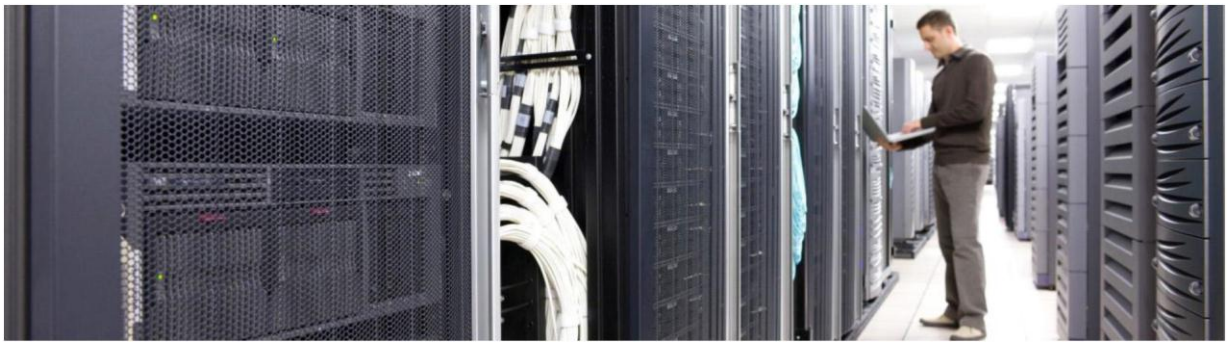
Решения Cisco для защищенного ЦОД снижают риск при переходе к частному облаку



Облачные вычисления привлекают все больше внимания, так как рассматриваются как следующий этап развития информационных технологий. Однако, при всех многочисленных преимуществах (рост гибкости, возможности масштабирования и эффективности, снижение затрат), их использование приводит к возникновению новых проблем в области безопасности. Сложность этих проблем вызвана тем, что они имеют не только технический характер, но и связаны со значительными изменениями процессов, вызванными внедрением новых моделей вычисления для бизнеса.

Многие компании не отказываются от облачных технологий и используют частные облачные среды, в которых предусматривается управление политиками и соответствие нормам, что обеспечивает защищенность ЦОД. Решения Cisco для защищенных ЦОД с использованием технологии частного облака помогают заказчикам определить эффективную стратегию и архитектуру перехода к вычислениям в частном облаке.

Характеристики и модели облаков

Национальным институтом стандартов и технологий (NIST) предложены 5 характеристик и 4 модели развертывания облачных сред.

Характеристики:

- Самообслуживание по запросу: заказчик может автоматически и самостоятельно определять для себя необходимые возможности для вычислений (время работы сервера и сетевые хранилища) без контакта с представителями провайдера.
- Объединение ресурсов: вычислительные ресурсы провайдера объединяются для обслуживания нескольких заказчиков с использованием многоклиентской модели и динамическим выделением физических и виртуальных ресурсов в соответствии с потребностями заказчиков. При этом заказчик, как правило, не определяет и не знает точное место нахождения предоставленных ресурсов, но может указать его на более высоком уровне абстракции. Возможно объединение таких ресурсов, как средства хранения и обработки данных, а также полосы пропускания сети.

- Эластичность: возможности могут быстро предоставляться и отзываться, иногда автоматически, для быстрого масштабирования в любом направлении в соответствии с запросами. Со стороны Заказчика возможности выглядят практически неограниченными, поскольку они могут быть выделены ему в любом объеме и в любое время.
- Контролируемый сервис: системы облачных вычислений автоматически управляют оптимизацией ресурсов, определяя их количественные параметры на уровне абстракции, приемлемом для типа сервиса (например, хранения и обработки данных, полосы пропускания и работы с активными учетными записями). Контроль использования ресурсов обеспечивает прозрачность их потребления и для провайдера, и для заказчика.
- Широкополосный доступ: выделение ресурсов и доступ к ним производятся по сети с использованием стандартных механизмов, помогающим равномерно использовать платформы тонких и толстых клиентов (например, мобильные телефоны, планшеты, ноутбуки и рабочие станции).

Модели развертывания облачных сред:

- Облако сообщества: общая инфраструктура для нескольких организаций, образующих определенное сообщество, с общими задачами (например, безопасность, контроль соответствия нормам, сферу полномочий). У такого облака может быть внутреннее или внешнее управление и размещение как на собственных, так и на внешних серверах.
- Общедоступное облако: его инфраструктура предоставляется провайдером для использования заказчиком любого типа. Функции владения, управления и эксплуатации такой инфраструктуры могут принадлежать коммерческим, научным или государственным организациям как отдельно, так и совместно.
- Частное облако: его инфраструктура предоставляется только одной организации. У нее может быть внутреннее или внешнее управление с размещением на внешних серверах (виртуальное частное облако). В таком облаке возможно разделение отдельных подразделений организации в форме отдельных клиентских групп. При этом провайдер владеет всей информацией о расположении ресурсов, поскольку распоряжается инфраструктурой.
- Гибридное облако: это несколько облаков разного типа, сохраняющих свою уникальность, но связанных между собой для использования преимуществ разных моделей развертывания. Такое облако может также состоять из нескольких облачных систем, соединенных между собой для свободного перемещения программ и данных между ними.

Преимущества перехода к частному облаку для бизнеса

По сравнению с традиционными ЦОД, привязанными к определенным физическим серверам, частное облако позволяет снизить затраты и улучшить гибкость, эффективность и возможности масштабирования деятельности компании. Выбирая между моделями общедоступного, гибридного или частного облака, многие склоняются к последней, поскольку она способна решить задачи обеспечения безопасности, соответствия нормам и единства политик. Результаты исследования систем облачных вычислений, проведенного CSO в 2012 г., показали, что у 23% опрошенных организаций информация хранится в частном облаке. По результатам исследования частное облако занимает первое место по популярности, а гибридное - второе (11%).[1]

[1] Bragdon, Bob, 2012 CSO Cloud Computing Study, 19 июня 2012 г., стр. 6.

У частных облаков много преимуществ: самообслуживание при выделении сервисов (на уровне не ниже, чем у внешних провайдеров), адаптация приложений и сервисов под нужды предприятия, высокий уровень безопасности и соблюдения норм (недостижимый у провайдеров общедоступных облаков) и возможность масштабирования ресурсов с их автоматическим предоставлением, что обеспечивает высокий уровень эффективности и гибкости. Такая инфраструктура также позволяет снизить затраты за счет консолидации нагрузок для оптимизации загрузки серверов без ущерба для эффективности и гибкости работы. Расчет экономической эффективности частного облака по сравнению с общедоступным показывает, что у предприятий со значительными вычислительными ресурсами снижение затрат составляет до 40% при переходе к частной облачной среде.[2]

Препятствия на пути перехода к облаку

Самым серьезным из них является безопасность. Результаты обследования CSO показывают, что 68 % компаний сомневаются в надежности защиты своих данных, размещенных в облаке. Ниже описаны основные проблемы обеспечения безопасности при переходе к облачным технологиям.

Информационная безопасность

- Многоклиентская архитектура. В то время как в небольших и распределенных центрах обработки данных размещается незначительное количество приложений и поддерживается одна организация, в современных консолидированных ЦОД и облачных средах часто работают разные группы пользователей, которым требуется полное разделение сетевого трафика и строгие политики контроля доступа, даже если их физические серверы и сетевая инфраструктура являются общими. Такие же требования применяются к частным виртуальным центрам обработки данных и частным облачным средам, в которых внутренним пользователям необходимо разделение.
- Неподвижные и подвижные данные. Перемещение приложений между серверами, удаленными ЦОД и облаками увеличивает сложность того уровня сети, который отвечает за безопасность. Обычно он работает с неподвижными ресурсами и статичными частными сетями при реализации политик безопасности. Гибкость перемещения политик безопасности в соответствии с изменением виртуальных рабочих нагрузок является сложной задачей.

Доступ к данным и приложениям

- Проверка подлинности и авторизация. В мире повышения уровня мобильности, незащищенных устройств и появления сложных угроз большая часть задач по реализации политики безопасности должна перейти из приложений в сеть. Таким образом, сетевая инфраструктура реализует значительный объем действий по аутентификации, авторизации пользователей и применению политики доступа, которые были перенесены из приложений в сеть в связи с увеличением контекстной зависимости сети. Инфраструктура сетевой безопасности все в большей степени задействуется для реализации политик идентификации и политик на основе ролей, а также для принятия других связанных с контекстом решений. Происходит изменение в механизмах политик разграничения доступа – теперь контроль потоков данных выполняется на основе анализа идентификационных данных, роли пользователя, процесса или приложения в сетевой транзакции, стандартного механизма принятия решения на базе статических атрибутов (например, IP-адресов источника и назначения пакетов и номеров портов) более не достаточно.
- Локальный и удаленный доступ. Кроме идентификационных данных, доступ также может зависеть от привязанных к контексту характеристик, включая тип устройства, обращающегося к приложению, местоположение пользователя, время запроса и многое другое. Реализацию этих контекстно-зависимых политик все чаще берут не себя межсетевой экран ЦОД и система предотвращения вторжений (IPS), которые должны расширить свои возможности с целью обнаружения и контроля трафика на основе указанных политик, а также для мониторинга наличия вредоносных программ, попыток несанкционированного доступа и распространения сложных атак. На современном предприятии выполняется множество критически важных и специализированных приложений. Данные в этих приложениях являются ценным объектом для злоумышленников, поскольку доступ к ним имеет первостепенное значение для производительности и успеха предприятия.

[2] Andi Mann, Kurt Milne and Jeanne Morain, “Calculating the Cost Advantages of Private Cloud” http://searchcloudcomputing.techtarget.com/feature/Calculating-the-cost-advantages-of-private-cloud, апрель 2011 г.

Потеря контроля и прозрачности

- Сложность системы и многокомандный подход управления. Многие компании замечают потерю прозрачности при переходе к облачным технологиям. Традиционные межсетевые экраны и системы предотвращения вторжений за пределами виртуальных зон не отслеживают трафик между виртуальными машинами. Во многих типах облаков клиенты не имеют представления обо всех базовых продуктах обеспечения безопасности, поскольку управление облачной средой осуществляется извне.
- Соответствие нормативным требованиям. Облачная инфраструктура должна соответствовать отраслевым стандартам, стандартам клиентов и нормативным требованиям. Она должна поддерживать возможности прозрачности и аудита. На таких предприятиях с высокими требованиями к соблюдению норм, как организации здравоохранения, финансовые и государственные учреждения, необходимо предусматривать возможность аудита информационных систем.
- Боясь потерять контроль и прозрачность, многие компании предпочитают перейти именно к частному облаку. Но вопросы безопасности, включая доступ к данным и приложениям, сохраняют важность и для частного облака. В решениях Cisco система безопасности является элементом всей архитектуры вычислений частного облака.

Архитектура частного облака

С точки зрения архитектуры, основными элементами частного облака являются базовая инфраструктура, разнообразные сервисы и определенные функции, например обеспечения безопасности и устойчивости. Кроме того, система обеспечения безопасности облака имеет свою архитектуру. Ряд важных соображений относительно архитектуры системы безопасности перечислен ниже.

- Логическое разделение. Важное преимущество облачных вычислений - эластичность вычислительных возможностей, т.е. их быстрое изменение в соответствии с потребностями. Для поддержки такой динамичной рабочей модели безопасность должна обеспечиваться в схожем режиме. Статичная инфраструктура обеспечения безопасности, ориентированная на физические ресурсы. Например, сетевая инфраструктура, построенная на базе технологии виртуальных локальных сетей (VLAN), требует больших трудозатрат в процессе функционирования и не способна на быструю реакцию на запросы ресурсов. Необходимы новые подходы к логическому разделению при обеспечении безопасности в динамичной среде с общими ресурсами и большим числом пользователей.
- Единство политики. Наличие всеобъемлющей системы единых политик имеет особую важность для обеспечения безопасности в облаке. Например, удачным решением для надежного динамичного логического разделения является внедрение средств защиты на основе определенных политик для разных зон. Зона описывается группой параметров, в которую могут входить IP-адрес, сетевые протоколы и номера портов. Помимо того к параметрам зоны могут относиться атрибуты виртуальной машины и другие задаваемые параметры. Такой подход обеспечивает единство политик в динамичной облачной среде, в которой виртуальные машины обычно перемещаются между физическими серверами.
- Автоматизация. Основным преимуществом облачных вычислений является быстрота и эффективность решения повторяющихся задач. Пользователи могут использовать результаты их решения ИТ-персоналом, переведя такие задачи в режим самообслуживания. Централизованная инфраструктура политики безопасности с автоматизацией запуска решения задач существенно повышает эффективность работы предприятия, переведя типовые вопросы обеспечения безопасности с административного на технический уровень.
- Возможность масштабирования и производительность. Эти функции, тесно связанные с автоматизацией, необходимы для обеспечения безопасности облачной среды из-за высокой нагруженности и жестких требований к защите данных. Инновационные технологии, способные резко повысить эффективность работы без ущерба для безопасности являются критически важным фактором при обеспечении безопасности облачной среды.
- Аутентификация и контроль доступа. Как уже говорилось, контроль доступа к частному облаку определяется контекстом, а также именем, типом устройства и местом нахождения пользователя. Средства защиты, встроенные в сетевую инфраструктуру, межсетевой экран, система

предотвращения вторжений и средства VPN - все это необходимо для контроля доступа пользователей в частную облачную среду.

Решения защищенного ЦОД Cisco для частных облачных сред

Первым из таких решений является Cisco CloudVerse - набор средств интеграции унифицированного ЦОД Cisco с интеллектуальной облачной сетью Cisco для предоставления облачных сервисов и приложений. В его основе лежат три принципа:

- Cisco предоставляет средства для разработки архитектуры, решения и интегрированные системы для создания облачной среды у заказчика
- Cisco тесно сотрудничает с партнерами высшего уровня для предоставления полностью проверенных интегрированных решений для заказчиков, внедряющих облачные сервисы
- Cisco упрощает и ускоряет использование облачных сервисов за счет возможности быстрого предложения облачных сервисов для пользователей

Решения Cisco для защищенного ЦОД ориентированы на работу в защищенной облачной среде. В их состав входят следующие средства:

- Многофункциональное устройство обеспечения безопасности Cisco ASA 5585-X или сервисный модуль ASA SM для Cisco Catalyst® серии 6500
- ПО для платформы многофункциональных устройств обеспечения безопасности Cisco ASA версии 9.0
- Выделенные сенсоры системы предотвращения вторжений Cisco IPS 4500 или блейд-модуль IPS для ASA 5585-X
- Комплекс средств обеспечения контролируемого доступа для групп безопасности Cisco TrustSec®
- ПО централизованного мониторинга и управления Cisco Security Manager 4.3
- Виртуальные коммутаторы Cisco Nexus 1000V
- Виртуальный шлюз безопасности Cisco (VSG)
- Облачный межсетевой экран Cisco ASA 1000V
- Центр управления виртуальными сетями Cisco (VNMC)

Высокопроизводительные устройства Cisco ASA 5585-X имеют уникальные возможности по обеспечению безопасности для защиты нового виртуализированного ЦОД и расширенного облака за счет использования функций межсетевого экрана и предотвращения вторжений. Развертывание устройства ASA 5585-X в облачном ЦОД на уровне распределения надежно защищает его ресурсы и серверы. Это устройство поддерживает такие современные технологии для виртуальных ЦОД, как Cisco virtual Port Channel (vPC), Cisco Virtual Switching System for Catalyst 6500 (VSS) и Virtual Device Contexts Cisco Nexus 7000 (VDC). Что обеспечивает прекрасные возможности масштабирования и эффективную работу в облачных средах. Кроме того, они поддерживают функционал логического сегментирования на контексты безопасности (ASA Security Contexts) для эффективного и безопасного логического разделения трафика всех пользователей в многопользовательской среде.

В устройстве Cisco ASA 5585-X используется решение MultiScale™, обеспечивающее быструю обработку новых. соединений, большое число одновременных сеансов, высокую пропускную способность и различные защитные сервисы для исключительной гибкости в работе. Оно может обеспечить скорость до 20 Гб/с для типового HTTP-паттерна трафика и до 35 Гб/с при передаче больших пакетов данных. Кроме того, оно обеспечивает выполнение до 350 000 подключений в секунду, поддерживая одновременно до 2 млн. подключений.

Сервисный модуль Cisco ASA имеет схожие характеристики, но в исполнении модуля для коммутаторов Catalyst 6500.

Программное обеспечение Cisco ASA версии 9.0 для платформы многофункциональных устройств безопасности ASA поддерживает устройства различных исполнений, включая широкий диапазон автономных устройств и блейд-модулей, а также программное обеспечение для защиты общедоступных и частных облаков. Эта версия ПО отличается возможностью кластеризации; интеграцией с решением Cisco Cloud Web Security (прежнее название - ScanSafe), что позволяет обеспечить детализацию контроля доступа в Интернет и реализовать политики работы с веб-приложениями с одновременной защитой от вирусов и вредоносных программ. Кроме того, поддерживается использование меток групп безопасности технологии Cisco TrustSec, что обеспечивает интеграцию средств защиты непосредственно в сеть для расширения политики, созданной на платформе ASA.

Технология доступа для групп безопасности Cisco TrustSec - это инновационное решение, классифицирующее системы и/или пользователей на основе контекста при их подключении с последующим преобразованием порядка применения политики безопасности во всей инфраструктуре ЦОД. Такая классификация использует метки групп безопасности (SGTs) для формирования решений о допуске к ресурсам ЦОД или отказе от допуска на основе интеллектуальной политики. Кроме того, эта технология автоматизирует разработку правил работы межсетевого экрана, снижая уровень сложности при организации контроля и разграничения доступа.

Cisco также предоставляет самую распространенную на рынке технологию предотвращения вторжений (IPS), предлагая сенсоры IPS или межсетевой экран ASA со встроенными сервисами IPS. Аппаратные сенсоры Cisco IPS 4500 или блейд-модуль IPS для устройства ASA 5585-X помогают обеспечить безопасность и доступность для критически важных приложений и элементов инфраструктуры ЦОД, поддерживая анализ более 100 000 одновременных подключений в секунду. Расширяемое шасси с поддержкой 10 Gigabit Ethernet малого размера (2RU) обеспечивает возможность масштабирования и защиту инвестиций без ущерба для экологической эффективности ЦОД.

Решение IPS 4500 защищает инфраструктуру и приложения от самых современных вероятных угроз (APT) и других современных атак с помощью таких передовых технологий, как выявление и анализ угроз, пассивный контроль признаков ОС, а также анализ репутации и контекста, обеспечивая высокий уровень безопасности. Благодаря поддержке центра глобального анализа угроз Cisco® SIO, решение Cisco IPS обеспечивает прозрачность на основе сотен параметров безопасности, миллионов правил обнаружения и 8 Тб данных телеметрии угроз в сутки, ежедневно предоставляемую ведущими отраслевыми почтовыми и web-клиентами, а также клиентами межсетевых экранов, устройств IPS и оконечных устройств.

Cisco Security Manager 4.3 - это комплексное решение для управления, обеспечивающее постоянное соблюдение политик, устранение проблем с безопасностью и подготовку обобщенных отчетов по объекту управления. Данное решение управляет защитной средой Cisco во всем жизненном цикле, обеспечивая прозрачность на объекте управления и совместное использование данных важными сетевыми серверами. Внедрение Cisco Security Manager повышает эффективность работы за счет использования мощного комплекса средств автоматизации. Cisco Security Manager управляет жизненным циклом следующих платформ: многофункциональные устройства обеспечения безопасности Cisco ASA серии 5500, устройства обнаружения и предотвращения вторжений Cisco IPS серии 4500, программный клиент Cisco AnyConnect™ Secure Mobility Client, а также маршрутизаторы Cisco с интегрированными функциями безопасности.

Виртуальный шлюз безопасности Cisco (VSG) работает вместе с коммутаторами Cisco Nexus 1000V, обеспечивая безопасность для различных зон с учетом политик на уровне виртуальных машин. Cisco VSG позволяет использовать существующие политики безопасности в виртуальных и облачных средах. Шлюз обеспечивает безопасное логическое разделение на уровне виртуальных машин. Поскольку он выбирает политику безопасности по типу зоны, а не по статическому IP-адресу, он обеспечивает единообразие политик безопасности даже при перемещении виртуальных машин между физическими серверами. Поддержка мобильности виртуальных машин особо важна для поддержания единообразия политик в автоматизированной облачной среде с произвольным выбором места обработки вычислительных задач.

Помимо того, шлюз Cisco VSG обеспечивает возможность аудита и прозрачность на уровне пользователей, что важно для обеспечения соответствия нормам. Устройство Cisco Nexus 1000V расширяет функции обеспечения безопасности и контроля на уровне контроля доступа за счет использования встроенных технологий безопасности: private VLANs (PVLANs), IP Source Guard, Dynamic Host Configuration Protocol (DHCP) snooping, Address Resolution Protocol (ARP) inspection, and NetFlow. Интеллектуальная технология vPath, используемая в коммутаторе Cisco Nexus 1000V, позволяет снять нагрузку с гипервизора при применении политики безопасности, увеличивая эффективность работы виртуального шлюза защиты. И, наконец, один такой шлюз может защитить несколько физических серверов. Такая гибкость существенно увеличивает возможности масштабирования облачных средств защиты Cisco, упрощая систему за счет отказа от управления виртуальными межсетевыми экранами на каждом физическом сервере.

Облачный межсетевой экран Cisco ASA 1000V вместе с виртуальным коммутатором Cisco Nexus 1000V помогает защитить виртуальные и облачные многоклиентские среды на уровне границ между клиентскими зонами. Работая как основной шлюз для системы, он обеспечивает защиту от сетевых атак. Этот экран, созданный с использованием платформы ASA, позволяет сформировать интеллектуальные границы с использованием технологий VPN для связи между объектами, преобразования сетевых адресов (NAT), протокола DHCP и инспекции протоколов. Многоклиентский ЦОД или частная облачная среда, требуют изоляции трафика приложений для различных клиентов, приложений и групп пользователей в соответствии с принятыми политиками.

Совместное использование виртуального шлюза безопасности и межсетевого экрана обеспечивает комплексную защиту частных и общедоступных облачных сред. Спроектированные для плотной интеграции с Cisco Nexus 1000V и гипервизором на уровне виртуализации, решения Cisco VSG и Cisco ASA 1000V позволяют детально контролировать выполнение политик безопасности индивидуально для виртуальных машин. В таком решении виртуальные машины создаются или перемещаются между серверами, политики безопасности для них перемещаются вместе с ними, предоставляя все сервисы безопасности автоматически. Коммутатор Cisco Nexus 1000V обеспечивает взаимодействие между виртуальным шлюзом безопасности VSG и межсетевым экраном ASA 1000V.

Виртуальные МСЭ можно создавать и использовать совместно в зависимости от потребностей для оптимизации использования ресурсов. И экран Cisco ASA 1000V, и шлюз Cisco VSG используют технологию управления трафиком vPath коммутатора Cisco Nexus 1000V для передачи трафика к нужным сетевым сервисам для реализации политик. Это позволяет таким устройствам за один шаг обеспечивать защиту виртуальных машин на различных серверах с возможностью масштабирования инфраструктуры безопасности ЦОД или облака и простого управления ей. Число шагов масштабирования этих устройств определяется по необходимости, позволяя реализовать большое число политик с учетом особенностей разных виртуальных приложений. Такая гибкая архитектура позволяет конечному пользователю оптимизировать использование ресурсов и снизить затраты.

Интегрированное решение Cisco также рассчитано на масштабирование в гетерогенных средах гипервизоров. По мере масштабирования коммутатора Cisco Nexus 1000V на разных типах гипервизоров его сервисы, включая виртуальный шлюз безопасности и межсетевой экран ASA 1000V, также масштабируются, что исключает необходимость использования отдельных решений для каждого гипервизора.

Центр управления виртуальными сетями Cisco (Virtual Network Management Center , VNMC) — это централизованная консоль управления для администрирования политик безопасности облачного межсетевого экрана Cisco ASA 1000V и виртуального шлюза безопасности Cisco VSG. Cisco VNMC - это прозрачное масштабируемое многопользовательское решение для управления объектами виртуальных и облачных сред на основе комплексных политик безопасности. Данное решение обеспечивает быстрое внедрение политик с использованием шаблонов и профилей безопасности. Оно обеспечивает повышение гибкости управления благодаря интерфейсу API XML, поддерживающему интеграцию со сторонними средствами управления.

Весь портфель средств безопасности Cisco обеспечивает комплексную защиту облачной среды за счет логического разделения, единообразия политик, автоматизации и контроля доступа. Решения Cisco помогают обеспечить безопасную работу большого числа клиентов в частных облачных средах, а также прозрачность трафика и взаимодействий. Все это помогает и заказчикам, и пользователям улучшить процессы управления этими средами.

Виртуализированный многопользовательский ЦОД Cisco, рекомендуемый дизайн

Cisco Virtualized Multiservice Data Center представляет собой проверенный комплексный дизайн для сетей нового поколения. Он использует решения защиты ЦОД Cisco для частных облачных сред, встроенные в архитектуру унифицированного ЦОД Cisco. Унифицированный ЦОД Cisco позволяет изменить экономику центра обработки данных путем объединения вычислений, систем хранений, сетей, виртуализации и управления в единую платформу на основе коммутации, предназначенную для повышения операционной эффективности, упрощения ИТ-процессов и обеспечения гибкости бизнеса. В отличие от других решений, в которых для достижения интеграции вводятся дополнительные уровни программного обеспечения по управлению, унифицированный ЦОД Cisco разработан специально для виртуализации и автоматизации, а также предоставления ресурсов по запросу из общих пулов инфраструктуры в физических и виртуальных средах, что является идеальным решением для частных облачных инфраструктур. В результате информационные технологии превращаются из центра затрат в источник сервисов, повышающих конкурентоспособность предприятия. Все это позволяет повысить уровень безопасности, надежность и предсказуемость, а также скорость развертывания систем заказчика при переходе к частным облачным средам. Проработанный комплект документации упрощает работу ИТ-персонала при проектировании и настройке систем.

Заключение

Решения Cisco для защищенного центра обработки данных для частного облака обеспечивают безопасную работу большого числа клиентов в таких средах и позволяют заказчикам контролировать сетевой трафик и работу сети с целью поддержки процессов управления в облаке. Тем, кто готов перейти на облачные вычисления, Cisco поможет сократить риски за счет единообразия формирования и реализации политик, улучшения возможностей масштабирования и роста эффективности работы. Решения для обеспечения безопасности Cisco вместе с унифицированным ЦОД Cisco помогают перейти к облачным технологиям как при модернизации ЦОД, так и при создании новых центров. Безопасное внедрение облачных вычислений действительно позволяет получить экономию и рост эффективности для заказчиков.

Дополнительная информация

Средства обеспечения безопасности ЦОД Cisco

Многофункциональное устройство обеспечения безопасности Cisco ASA 5585-X или сервисный модуль Cisco Catalyst® серии 6500 ASA

Сенсоры Cisco IPS 4500 или блейд-модуль IPS для ASA 5585-X

Cisco TrustSec

Cisco Security Manager

Коммутаторы Cisco Nexus 1000V

Виртуальный шлюз безопасности Cisco (VSG)

Облачный межсетевой экран Cisco ASA 1000V

Центр управления виртуальными сетями Cisco (VNMC)

Унифицированный центр обработки данных Cisco

Виртуализованный многоклиентский ЦОД Cisco – рекомендованный дизайн

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.

Отпечатано в США C11-714844-00 09/12