Три необходимых компонента для обеспечения безопасности при осуществлении преобразования ЦОД

Официальный документ

Краткий обзор

Центры обработки данных играют важнейшую роль в развитии бизнеса. Актуальной тенденцией сегодня является перенос все большей части «традиционной» вычислительной нагрузки ЦОД в виртуализированные среды и среды облачных вычислений. Чтобы инновации не нарушали безопасность ЦОД, необходима специальная тактика планирования и дополнительные элементы управления.

Безопасность должна быть адаптивной, защищать границы при разделении физических и виртуальных ресурсов, обнаруживать проблемы и применять политики. Комплексные политики безопасности должны быть привязаны к конкретной вычислительной нагрузке, которая возникает в данный момент – например, при переносе архива данных в облако. Кроме того, соответствие нормативным требованиям должно подтверждаться отчетами, удобными для аудиторов.

При виртуализации центров обработки данных и использовании преимуществ технологий облачных вычислений, руководители высшего звена и сотрудники ЦОД получают возможность превращения безопасности в управляемый элемент, полностью интегрируемый в инфраструктуру коммуникаций ЦОД. Это уникальные особенности архитектуры и возможности, которые обеспечивает Cisco. Платформы Cisco предусматривают интеграцию функций безопасности на стадии проектирования, а не добавление этих функций, как дополнительных компонентов после внедрения. Архитектура безопасности Cisco устраняет общеизвестный компромисс между потребностями бизнеса и обеспечением безопасности.

Чтобы инновации не нарушали безопасность ЦОД и обеспечивали быстрое развитие бизнеса, ИТ-подразделениям необходимо:

1. Предусмотреть согласованную реализацию политик безопасности в физической, виртуальной и облачной инфраструктурах для поддержки непредсказуемых и быстро меняющихся бизнес-требований
2. Реализовать контекстно-зависимые механизмы управления безопасностью, согласующиеся с потребностями бизнеса, для полноценной поддержки интерактивных и сложных способов обработки информации.
3. Внедрить эффективную защиту прикладных сред для поддержки бизнеса при переходе на новые сервисы с расширенными возможностями.

> «Наши клиенты ставят безопасность на первое место. «Продолжая свое развитие, мы будем встраивать элементы безопасности в каждую микросхему ASIC, каждый продукт, каждую программную функцию, объединяя все это так, как не может никто другой».
>
> – Джон Чемберс (John Chambers), председатель правления и генеральный директор Cisco

Рис. 1. Три обязательные составляющие, обеспечивающие безопасность при внедрении инноваций в быстро изменяющейся инфраструктуре.

Почему поддержка важнейших потребностей бизнеса требует совершенствования систем безопасности

Согласно Cisco Global Cloud Index (Индекс глобальных облачных вычислений) (2011-2016)[1], к 2016 году на облачный трафик будет приходиться около двух третей трафика ЦОД.

Кроме того, результаты исследований, проведенных компанией Enterprise Strategy Group (ESG)[2] позволяют прогнозировать стремительный процесс виртуализации серверов и более полную консолидацию центров обработки данных, ведущую к росту количества пользователей. Организации больше не занимаются виртуализацией ради удобства обработки повседневной информации; теперь фокус смещен в сторону критических для бизнеса вычислений с целью повышения эффективности самых важных бизнес-приложений.

При стандартных подходах к обеспечению безопасности возникают проблемы, препятствующие быстрому переходу к новым технологиям.

- Поскольку виртуализованные приложения не привязаны к физическим вычислительным ресурсам, традиционные подходы к обеспечению безопасности могут приводить к образованию не согласованных сетевых политик, неконтролируемых областей, пробелов в системе безопасности и узких мест при передаче трафика.
- Облачные вычисления строятся вокруг совместно используемых и виртуализированных ресурсов. В результате приходится иметь дело не только с проблемами, возникающими при виртуализации, но и с дополнительными рисками, связанными с организацией облака, наличием независимого персонала и большого количества различных клиентов, которые совместно используют виртуализированные физические ресурсы.

В силу этих причин многие ИТ команды предпочитают гибридный подход. Так организация предоставляет и управляет большинством своих ресурсов - набора физических, виртуальных и частных облачных вычислительных мощностей. При этом используются и другие, внешние ресурсы, вносящие минимальный риск с точки зрения безопасности, в том числе общедоступные облака.

[1] Cisco Global Cloud Index (2011-2016)
[2] «Изменения среды ЦОД в 2012 г. откроют дверь таким технологиям как архитектуры коммутации, SDN и OpenFlow», – Джон Олтсик (Jon Oltsik), Network World, Data Center Networking Discontinuity, январь 2012 г.

Стратегический и архитектурный подходы к безопасности

Cisco помогает клиентам подготовиться ко внедрению ЦОД любого типа – физического, виртуального или гибридного.

Cisco реализует уникальный подход к обеспечению безопасности, используя свои основные сильные стороны при создании инфраструктуры, сетей и систем безопасности. Безопасность – это программируемый элемент, который использует преимущества соответствующей сетевой инфраструктуры, распространяется на устройства различного типа и присутствует в разных точках сети. Такой подход позволяет ускорить принятие решений, связанных с обеспечением безопасности, и обслуживать потребности бизнеса без введения задержки при передаче данных[3]. Безопасность также можно рассматривать как объединяющий фактор, который обеспечивает бесперебойную передачу потоков доверенной информации от оконечного устройства к серверу и от пользователя к приложению. Такой подход резко отличается от того, что некоторые аналитики называют сетевыми возможностями периода динозавров[4]; отличается он и от использования разрозненных функций обеспечения безопасности, которые обычно присутствуют в платформах других сетевых разработчиков.

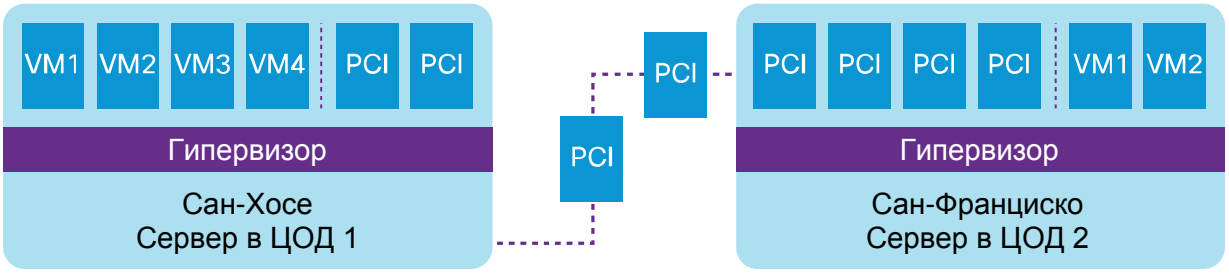
Необходимый компонент № 1: Обеспечение безопасности согласуемое с задачами бизнеса

Значительный технологический прогресс привел к повышению производительности центров обработки данных и позволил лучше адаптировать их к потребностям бизнеса. Увеличение быстродействия и конвергенция, рост плотности портов обеспечили новый уровень производительности транспортной инфраструктуры ЦОД. Уходят в прошлое отдельные друг от друга вычислительные операции в сети, в системе хранения данных и на сервере. Аналогичный подход необходим и в области обеспечения безопасности, что позволит легко перевести ЦОД на гибридную модель, охватывающую физическую, виртуальную и облачную среду.

Подход Cisco к целостному обеспечению безопасности во всех средах – физической, виртуальной и облачной – позволяет получить следующие основные бизнес-преимущества

- **Централизованная политика безопасности ведет к повышению автоматизации:** набор политик, построенных на использовании шаблонов и типовых механизмов внедрения, ускоряет решение ИТ-задач. При этом виртуализированные и облачные задачи становятся частью модели самообслуживания для бизнеса.
- **Целостное обеспечение безопасности позволяет получить максимальную отдачу от облачных вычислений:** атрибуты централизованной политики безопасности, примененные к шаблонам, обеспечивают быстрое выделение и масштабирование виртуальных машин. Так устраняются возможные нарушения нормативных требований, как, например, совместная обработка различных классов данных.
- **Динамическое определение зон безопасности предоставляет более высокую гибкость:** зоны безопасности, основанные на динамических политиках, отражающих атрибуты безопасности виртуальных машин, и другие значимые атрибуты безопасности (в отличие, например, от статических IP-атрибутов), позволяют лучше разграничить физические и виртуальные ресурсы. С помощью зон безопасности обеспечивается гибкий перенос рабочей нагрузки между физической, виртуальной и облачной инфраструктурами. Создавая возможность реализации безопасных многоклиентских сред.

Рис. 2. Динамические зоны безопасности обеспечивают более высокую гибкость. Например, безопасный перенос виртуальной нагрузки.



[3] The Future of Network Security: Cisco's SecureX Architecture (Будущее сетевой безопасности: архитектура SecureX Architecture Cisco).
[4] «Изменения среды ЦОД в 2012 г. откроют дверь таким технологиям как архитектуры коммутации, SDN и OpenFlow», – Джон Олтсик (Jon Oltsik), Network World, Data Center Networking Discontinuity, январь 2012 г.

«Контекстно-зависимое адаптивное обеспечение безопасности будет единственным способом для безопасной поддержки динамического бизнеса и ИТ-инфраструктур, которые появятся в течение следующих 10 лет.»[6]

- Нейл Макдональд (Neil MacDonald), вице-президент, ведущий аналитик и заслуженный сотрудник Gartner

Необходимый компонент № 2: контекстно-зависимое управление, соответствующее сложным бизнес-потребностям

Быстро меняющиеся потребности бизнеса и увеличение количества мобильных работников заставили ИТ-специалистов изменить политики предоставления доступа пользователям и ввели новые требования по безопасности. Современным пользователям необходим доступ к приложениям и важнейшим активам в ЦОД из любого места. Это разительно отличается от статических центров обработки данных, которые существовали десять лет назад, когда доступ к ресурсам ЦОД имели только несколько доверенных лиц и когда сами ЦОД представляли собой преимущественно хранилища информации, где изредка проводились какие-то операции с данными.

Большинство специалистов и аналитиков отрасли согласны с тем, что применение контекстно-зависимой безопасности позволяет правильно идентифицировать пользователей и обеспечивает законное использование данных. Cisco использует сканирующие элементы следующего поколения для встраивания функционала контекстного анализа в сетевую инфраструктуру, что позволяет получить следующие преимущества[5].

- **Безопасный доступ для мобильных работников в любое время и из любого места:** контекстно-зависимые комбинации аутентификации, в которых присутствуют такие факторы как «кто», «где», «что» и «когда», а также более подробные характеристики позволяют принимать более интеллектуальные решения о допуске. Например, можно предотвратить потенциальную угрозу, если соотнести такие факты, что сотрудник вошел в сеть из офисного здания, но при этом он пытается получить доступ к CRM-порталу из кафе, находящегося в другом месте.
- **Безопасные операции с данными, исходя из бизнес-контекста:** используя программируемые элементы, можно динамически распространить политику безопасности на шифрование данных пользователя в зависимости от контекста. Например, данные сотрудника финансового департамента, имеющего доступ к платёжной ведомости, должны быть надежно зашифрованы.
- **Распространение политики безопасности на устройства, не требующие авторизации:** такие устройства как принтеры и камеры играют все возрастающую роль в бизнесе. Необходимо учитывать риски, связанные с ними.
- **Гибкое развертывание и множество способов обеспечения безопасности для гибридных сред:** межсетевой экран, прокси-сервер для веб-трафика, обеспечивающий антивирусную защиту, маршрутизатор и политики контроля доступа – все они работают вместе, обеспечивая безопасность пользователя. Различное конструктивное исполнение предназначено для поддержки все возрастающего количества распределенных и гибридных сред. Например, это могут быть выделенное устройство в корпоративном ЦОД, который расположен на территории компании, или модуль для маршрутизатора в филиале или приложение в облаке.

Необходимый компонент № 3: мощные возможности защиты приложений, обеспечивающие развитие новых видов бизнеса

Необходимость высокой доступности приложений продолжает создавать проблемы для ИТ-руководителей и специалистов ЦОД. Функционирование бизнеса существенно зависит от используемых веб-приложений, которые позволяют компаниям оказывать услуги пользователям, сотрудничать с партнерами и способствуют более производительной работе персонала. Состав корпоративных приложений меняется; проявляется тенденция к большему использованию инструментов бизнес-аналитики, CRM, специально созданных рабочих процессов, приложений для передачи видео и WEB-конференций. Некоторые из этих приложений могут занимать большую часть пропускной способности сети. Однако, имея множество приложений, как можно понять, какие из них безопасны, а какие связаны с рисками? При этом пользователи ожидают немедленного отклика от приложений при работе в сети. Результат - огромная нагрузка на сети с точки зрения скоростей передачи данных, надежности и безопасности.

[5] The Future of Network Security: Cisco's SecureX Architecture (Будущее сетевой безопасности: архитектура Cisco SecureX).
[6] Gartner, “The Future of Information Security Is Context Aware and Adaptive” (Будущее информационной безопасности является контекстно-зависимым и адаптивным), Нейл Макдональд (Neil MacDonald), 2012 г.

В противоположность этому, Cisco организует непрерывную доверительную цепочку, которая тянется от пользователя к приложению, и на всем ее протяжении используется интеллектуальный контекстно-зависимый анализ параметров. Приложения Cisco обеспечивают прозрачность и контроль инфраструктуры передачи данных ЦОД за счет возможностей интеллектуальной инспекции IP-пакетов на высокопроизводительном оборудовании. Такой подход имеет следующие основные преимущества:

- **Более быстрая работа для конечного пользователя:** благодаря тому, что клиентское устройство (ноутбук или одно из многих других поддерживаемых устройств) автоматически находит ближайший сканирующий элемент в структуре коммутации (например, маршрутизатор) и легко осуществляет подключение. Платформы Cisco снижают задержку в сети и сложность архитектуры, которые характерны для большинства других подходов, где трафик приложений приходится сначала направлять на другой конец света, чтобы потом он попал на межсетевой экран 3-го уровня.
- **Улучшенная прозрачность и контроль использования приложений:** интеллектуальная проверка сетевых пакетов наряду с обеспечением контекстно-зависимой безопасности гарантируют быструю классификацию приложений, что позволяет эффективно блокировать любые злонамеренные действия, связанные с приложениями.
- **Улучшенное управление пропускной способностью сети:** большое количество подключений в секунду и большое максимально возможное количество подключений позволяют ИТ-специалистам надежно структурировать потоки данных в сторону back-end серверов, что необходимо в соответствии с бизнес-требованиями. Кроме того, возможно использование текущих параметров сети для определения того, можно ли разрешить продолжение данного сеанса или следует ограничить полосу пропускания для общего повышения производительности приложений.

Направление дальнейших действий

Подход Cisco к обеспечению безопасности помогает ускорить внедрение гибридной модели ЦОД благодаря использованию проверенного дизайна и рекомендованных архитектур. Cisco предоставляет пользователям уникальную программируемую систему безопасности, которая интегрируется в инфраструктуру коммутации ЦОД на этапе разработки дизайна проекта, а не надстраивается на более поздней стадии. Клиенты получают преимущество от решений, которые обеспечивают максимальную производительность при меньшем количестве оборудования и более низких эксплуатационных затратах. Экосистема, созданная многочисленными партнерами и интеграторами, позволяет клиентам легко внедрять средства обеспечения безопасности в быстро развивающуюся инфраструктуру. В условиях, когда непрерывно появляются инновационные разработки для организации сетей и обеспечения безопасности, ИТ-руководители могут быть уверены в том, что Cisco поможет им трансформировать центры обработки данных в гибридные структуры, которые будут безопасно обслуживать будущие потребности бизнеса.

Дополнительная информация

Более подробные сведения о решениях Cisco для обеспечения безопасности ЦОД можно найти по адресу http://www.cisco.com/go/securedatacenter.

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465

Компания Cisco имеет более 200 офисов по всему миру. Адреса, номера телефонов и факсов приведены на web-сайте компании Cisco по адресу www.cisco.com/go/offices.