псевдокластере необхо-

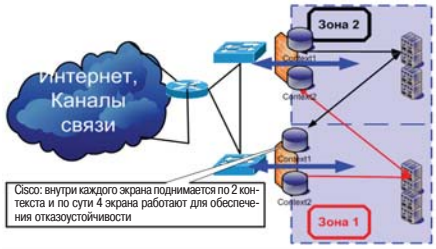

Рис. 4. Cisco Systems предполагает также 2 варианта резервирования оборудования аналогичные Juniper.

димо, чтобы оба устройства были абсолютно идентичны (можно только иметь разную флэш-память и один из них должен быть Unrestricted (для PIX)) и в каждом из них должно быть поднято по 2 контекста (context – виртуальный файрвол), т.е., если смотреть с точки зрения количества устройств, участвующих в процессе, то их 4! Один из них является основным для другого в соседнем устройстве и наоборот (см. рис. 4).

Как уже упоминалось, схема позволяет резервировать оборудование и одновременно использовать все имеющееся оборудование. Недостатками такой схемы можно считать невозможность масштабирования – нельзя добавить еще устройств (соответственно, рекомендуется не загружать на полную мощность устройства), кроме того – сложность администрирования и необходимость наличия дополнительного оборудования (router и др.) для работы экранов.

Другой подход демонстрирует МЭ Stonegate производства компании Stonesoft. Поскольку долгое время компания выпускала кластерное программное обеспечение как раз для межсетевых экранов (например, Checkpoint), то для работы МЭ ничего дополнительного не требуется. Межсетевые экраны образуют

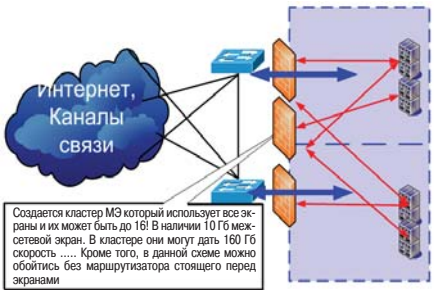

Рис. 5. Межсетевые экраны Stonegate производства компании Stonesoft образуют полноценный кластер, который виден администратору как один МЭ.

полноценный кластер, который виден администратору как один МЭ, и работает он, соответственно, более просто (рис. 5).

Все устройства работают параллельно и перераспределяют нагрузку между собой. В отличие от других решений, в данном случае не существенно, что добавляется в качестве еще одного МЭ в кластер. Требований по идентичности оборудования нет, что дает возможность более эффективно использовать закупленные экраны. Пропускная способность кластера равна суммарной пропускной способности всех компонентов (экранов), входящих в кластер, общая пропускная способность может достигать 160 Гбит/с! При этом неважно, какой именно или сколько экранов выйдут из строя. Пока хотя бы один работоспособен, все будет работать. При этом сохраняется возможность балансировать нагрузку между внутренними серверами, обеспечивая тем самым равномерную нагрузку между пулом внутренних серверов и оптимизируя нагрузку внутри ЦОД.

Нечто подобное (правда, с сильными ограничениями и не с такими широкими возможностями) предлагает и Checkpoint: ее продукт также иногда подозрительно похож на Stonegate (поскольку появился позже, чем Stonegate и до этого использовались разработки фирмы-производителя Stonegate). Данный продукт умеет поддерживать до 4 устройств и перераспределять нагрузку между экранами.

Совместное использование нескольких каналов связи

Другой вопрос заключается в необходимости использования разных каналов связи. Для обеспечения бесперебойности сейчас уже стало нормой использовать 2–3 провайдера каналов связи или интернет. Для обеспечения бесперебойности связи традиционно используются маршрутизаторы, на которых поднимаются сложные протоколы маршрутизации и отслеживается состояние канала.

Однако в последнее время появилось оборудование, которое при установке перед экранами позволяет без использования каких-либо протоколов типа BGP обеспечивать надежную балансировку нагрузки, подключая при этом большое количество провайдеров интернет, или предоставляющих услуги связи. Это значительно упрощает работу оборудования в целом, снижая риск остаться без связи в случае, когда администратор со стороны провайдера или администратор сетевого оборудования компании что-либо неправильно сконфигурировал.

В этом плане более интересный подход показывает, например, оборудование Checkpoint, к которому можно подключить 2 канала связи и на нем будет балансироваться нагрузка.

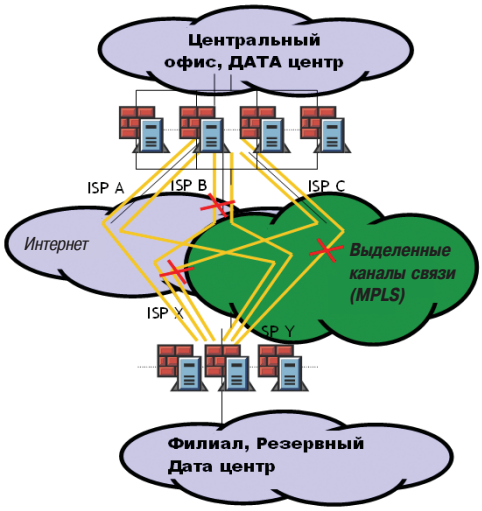

Рис. 6. К каждому кластеру Stonegate (независимо от количества экранов в кластере) можно подключить до 16 каналов связи (например, интернет), которые будут полностью сбалансированы по нагрузке.

Дальше всех "пошел" Stonegate. К каждому кластеру (независимо от количества экранов в кластере) можно подключить до 16 каналов связи (например, интернет), соответственно, для всего множества каналов связи со всех сторон создается множество туннелей, работающих одновременно (рис. 6).

Таким образом, информация передается по всем каналам, и пропускная способность VPN определяется суммой потоков всех каналов, и можно добиться скорости потоков более 6 Гбит/с. При неисправности в любой точке нагрузка равномерно перераспределяется между оставшимися, обеспечивая тем самым устойчивую и бесперебойную связь.

В плане оптимального использования каналов связи маленьким, но интересным моментом в увеличении эффективной полосы пропускания оборудования при передаче информации между ЦОД могут стать системы оптимизации трафика. Сейчас на рынке присутствуют такие производители как Juniper, Cisco, Digi и другие. Суть использования таких устройств заключается в установке их после межсетевых экранов между ними и внутренними сетями, таким образом, чтобы весь трафик проходил через них. Используя специальные алгоритмы сжатия для каждого протокола application-уровня, такие устройства позволяют уменьшить количество информации, посылаемой в канал связи, таким образом увеличивая количество информации, которое может быть передано по одному и тому же каналу связи. Для отдельных типов трафика достигается уровень сжатия трафика в несколько сотен раз!

Обеспечение отказоустойчивости систем IDS/IPS

Следующей проблемой является обеспечение отказоустойчивости систем IDS/IPS. Много говорится о скоростных показателях данных устройств и часто встречается ситуация, когда, например, для защиты от атак при использовании оборудования CISCO проектировщики вставляют в обладающий очень большой производительностью Catalyst 6500 специализированный модуль IDSM-2 с паспортной пропускной способностью 600 Мбит/с и пытаются мониторить потоки в несколько гигабит. Причем, паспортная мощность обычно рассчитывается на пакетах размером 1500 байт, а в интернете, к примеру, такие большие пакеты редко можно встретить, соответственно, и реальные скорости могут отличаться – чуть ли не вполовину меньше.

На рынке IPS высокоскоростные устройства предлагает небольшое количество фирм: Tipping Point – 5Гбит/с, ISS – 2 Гбит/с, Stonesoft (stonegate) – 2 Гбит/с. Скорость остальных – обычно не выше 1 Гбит/с. Соответственно, встает вопрос, как обеспечить нужную пропускную способность и при этом обеспечить и надежность решения?

Надежность состоит из двух компонент: при выключении системы предотвращения доступа (или других неполадках) часто требуется обеспечить бесперебойную связь. Вот тут-то на помощь приходят устройства под названием TAP (bypass), аппаратно обеспечивающие бесперебойность канала связи даже при выключении питания, но и полностью сохраняющие контроль над линией, позволяя IPS/IDS реагировать на нарушения. Производителей на рынке много, например, Intrusion, Critical Tap, и устройства работают вполне надежно. Данные модули очень полезны и тем, что в коммутаторах редко встречается более 2–3 полноценных сессий перенаправления трафика на Span-порт.

Как правило, старшие модели Juniper, Cisco и все модели Tipping Point и Stonegate обладают встроенными аппаратными модулями Bypass, что облегчает их внедрение в режиме IPS.

Для обеспечения надежного мониторинга линий системы IPS могут включаться последовательно и обеспечивать анализ трафика в случае выхода одного из компонентов из строя (рис. 7).

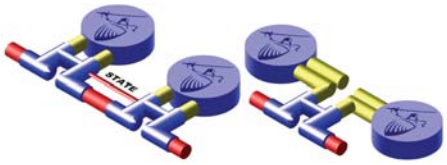

Рис. 7. Для обеспечения надежного мониторинга линий системы IPS могут включаться последовательно и обеспечивать анализ трафика в случае выхода одного из компонентов из строя.

В случае, если один сенсор пропустил атаку или вышел из строя, другой проведет анализ и выявит нарушение. В таком режиме часто ставят разновендорные IPS-системы для более детального и надежного анализа.

Другой аспект – каким образом добиться необходимой пропускной способности?

В этом помогут такие технологии, как, например, Ether channel, когда потоки распределяются равномерно между несколькими линиями и на каждую линию можно установить свою IPS-систему.

Кроме того, существуют способы обеспечения распределения нагрузки, например, используя контентные балансировщики нагрузки или возможности некоторых маршрутизаторов по балансированию нагрузки между портами, к каждому из которых можно подключить по IPS и залить централизованно политики. Однако, с точки зрения управления, это будет не самый простой способ и точно знать, что

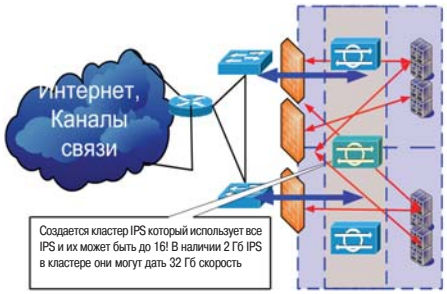

Рис. 8. Только 2 вендора предлагают кластеризацию своих продуктов: Symantec и Stonesoft. В Stonesoft кластеризация осуществляется таким же способом, как и в межсетевом экране Stonegate. При этом можно провести кластеризацию до 16 устройств, получив суммарную производительность до 32 Гбит/с.

все сетевые пакеты и соединения были проанализированы, будет нельзя.

Только 2 вендора предлагают кластеризацию своих продуктов: Symantec и Stonesoft.

В Stonesoft кластеризация осуществляется таким же способом, как и в межсетевом экране Stonegate. При этом можно провести кластеризацию до 16 устройств, получив суммарную производительность до 32 Гбит/с (рис. 8).

Кластер позволит контролировать потоки информации и управлять всем, как одним устройством, что удобно, когда необходимо задать единую политику безопасности и обеспечивать балансировку нагрузки между устройствами.

Обеспечение отказоустойчивости систем управления

Отказоустойчивости систем управления долгое время не придавалось большого значения. Считалось, что при неисправности системы управления ничего не происходит и можно всегда успеть переставить систему без каких-либо проблем, с точки зрения работоспособности собственно сети и инфраструктуры информационной системы. Однако в последнее время, когда появились распределенные системы безопасности, многие столкнулись с необходимостью оперативного управления как собственно системой, так и управления системами доступа пользователей и оперативного мониторинга событий. Здесь выбор пока ограничен: Checkpoint предлагает вариант основной-резервный, Stonegate по-

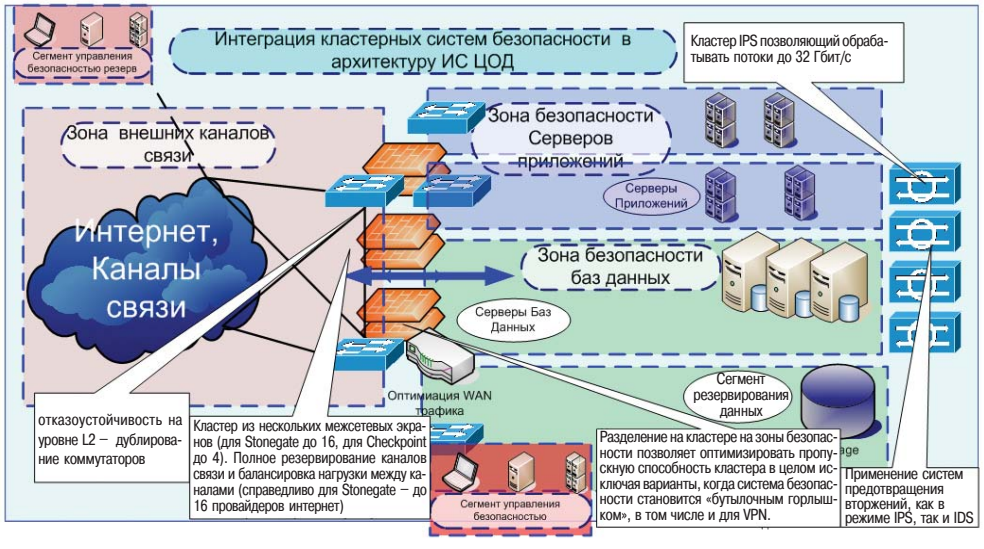

Рис. 9. Современная система безопасности центров обработки данных.

зволяет создать до 5 распределенных систем управления, каждая из которых обладает актуальной и полной информацией о политиках, правилах доступа и др. Вся управляющая информация регулярно обновляется на всех системах управления. При этом резервируется и система сбора журналов безопасности (лог сервера).

Таким образом, современная система безопасности центров обработки данных может приобрести несколько другой вид (рис. 9).

Мы получаем единый кластер межсетевых экранов, который позволяет обрабатывать трафик с большой скоростью без существенных задержек, образуя несколько зон безопасности и контролируя все потоки информации, проходящие в датацентре. При этом обеспечивается высшая степень отказоустойчивости системы. Системы предотвращения вторжений также кластеризуются и обеспечивают анализ всех сегментов безопасности на вредоносные воздействия, и при этом можно допустить выход из строя нескольких из них без потери контроля над безопасностью всех сегментов, поскольку вышедшие из строя системы замещаются другими. Системы межсетевого экранирования совместно с IPS становятся не только средством, позволяющим разделить информационную систему на зоны безопасности, не снижая производительности системы в целом, но и средством управления потоками безопасности.

Каналы связи подключаются непосредственно к системе межсетевого экранирования, и при этом никто не решает проблемы маршрутизации информации через нескольких провайдеров связи – кластер это решает автоматически. Причем все системы безопасности резервированы не только сами, но также их система управления и мониторинга. Пропускная способность каналов связи используется полностью за счет как оптимизации прохождения трафика, так и за счет его эффективного сжатия перед передачей по каналам связи, что сильно снижает общую стоимость владения такой системой.

Выводы

Новые тенденции порождают новые задачи для систем безопасности, о которых ранее не задумывались разработчики. Подходы, реализуемые в настоящий момент, очень разные, и при построении системы безопасности надо пристальное внимание уделять вопросам обеспечения непрерывности выполнения своих функций подсистемами безопасности. Как показано в статье, применение систем изначально ориентированных на обеспечение непрерывности бизнеса, сильно облегчают как задачу обеспечения безопасности потоков информации и собственно информации в целом, так и вопросы обеспечения работоспособности в критических условиях. На рынке ситуация меняется в сторону обеспечения надежности, и здесь на смену традиционным концепциям приходят новые, более эффективные.

Михаил Романов,
начальник отдела информационной безопасности и планирования непрерывности бизнеса, компания "ТехноСерв А/С

Cisco и RSA улучшают шифрование данных

Май 2007 г. – Компании Cisco® и RSA (подразделение компании EMC, занимающееся исследованиями и разработками в области информационной безопасности) расширили стратегическое сотрудничество, объявив о совместной разработке технологии, которая поможет заказчикам усовершенствовать и упростить шифрование конфиденциальной информации: медицинских записей, идентификаторов социальной защиты и номеров кредитных карточек. Новая технология позволит шифровать данные, сброшенные на ленточные накопители и другие средства хранения, а также управлять ключами защиты в сетях SAN. Этот подход, не требуя вмешательства в структуру данных, повышает уровень их защиты и отличается простотой управления.

При разработке совместных технологий компании Cisco и RSA будут использовать систему Cisco SME (Storage Media Encryption), которая предлагает шифрование хранимых данных как услугу коммутации, и систему RSA® Key Manager (централизованное решение для управления шифрованием в течение всего жизненного цикла данных). Сочетание этих систем предоставит общим заказчикам Cisco и RSA надежную, хорошо масштабируемую технологию безопасности для управления шифрованными данными и ключами шифрования. Технология Storage Media Encryption поможет удовлетворить строгие нормативные и законодательные требования и обеспечить надежную защиту данных даже в случае кражи или потери носителя. Новая технология будет пользоваться открытыми интерфейсами API для управления ключами, что позволит гибко внедрять решения для хранения и шифрования данных, в наибольшей степени отвечающие требованиям бизнеса.

Intel: сервер хранения на базе 4-ядерных процессоров

Апрель 2007 г. – Корпорация Intel объявила о выпуске сервера хранения данных Intel® SSR212MC2 – первого в отрасли интегрированного сервера хранения данных высотой 2U на базе четырехъядерного процессора – Intel® Xeon® серии 5300, оснащенного 12 жесткими дисками. Сервер легко конфигурируется в NAS-сервер, SAN-сервер и сервер-приложений и позиционируется для компаний малого и среднего бизнеса.

Производительность сервера увеличилась почти вдвое по сравнению с предыдущим поколением серверов. Он может поставляться с одним или с двумя двухъядерными процессорами Intel Xeon серии 5100. Можно будет также выбрать тип используемых жестких дисков – SAS уровня предприятия или SATA большой емкости.

Intel обеспечивает совместимость ОС и/или приложений широкого круга сторонних разработчиков программных решений с новой платформой, включая такие компании, как: Microsoft, FalconStor, Open-E, Open SuSE, RedHat и Wasabi Systems. Также Intel также сотрудничает с основными поставщиками аппаратного обеспечения, включая Emulex и Mellanox, давая возможность использования в новой платформе широкого ряда сетевых решений, таких, как Fibre Channel и InfiniBand.

Стоимость сервера Intel SSR212MC2 – около $2800 в комплектации без RAID-контроллера и $3600 с RAID-контроллером Intel SRCSAS144e.

Объем российского рынка WAFS/WDS-решений – более $20 млн

Апрель 2007 г. – Компании "Ай-Теко", Riverbed и Zycko провели совместный семинар по представлению решений компании Riverbed Technology на российском рынке. С презентациями выступили: директор ZYCKO Russia Алексей Немыченков, менеджер по развитию бизнеса "Ай-Теко" Максим Матросов, управляющий директор Riverbed по Центральной и Восточной Европе Джерард Бауэр *(Gerard Bauer)* и др.

Джерард Бауэр *(Gerard Bauer)* – управляющий директор Riverbed Technologies по Центральной и Восточной Европе.

Компания Riverbed Technology является разработчиком ПО в области WAFS/WDS-решений (Wide Area Files Servies/Wide-area Data Services) – быстро растущей категории продуктов для решения проблем пропускной способности и задержек в распределенных сетях. В соответствии с одним из последних аналитических отчетов Garner (сент. 2006 г.) среди производителей WAFS/WDS-решений (Wide Area Files Servies/Wide-area Data Services), компания Riverbed Technology Inc. была отнесена к группе лидеров.

Продукты компании Riverbed представляют собой программно-аппаратные комплексы (стандартный сервер с установленным ПО) для различных групп пользоавателей, позволяя уменьшать объем передаваемого WAN-трафика до 95% и увеличивая скорость работы приложений до 100 раз. Это достигается за счет удаления эффектов ограниченной полосы пропускания и высоких задержек, вследствие чего осуществляется оптимизация всего TCP-трафика, включая файловые, почтовые, ERP-приложения,