ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ CISCO ДЛЯ ПРЕДПРИЯТИЙ: РЕШЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Интегрированный подход к обеспечению безопасности консолидированных центров обработки данных на всех уровнях

КРАТКОЕ СОДЕРЖАНИЕ

Администраторы, занимающиеся консолидацией ресурсов центров обработки данных для повышения эффективности работы центров, должны учитывать влияние, оказываемое вносимыми изменениями, на безопасность. Cisco предлагает интегрированную стратегию обеспечения безопасности центра обработки данных на всех уровнях, позволяющую администраторам разделять центры обработки данных на "зоны" безопасности, в которых для каждого приложения применяются соответствующие политики безопасности, тем самым, ограничивая проникновение вирусов или Интернет-червей, которые могут нарушать систему безопасности. В этой стратегии используются преимущества, предлагаемые архитектурой Business Ready Data Center ("Центр обработки данных для предприятий") и средства обеспечения безопасности, которые интегрированы в сетевые решения Cisco.

ЗАДАЧИ

Центры обработки данных (ЦОД) привлекают внимание многих злоумышленников. Центр обработки данных, не имеющий надлежащей защиты, является объектами атак со стороны взломщиков и проникновения Интернет-червей, которые могут внести хаос в работу центра и причинить значительный материальный ущерб. К сожалению, при быстром внедрении центров обработки данных в период экономического бума 1990-х годов вопросам обеспечения их безопасности уделялось недостаточно внимания, и построенные в то время многочисленные "островки" приложений и хранилищ чаще всего уязвимы для атак и взлома. Частично, высокая скорость распространения Интернет-червей и вирусов обусловлена и тем фактом, что в центрах обработки данных по всему миру используются недостаточные или неадекватные технологии и процедуры обеспечения безопасности.

В соответствии с основными задачами управления предприятием, среди которых можно выделить обеспечение безопасности работы, оптимизацию бизнес-процессов и расширение сферы деятельности, многие ИТ-организации стремятся консолидировать ресурсы центров обработки данных: серверы, хранилища данных, сети и приложения. При проведении такой консолидации сотрудники ИТ-отделов и сетевые администраторы должны учитывать влияние вносимых изменений на средства обеспечения безопасности и на отказоустойчивость приложений. Раньше при обеспечении безопасности администраторы полагались на физическую изоляцию приложений или на средства обеспечения безопасности периметра. Сегодня эти меры уже не способны защитить ресурсы и приложения от атак, которые постоянно становятся все более изощренными и опасными. Любой начинающий злоумышленник может загрузить средства для взлома с одного из многочисленных web-сайтов, воспользоваться загруженной программой и нанести серьезный ущерб слабо защищенному центру обработки данных. Способы нападения совершенствуются быстрее, чем когда-либо. Сегодня ущерб, нанесенный всего за несколько секунд, может превышать ущерб, который пять лет назад мог бы быть нанесен только за несколько дней. На распространение по всему миру червей Slammer, Blaster и MyDoom потребовалось несколько минут. Теперь понятно, что центрам обработки данных нужна такая защита, которая обеспечивала бы предотвращение успешной реализации совершенно новых атак, в которых используются пока неизвестные широкому кругу специалистов уязвимости (так называемые, атаки типа "0 day").

Угрозы изнутри предприятия могут характеризоваться даже более разрушительными последствиями, так как в этом случае злоумышленникам доступна подробная информация об организации, и они могут непреднамеренно или умышленно нанести предприятию серьезный материальный ущерб. В число злоумышленников могут входить сотрудники предприятия, временные работники и консультанты. Для обеспечения надежной защиты приложений администраторам ЦОД следует использовать современные технологии, позволяющие предоставлять пользователям доступ только к тем ресурсами, которые действительно необходимы для выполнения должностных обязанностей.

Важно, чтобы специалисты по обеспечению безопасности и сетевые администраторы сообща прорабатывали конкретные уязвимости и угрозы нарушения безопасности ресурсов ЦОД, только так они смогут разработать надежную архитектуру обеспечения сетевой безопасности. Уязвимости и угрозы могут усложнять доступ пользователей к критически важным приложениям, нарушать работу приложений либо приводить к раскрытию конфиденциальной или ценной информации. Среди сетевых угроз можно выделить следующие:

- Атаки на критически важные приложения, сервера приложений, базы данных, сервера баз данных и ресурсы хранилища данных, с использованием переполнения буфера приложений, вредоносных червей, вирусов и методов несанкционированного получения прав администратора.
- Использование уязвимостей, вызванных ошибками в конфигурации систем и использованием некорректного или устаревшего программного обеспечения. Предотвращение таких атак – это трудоемкий процесс, заставляющий ИТ-менеджеров тратить большое количество времени на установку обновлений операционной системы и приложений, что может приводить к перебоям в работе системы и снижению производительности работы предприятия.

- Несанкционированное получение прав администратора при проведении атак на элементы и устройства сети, например, на маршрутизаторы, коммутаторы и межсетевые экраны.
- Угрозы нарушения безопасности сетевой инфраструктуры с помощью распределенных атак типа "отказ в обслуживании" (например, атак типа "syn flood").

ЦЕНТР ОБРАБОТКИ ДАННЫХ CISCO ДЛЯ ПРЕДПРИЯТИЙ

Концепция ЦОД Cisco для предприятий представляет единую архитектуру, обеспечивающую решение первоочередных задач ЦОД: выполнение консолидации ресурсов, обеспечение непрерывности работы и обеспечения безопасности деятельности предприятия. При этом предусмотрено использование новые технологий сервис-ориентированной сетевой архитектуры (SONA) и предоставления вычислительных ресурсов как сервиса (utility computing): использование блейд серверов, обеспечение виртуализации, активное использование Web-сервисов и механизмов распределенных вычислений (GRID). Такая архитектура ЦОД, предложенная мировым лидером в области сетевых технологий – компанией Cisco, предоставляет сетевым администраторам всеобъемлющие стратегии обеспечения безопасности на всех уровнях и решения, позволяющие предотвращать сетевые атаки на ЦОД или ограничивать их распространение. Центр обработки данных Cisco для предприятий, построенный на базе интеллектуальной сети, готов к борьбе с прямыми угрозами нарушения безопасности, кроме того, предусмотрены возможности перехода на современные сетевые системы, такие как самозащищающаяся сеть. В помощь ИТ-администраторам, занимающимся внедрением этой архитектуры, Cisco предлагает испытанные и проверенные эталонные архитектуры, проверенные принципы проектирования, а также стандартные шаблоны конфигурации и шаблоны, оптимизированные с учетом использования решений партнеров Cisco, что позволяет снизить риск, уменьшить временные и финансовые затраты. Гибкость архитектуры Cisco дает предприятию возможность внедрять те технологии коммутации, хранения данных и программного обеспечения, которые наилучшим образом соответствуют целям предприятия и предоставляют возможности по внедрению новых сервисов и приложений с большей эффективностью. Внедряя решение на базе адаптивной архитектуры сети ЦОД , ИТ-организации получают превосходный задел для решения задач управления предприятием, среди которых можно выделить обеспечение безопасности работы, оптимизацию бизнес-процессов и расширение сферы деятельности. Архитектура ЦОД Cisco для предприятий предлагает средства для защиты важных приложений и конфиденциальных данных, позволяет повысить эффективность работы центра обработки данных и быстро создавать новые безопасные среды для работы приложений, обеспечивающих поддержку новых производственных процессов. Используя отказоустойчивый эффективный ЦОД на базе адаптивной сети, предприятия могут перераспределять свои ресурсы, выделенные на развитие организации, адекватно реагируя на действия конкурентов, расширяя рынок своих сервисов, а также ускорения процесс разработки новых сервисов.

В архитектуре ЦОД Cisco для предприятий предусмотрены три уровня (см. рис. 1):

- УРОВЕНЬ БАЗОВОЙ ИНФРАСТРУКТУРЫ включает инфраструктуру IP-сети, современные средства хранения данных и обеспечения доступа к ЦОД.
- УРОВЕНЬ ИНТЕЛЛЕКТУАЛЬНЫХ СЕТЕВЫХ МЕХАНИЗМОВ включает средства обеспечения безопасности, оптимизации доставки данных, управления, а также обеспечения доступности.
- УРОВЕНЬ ВСТРОЕННЫХ ПРИЛОЖЕНИЙ И СЕРВИСОВ ХРАНЕНИЯ включает средства виртуализации хранилища, тиражирования и распространения данных, а также расширенные сервисы приложений.

Рисунок 1. Интеграция средств безопасности в архитектуру ЦОД предприятия

МНОГОУРОВНЕВАЯ СТРАТЕГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЦОД

Стратегии Cisco по обеспечению безопасности ЦОД разработаны с учетом того факта, что обеспечение безопасности является непрерывным процессом, который должен быть интегрирован с работой ЦОД, понятен сообществу пользователей и принят им, а также встроен в культуру производства и способ ведения деятельности, принятые в организации. В эффективных стратегиях обеспечения безопасности используется концепция "обеспечения безопасности на всех уровнях" с учетом различных уровней и введением дополнительных функций, что позволяет снизить риск нарушения безопасности в масштабе всего ЦОД.

Любая стратегия обеспечения безопасности начинается с выбора политики безопасности, в которой учитываются требования производственного процесса и задачи обеспечения безопасности, а также определяются процессы и средства для решения этих задач. Одна из составляющих такой политики безопасности должна учитывать специфические требования к обеспечению безопасности ЦОД, особенности приложений ЦОД, а также описывать процедуру аутентификации групп пользователей и правила разграничения доступа для каждого приложения. Эффективная политика безопасности может быть создана только в результате сотрудничества всех сторон, заинтересованных в работе ЦОД, т.е. команд менеджеров ЦОД, совета директоров, а также групп пользователей во всех подразделениях организации. Политика задает архитектуру безопасности, процессы управления, а также технологии, позволяющие реализовать внедрение и обеспечение выполнения политики безопасности, причем такая политика не является установленной раз и навсегда без возможности модификации. Корректное введение политики безопасности подразумевает регулярное уточнение и доработку политики при изменении ситуации в сфере безопасности.

Оценка текущей ситуации в области обеспечения безопасности может помочь выявить конкретные уязвимости и риски в существующей системе, а также дать рекомендации относительно того, как их уменьшить. Эти рекомендации следует включить в политику безопасности и неуклонно обеспечивать их выполнение. Сеть является средством, которое обеспечивает взаимодействие приложений и пользователей, на этом основании она является важным компонентом системы обеспечения безопасности. Сеть должна обеспечивать защиту системы на первом рубеже и дополнять средства обеспечения безопасности, предусмотренные на уровне операционной системы и на уровне приложений. Сеть используется для обеспечения безопасной рабочей среды не только на периметре, но также в зонах безопасности в самом ЦОД. Разделение сети на виртуальные сегменты позволяет администраторам безопасности эффективно консолидировать ресурсы и обеспечивать разграничение доступа пользователей приложениям.

Безопасность обмена данными в рамках всего центра обработки данных Cisco для предприятий, его производительность и надежность функционирования средств управления обеспечиваются за счет

интеграции средств обеспечения безопасности непосредственно в инфраструктуру сети. Для достижения поставленной цели используются расширенные возможности интегрированных средств обеспечения безопасности коммутаторов Cisco Catalyst® и платформ для построения интеллектуальных сетевых хранилищ данных Cisco MDS. Интегрированные программные модули для обеспечения безопасности и сервисные модули коммутаторов Cisco Catalyst серии 6500 позволяют реализовывать на их базе межсетевой экран и систему обнаружения вторжений, выполнять обмен данными по протоколу SSL и предоставлять сервисы IPSec VPN с высоким уровнем производительности. Это необходимо для сетей ЦОД, которые предъявляют повышенные требованиями к пропускной способности сети. В сети хранения данных коммутатор класса "директор" Cisco MDS 9000 Series предлагает сервисы организации виртуальных сетей хранения данных (VSAN) и расширенные сервисы безопасности.

Для дополнения этих интегрированных средств обеспечения безопасности могут использоваться разнообразные технологии обеспечения безопасности, которые можно разбить на следующие категории:

- *Защита от угроз.* Технологии предназначены для отслеживания подозрительного поведения сетевых объектов; примерами могут послужить межсетевые экраны и системы обнаружения/предотвращения вторжений (IDS/IPS);
- *Управление доверительными отношениями и проведение идентификации.* Технологии предназначены для предоставления или предотвращения доступа к сервисам со стороны устройств и пользователей и действуют на основании политик; примерами могут послужить серверы контроля доступа RADIUS;
- *Обеспечение безопасного взаимодействия*. Технологии предназначены для обеспечения конфиденциальности каналов передачи информации; примером может послужить виртуальная частная сеть, в которой используются средства шифрования.

Более подробную информацию об этих решениях см. в параграфе "*Решения Cisco для обеспечения безопасности*" ниже.

ПРЕИМУЩЕСТВА ДЛЯ ПРЕДПРИЯТИЯ

Стратегия Cisco по обеспечению безопасности ЦОД предоставляет предприятиям следующие преимущества:

- *Защита на всех уровнях*. Снижает известные и неизвестные риски и предотвращает реализацию угроз на многих уровнях;
- *Безопасная консолидация.* Разделение консолидированной инфраструктуры на зоны безопасности позволяет ограничить зону распространения сетевой атаки и позволяет использовать развитые средства контроля и разграничения доступа;
- *Снижение риска успешного проведения атак на "неизвестные уязвимости" (0-day)*. Обеспечивает путем обнаружения и блокирования подозрительного поведения объектов сети;
- *Повышение степени целостности сервисов.* Средства обеспечения целостности информации выполняют защиту и проверку правильности конфиденциальных данных на серверах и в системах хранения данных;
- *Более простые средства управления, меньшая стоимость владения*. Средства централизованного управления позволяют автоматизировать процессы конфигурирования и мониторинга, эффективно выполнять внедрение новых технологий, а также обеспечивать выполнение политик безопасности в пределах всего центра обработки данных;
- *Гибкость.* Быстрая адаптация к новым угрозам;
- *Снижение капиталовложений.* Достигается за счет консолидации и виртуализации функций обеспечения безопасности на меньшем количестве физических устройств.

АРХИТЕКТУРА БЕЗОПАСНОСТИ

Для обеспечения безопасности ЦОД необходимо, чтобы представителя высшего руководящего звена провели экономическую оценку задач обеспечения безопасности и выделили набор приоритетных задач. Располагая четко сформулированной политикой безопасности, администраторы безопасности совместно с администраторами ЦОД и сетевыми администраторами смогут разработать архитектуру безопасности, обеспечивающую надежную защиту консолидированного ЦОД.

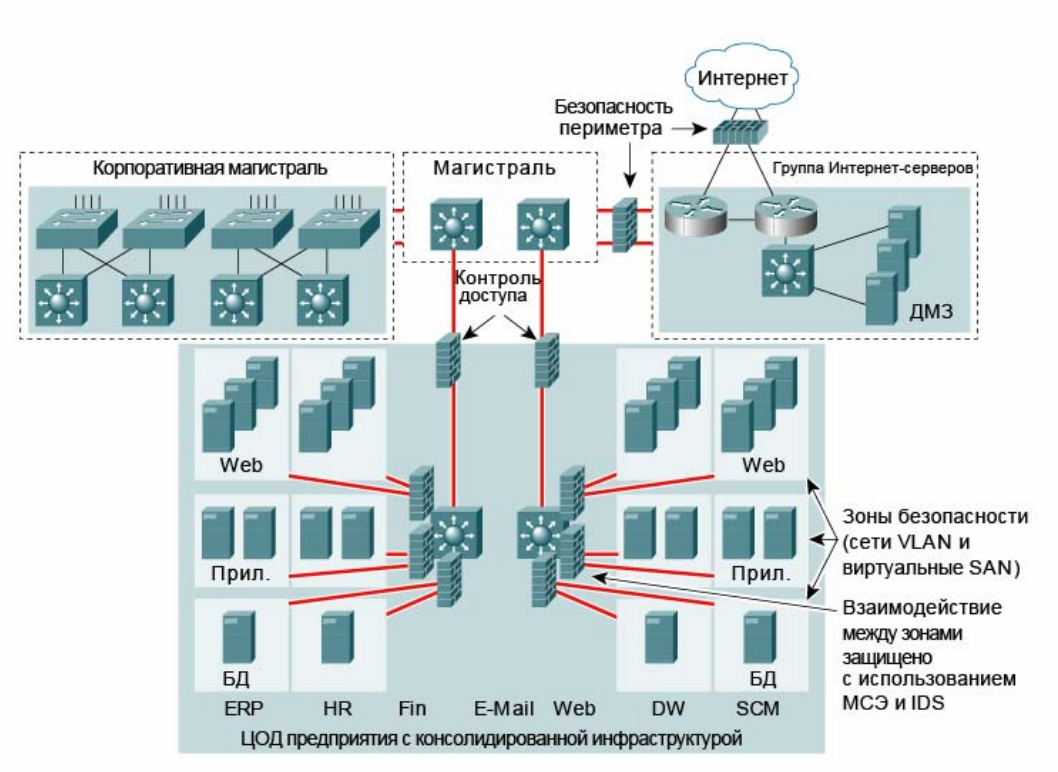
Для разработки оптимальной архитектуры ЦОД с интегрированными сервисными модулями для обеспечения безопасности Cisco рекомендует администраторам ЦОД реализовать специальный уровень "сервисов", функционирующий между уровнями доступа и опорной сети. Такой подход позволяет обеспечить наиболее эффективную и производительную работу распределенных сервисов обеспечения безопасности.

Реализация системы обеспечения безопасности ЦОД

После создания политики безопасности, в которой цели предприятия сопоставлены задачам по защите ресурсов, Cisco рекомендует администраторам безопасности предпринять следующие шаги по обеспечению безопасности ЦОД:

- *Определить зоны безопасности и установить для каждой из них уровни безопасности*. На этом этапе обеспечивается логическое разделение ЦОД на отдельные области, что позволяет свести ущерб от атак к минимуму. Понятие "зона" может означать отдельные приложения, отдельные уровни приложений, группы серверов, серверы баз данных, web-серверы, зоны электронной коммерции, а также ресурсы хранилища (см. рис. 2). Для защиты уровня приложений и уровня баз данных от случайного или намеренного повреждения информации доступ пользователей может быть ограничен доступом к web-серверам. Взаимодействие между приложениями может быть ограничено трафиком одного определенного типа, необходимого для интеграции приложений, объединения хранилищ баз данных и web-сервисов. Зоны могут обеспечивать логическое разделение среды хранилища для каждого приложения в рамках масштабируемой консолидированной сети хранилища данных. Для более эффективного функционирования такой структуры в нее можно включить виртуальные межсетевые экраны, обеспечивающие безопасность взаимодействия приложений и серверов (см. рис. 2).

Рисунок 2. Зоны безопасности с интегрированными виртуальными межсетевыми экранами обеспечивают защиту приложений в консолидированной инфраструктуре



- Провести оценку текущей ситуации в сфере безопасности для выявления уязвимостей и рисков нарушения безопасности с возможностью детализации по хостам, операционным системам, приложениям, видам данных, сетевым устройствам и каналам связи. Результаты такой оценки помогут определить соответствующие уровни риска для каждого из ресурсов, а также требования к техническому обслуживанию для обеспечения заданного уровня безопасности. Требования проведения такой оценки должно присутствовать в политике безопасности.

- Реализовать защиту оконечных устройств, таких как критически важные серверы и хосты. Функциональные возможности средств обеспечения безопасности позволяют обнаруживать попытки атак, защищать операционные системы и приложения, а также направлять сигналы тревоги на консоль управления при обнаружении попытки использования какой-либо уязвимости. Решение Cisco Security Agent, предназначенное для защиты оконечного устройства путем анализа и контроля поведения устройства, успешно предотвращало распространение червей Slammer и Blaster.

- Внедрить сетевую систему обнаружения вторжений (NIDS) для важных сетевых сегментов, для проведения анализа трафика с целью выявления и пресечения таких сетевых атак, как распределенные атаки типа "отказ в обслуживании" (DDoS), а также других действий злоумышленников. Система направляет извещения на консоль управления и/или в автоматическом режиме использует меры противодействия атакам, заложенные в сетевую инфраструктуру, и выполняет "перенаправление" или блокирование атак по мере их обнаружения. Система обнаружения вторжений (IDS) также может динамически изменять конфигурацию межсетевых экранов и маршрутизаторов для блокировки передачи пакетов от выявленных источников атаки, что позволяет уменьшить объем работ по отражению атаки.
- Ввести контроль межзонального доступа с использованием межсетевых экранов и маршрутизаторов. Межсетевые экраны обеспечивают контроль периметра путем контроля состояния входящих и исходящих соединений с ЦОД, а также блокируют доступ к внутренним сервисам и хостам с использованием фильтров входящего и исходящего трафика. Сегментация между зонами на уровне 3, маршрутизация между виртуальными локальными сетями, ограничение пропускной способности и анализ трафика обеспечиваются средствами маршрутизаторов.
- Установить ограничения доступа, путем внедрения VLAN на уровне маршрутизаторов. В условиях, когда каждый хост или сегмент работает в своей виртуальной локальной сети, администраторы безопасности могут помещать атаки "в карантин" и предотвращать их распространение на другие хосты; хосты внутри каждой из виртуальных локальных сетей могут обмениваться данными только со шлюзом по умолчанию и не могут обмениваться данными с другими хостами. Функции обеспечения безопасности, интегрированные в коммутатор Cisco Catalyst, обеспечивают комплексную защиту от попыток злоумышленников получить несанкционированный доступ к виртуальным локальным сетям путем подмены адреса отправителя пакета.
- Обеспечить безопасность сети хранилища данных. Традиционные хранилища данных считались безопасными в силу того, что являлись специализированным расширением тех компьютерных систем, к которым подключались. По мере того, как специализированные хранилища и небольшие сети хранения данных консолидируются в более крупные сети хранения данных, администраторы хранилища данных больше не могут полагаться на безопасность за счет изоляции: если сети хранилища данных простираются за пределы среды ЦОД, необходимо позаботиться об обеспечении безопасности в масштабах городских и глобальных сетей. Администратор должен рассматривать четыре аспекта защиты сети хранения данных:
  - Защита сети хранения данных от внешних угроз, таких как атаки злоумышленников;
  - Защита сети хранения данных от внутренних угроз, таких как несанкционированный доступ сотрудников или доступ с использованием взломанных устройств;
  - Защита сети хранения данных от непреднамеренных угроз нарушения безопасности со стороны авторизованных пользователей, таких как неправильная конфигурация или ошибка пользователя;
  - Защита и изоляция среды каждого хранилища данных от других, даже если они находятся в пределах одной физической сети.
- Внедрить сервисы управления доверительными отношениями и проведения идентификации, чтобы предоставлять доступ к ресурсам ЦОД только авторизованным пользователям и администраторам.
- Внедрить средства эффективного управления и мониторинга для обеспечения централизованного задания политик, выполнения мониторинга, а также для поиска и устранения неисправностей компонентов системы обеспечения безопасности и функций программного обеспечения Cisco IOS®. В это решение должны также входить средства мониторинга и проведения корреляционного анализа событий, позволяющие фильтровать извещения, которые направляются на консоль управления. Наибольшая безопасность взаимодействия с сетевыми устройствами ЦОД обеспечивается при использовании выделенной физически сети или отдельной VLAN для администрирования. Для защиты трафика системы управления Cisco рекомендует использовать протокол SSL, протокол SNMP версии 3 или средства SSH.

РЕШЕНИЯ CISCO ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Решения Cisco для обеспечения безопасности реализуют системный подход к обеспечению безопасности ЦОД предприятия и предназначены для защиты производственных процессов и ресурсов предприятия. Cisco разделяет свои продукты для обеспечения безопасности на три категории: защита от угроз, управление доверительными отношениями и проведение идентификации, обеспечение безопасного взаимодействия. Большая часть этих функциональных возможностей реализуется с помощью программного обеспечения Cisco IOS, интегрированных сервисных модулей для обеспечения безопасности для платформы Cisco Catalyst 6500 Series, а также средств обеспечения безопасности, интегрированных в коммутаторы Cisco MDS 9000 Series. Ниже приведен выборочный список продуктов Cisco для обеспечения безопасности, наиболее подходящих для реализации системы защиты ЦОД.

Аппаратные модули безопасности для платформы Cisco Catalyst 6500 Series позволяют реализовывать необходимые дополнительные сервисы безопасности без снижения производительности сети. Интеграция расширенных сетевых сервисов предлагает значительные преимущества по сравнению с использованием нескольких независимых программно-аппаратных решений. Интеграция модулей в корпус Catalyst позволяет сэкономить место в стойке, уменьшить количество необходимых соединений и упростить процедуру внедрения. Как правило, модули характеризуются более высокой производительностью и большим количеством портов по сравнению с аналогичными дополнительными устройствами, что увеличивает возможности масштабирования. В отличие от решений на базе дополнительных устройств, интегрированные модули могут использовать встроенные интеллектуальные механизмы программного обеспечения Cisco IOS и Catalyst, например, виртуальные локальные сети и механизмы управления качеством обслуживания (QoS), что предоставляет возможности для более тесной интеграции современных сетевых сервисов и создания эффективной информационной инфраструктуры.

Защита от угроз

Решения для защиты от угроз предназначены для противодействия таким атакам на сеть и хосты, как проникновение вирусов и червей, распределенные атаки типа "отказ в обслуживании" (DDoS) и блокированиях другого вредоносного сетевого трафика. Внедрение этих решений в масштабах ЦОД позволяет изолировать и блокировать действия нарушителей информационной безопасности, несанкционированных приложений и препятствовать передаче нежелательного трафика. В числе этих продуктов:

- *Сервисный модуль межсетевого экрана (FWSM) для Cisco Catalyst 6500 Series*. Этот модуль, разработанный на основе технологии межсетевого экрана Cisco PIX®, обеспечивает безопасность, надежность и производительность. При этом модуль характеризуется лучшей для межсетевых экранов скоростью обработки данных: пропускная способность 5 Гбит/с, 100 000 соединений в секунду, поддержка до одного миллиона параллельных соединений. Возможность установки до четырех модулей FWSM в одном корпусе обеспечивает масштабируемость пропускной способности устройства до 20 Гбит/с.
- *Сервисный модуль системы обнаружения вторжений (IDSM-2) для Cisco Catalyst 6500 Series*. Решение по защите от вторжений представляет собой необходимый элемент для защиты систем предприятия от действий вредоносных Интернет-червей, атак типа "отказ в обслуживании" (DoS), а также атак на приложения электронной коммерции. Использование данное модуля позволяет избежать нарушений безопасности сети, наносящих серьезный материальный ущерб и требующих существенных трудозатрат для восстановления функциональных возможностей сети. Модуль Cisco IDSM-2 работает совместно с другими интегрированными компонентами, повышая эффективность защиты сети ЦОД от вторжений.
- *ПО Cisco Security Agent*. Это решение предназначено для защиты оконечных хостов от атак на уровне системы. В основе функционирования CSA лежит принцип анализа поведения оконечного узла, по сути это ПО выполняет функции хостовой системы обнаружения вторжений.

Управление доверительными отношениями и проведение идентификации

Эти решения позволяют предоставлять доступ к сетевым сервисам и ресурсам ЦОД только авторизованным пользователям, администраторам и приложениям. Некоторые примеры таких решений:

- *Встроенные средства программного обеспечения Cisco IOS*. ПО Cisco IOS предоставляет богатый набор функциональных возможностей, обеспечивающих контроль доступа, а также другие функции обеспечения безопасности.
- *Сервер системы разграничения и контроля доступа Cisco Secure Access Control Server (ACS)*. Это решение обеспечивает централизованное администрирование процессов аутентификации, авторизации пользователей и учета их действий (AAA). Сервер ACS также позволяет выполнять централизованное администрирование решения Cisco NAC, обеспечивающего разграничение и контроль доступа к сети.

- *Решение для разграничения и контроля доступа к сети Cisco Network Admission Control (NAC)*. Решение Cisco NAC значительно расширяет возможности Cisco Security Agent по противодействию вирусам и червям, использующим пока неизвестные широкому кругу специалистов уязвимости (атаки типа "0 day"). Решение NAC, поступившее в продажу в середине 2004 года, дает предприятиям возможность определять установленные на устройстве пользователя обновления и последние исправления операционной системы, а также антивирусные средства, и переконфигурировать несовместимые или потенциально уязвимые системы для работы в среде с ограниченным или отсутствующим доступом к сети. Несовместимым оконечным устройствам может быть отказано в доступе, их могут перевести "в карантин" или же им могут быть предоставлены ограниченные права доступа к вычислительным ресурсам, для того чтобы пользователь мог провести обновление системы и установить исправления, обеспечивающие выполнение требований политики.

Обеспечение безопасного взаимодействия

Эти решения предназначены для обеспечения безопасности подключений пользователей к ЦОД и взаимодействия между ЦОД. Целостность и конфиденциальность данных обеспечивается за счет использования виртуальных частных сетей, соответствующих принятым стандартам, а также с помощью средств шифрования данных. Такие решение могут применяться для обеспечения взаимодействия нескольких ЦОД по волоконно-оптическому соединению или для взаимодействия с хранилищами данных, находящимися за пределами ЦОД. Среди продуктов, предназначенных для обеспечения безопасного взаимодействия, можно выделить:

- *Сервисный модуль SSL для Cisco Catalyst 6500 Series*. Этот модуль значительно повышает производительность и безопасность функционирования Интернет-приложений, обеспечивая безопасную передачу данных по сети. Его функционирование незаметно для пользователей.
- *Сервисный модуль Cisco IPSec VPN*. Высокоскоростной модуль для коммутаторов Cisco Catalyst 6500 Series, интегрирующий сервисы IPSec VPN в инфраструктуру. Данное решение позволяет решить задачу безопасного высокоскоростного взаимодействия ЦОД.
- *Виртуальные сети хранения данных (VSAN)*. Виртуальная сеть хранения данных похожа на виртуальную частную сеть, и также позволяет создавать несколько логических сетей хранения данных в общей физической инфраструктуре. В рамках каждой виртуальной сети хранения данных используется своя структура коммутации, что обеспечивает абсолютную изоляцию виртуальных структур коммутации. Это лишь одна из функций обеспечения безопасности, заложенных в коммутатор Cisco MDS 9000 Series.

Система управления безопасностью ЦОД

Управление безопасностью необходимо для выявления и блокирования нарушений политики прежде, чем возникнет реальный ущерб. Не представляется возможным измерить ни ценность доверия, которое испытывает пользователь к ресурсам ЦОД, ни стоимость ущерба, нанесенного организации в том случае, когда из-за нарушения безопасности нарушается целостность данных или останавливается работа приложений и серверов. Системы управления безопасностью ЦОД должны удовлетворять высочайшим стандартам простоты использования, степени автоматизации, качеству обработки данных, а также скорости и адекватности реакции.

Важным фактором обеспечения безопасности является конфигурирование, в ходе которого задаются правила обнаружения возможных вторжений, реакции на них, а также способы устранения уязвимостей. Система управления изменениями должна быть простой и должна предоставлять администраторам безопасности автоматизированные инструментальные средства обновления конфигурации устройств, выполняющих обнаружение угроз. Основным инструментом системы управления безопасностью является мониторинг, и администраторам необходимы инструментальные средства для обработки больших объемов данных, полученных от компонентов системы обеспечения безопасности, а также средства выявления подозрительной активности и упреждающего реагирования на угрозы. Для обеспечения эффективной совместной работы компонентов системы безопасности на разных уровнях требуется эффективный процесс поиска и устранения неполадок.

Система Cisco Security Management Suite ускоряет и упрощает процесс управления, а также корректирует возможные ошибки оператора, предлагая ролевую модель управления безопасностью, средства автоматизации процесса работы, а также возможности виртуализации внедряемых сервисов. Программный интерфейс Cisco Security Management Suite соответствует принятым стандартам и предлагает возможности интеграции с системами управления, разработанными сторонними производителями.

Cisco Security Management Suite предлагает администраторам ЦОД два мощных программных приложения для управления безопасностью:

- Решение для управления виртуальными частными сетями/комплексного управления безопасностью Cisco Security Manager представляет собой инструментальное средство с Web-интерфейсом, предназначенным для конфигурирования, мониторинга, поиска и устранения неполадок виртуальных частных сетей, межсетевых экранов, сетевых систем обнаружения вторжений. Решение Cisco Security Manager также предоставляет средства для инвентаризации сетевых устройств, распространения программного обеспечения и проведения аудита изменений.

- Решение для управления информацией, относящейся к обеспечению безопасности, Cisco MARS, осуществляет сбор, анализ и корреляционный анализ данных о событиях, зарегистрированных в системе обеспечения безопасности всего предприятии. Результаты анализа позволяют администраторам обнаруживать подозрительный трафик и принимать соответствующие меры. Решение Cisco MARS, предлагает средства комплексного мониторинга событий при использовании систем обеспечения безопасности многих поставщиков, а также средства корреляционного событий в режиме реального времени для обнаружения известных и неизвестных угроз, расширенные возможности визуализации для быстрого и понятного мониторинга системы безопасности, интегрированные средства оценки риска, позволяющие проводить оценку общей уязвимости любого конкретного ресурса предприятия, а также комплексные возможности составления отчетов по действиям службы безопасности на всех уровнях.
- Система управления устройствами CiscoView для коммутаторов Cisco Catalyst 6500 Series устанавливается в коммутатор и управляет некоторыми функциональными возможностями одного коммутатора на уровнях 2/3/4. Система управления CiscoView, функционирующая по принципу обработки задач, предлагает шаблоны конфигурации, составленные на основе рекомендованных внедрений, и упрощает первоначальную настройку и внедрение сервисов для всех модулей коммутатора.

СОТРУДНИЧЕСТВО В ОБЛАСТИ БЕЗОПАСНОСТИ

Сетевые решения Cisco для ЦОД являются отличным фундаментом, позволяющим предприятиям преобразовывать свои центры обработки данных в стратегические активы. Интеллектуальные сетевые технологии и технологии хранения данных Cisco позволяют ведущим поставщикам центров обработки данных строить на них свои решения. Сотрудничество Cisco с ведущими компаниями позволяет Cisco предоставлять своим клиентам простую, эффективную, интегрированную и безопасную инфраструктуру ЦОД, которая может быть легко изменена в соответствии с потребностями конкретного предприятия и легко модифицируется по мере расширения и изменения производственного процесса предприятия. Такое сотрудничество предоставляет в распоряжение администраторов ЦОД необходимые ресурсы для проектирования, внедрения и обслуживания гибких и безопасных центров обработки данных, оптимизированных для работы в соответствии с целями и задачами компаний.

CISCO – ПРИЗНАННЫЙ ЛИДЕР В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Центр обработки данных содержит данные, приложения и другие ресурсы, необходимые для производственной деятельности, и является основным функциональным узлом корпоративной сети. Для достижения успеха в работе любой организации необходимо обеспечивать постоянную защиту и непрерывную доступность этих ресурсов. Клиенты, партнеры и сотрудники компании должны быть уверены в том, что конфиденциальная информация не попадет в посторонние руки и не будет утрачена. Задачи обеспечения целостности сети и подключенных к ней ресурсов имеют огромное значение.

Cisco, признанный лидер в области сетевых технологий и технологий обеспечения безопасности, предлагает решения для обеспечения безопасности ЦОД крупного предприятия на базе своей архитектуры ЦОД для предприятий. В предложение входят руководства по проектированию и сборник "лучших решений", описанных в материалах Cisco SDN. Cisco и партнеры компании также предлагают широкий спектр профессиональных услуг по обеспечению безопасности, помогающих заказчикам определить свои требования к системам обеспечения безопасности и предпринять соответствующие меры. Решения Cisco в области обеспечения безопасности обеспечивают эффективную защиту и оптимизацию функционирования центров обработки данных без ущерба для масштабируемости и производительности. Интегрированные многоуровневые решения Cisco помогают защищать центры обработки данных от все более разрушительных и быстро распространяющихся сетевых атак, исходящих как из внутренней сети предприятия, так и из внешней сети.

Доверьте Cisco защиту наиболее ценного ресурса вашего предприятия – вашего центра обработки данных.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Решения Cisco для ЦОД:

http://www.cisco.com/go/datacenter

Инструкции Cisco по проектированию ЦОД:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns224/ns376/networking_solutions_package.html

Проекты SDN:

http://www.cisco.com/go/sdn

Управление безопасностью:

http://www.cisco.com/en/US/netsol/ns647/networking_solutions_package.html

Идентификация и контроль доступа:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

Конфигурирование и мониторинг:

http://www.cisco.com/en/US/products/ps6498/index.html

http://www.cisco.com/en/US/products/ps6241/index.html

Программа партнерства Cisco AVVID (архитектура для голоса, видео и интегрированных данных) для поставщиков продуктов и услуг в сфере безопасности:

http://www.cisco.com/en/US/partners/pr46/pr13/partners_program_solution09186a00800a3370.html

Расширенные сервисы в сфере обеспечения сетевой безопасности:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns 171 /ns267/networking_solutions_package.html

Cisco Systems
Россия, 115054, Москва,
бизнес-центр
«Риверсайд Тауерс»
Космодамианская наб., 52,
стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco Systems
Россия, 191186,
Санкт-Петербург,
бизнес-центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17,
Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099,
Алматы,
бизнес-центр «Самал 2»
Ул. О. Жолдасбекова, 97,
блок А2, этаж 14
Тел.: + 7 (3272) 58 46 58
Факс: + 7 (3272) 58 46 60
www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004, Киев,
бизнес-центр
«Горайзон Тауерс»
Ул. Шовковична, 42-44,
этаж 9
Тел.: + 7 (38044) 490 36 00
Факс: + 7 (38044) 490 56 66
www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel •Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe