Безопасная сегментация в унифицированной архитектуре центров обработки данных Cisco

Обзор содержания документа

Этот документ предназначен для технических специалистов, которые стремятся повысить производительность и гибкость своих центров обработки данных и изучают способы максимально эффективного развертывания системы безопасности в частных облачных средах и многоклиентских инфраструктурах ЦОД, используемых для предоставления ИТ как сервиса (ITaaS).

Преобразование ЦОД является непростым процессом на всех этапах с рядом предсказуемых сложных задач для ИТ. Интеграция безопасности в инфраструктуру ЦОД является распространенной проблемой для ИТ-отделов, поскольку им приходится соблюдать баланс при переходе с выделенной инфраструктуры для каждого приложения на модель общего пользования. Для решения этих проблем архитектуры Cisco® Unified Data Center предоставляет три основные технологии: унифицированные вычисления, унифицированная инфраструктура коммутации и унифицированное управление Cisco. В этом документе основное внимание уделяется функциям, возможностям и продуктам унифицированной структуры коммутации Cisco (Cisco Unified Fabric) и ее использовании при создании защищенной сети. После прочтения этого документа вы получите полное представление о концепции безопасного сегментирования. Вы также узнаете о факторах, которые необходимо учитывать при развертывании защищенного многоклиентского центра обработки данных.

Введение

В современных условиях компании испытывают сложности в предоставлении экономически выгодных и эффективных сервисов, призванных удовлетворить существующие и будущие потребности бизнеса. С точки зрения ИТ, в число основных актуальных задач входят инициативы по упрощению ИТ-операций за счет отказа от традиционных систем с низким коэффициентом использования и движение в сторону консолидации, унификации платформ, виртуализации и автоматизации ИТ-инфраструктуры. Эти же инициативы также должны быть направлены на повышение оперативности функционирования ИТ-команд , что позволит компаниям быстрее запускать новые приложения и сервисы. Для достижения этих целей начинается преобразование традиционных центров обработки данных в виртуализированную среду, которая в результате приведет к общедоступным, частным или гибридным облачным развертываниям.

Однако эта тенденция связана с появлением новых проблем в области обеспечения безопасности, которые должны быть устранены до перехода в облачную среду. Это сложные задачи, поскольку они имеют отношение как к технологическим вопросам, так и к значительным изменениям процессов, возникающим из-за продвижения новых моделей вычислений в деловом мире. Компании, которые стремятся выполнить переход на новую инфраструктуру, должны иметь полное представление об обеспечении безопасности в новых системах и адаптировать новые средства для гарантированной защиты передачи информации в масштабах их сред. Кроме того, компании должны убедиться, что новые политики безопасности и технологии не ограничивают масштабируемость и производительность их ЦОД.

Исключительно важным требованием безопасности для компаний и поставщиков услуг, владеющих общими, виртуальными средами является безопасная сегментация. Сегментация (или многоклиентский режим) представляет собой функционал разделения рабочих нагрузок и виртуальных машин для соответствия требованиям к разделению клиентов или пользователей, безопасности, соблюдению норм и соглашений об уровне обслуживания (SLA) при использовании общей инфраструктуры вычислений, систем хранения и сетей. В современных консолидированных ЦОД и облачных средах присутствуют различные группы пользователей, потребности которых связаны как с простой сегментацией, так и с полным разделением сетевого трафика и строгими политиками управления доступом, даже если они работают с общими физическими серверами и с сетевой инфраструктурой.

Предприятия переходят на частные облачные среды, виртуализируя базовую инфраструктуру, которая формально физически выделялась каждому клиенту ЦОД или каждому отделу. При этом предприятия должны обеспечить поддержку текущих уровней безопасности, соответствие нормативным требованиям и уровень качества обслуживания.

В этом документе приводятся сведения о различных вариантах сегментации на примерах сценариев использования. Здесь показывается, что по мере развития организации и ее перехода с физической среды на виртуальную и облачную среды возникает потребность в разных уровнях сегментирования. Материал содержит сценарий использования самых высоких уровней разделения. В документе рассматриваются уровни безопасности, необходимые организациям, находящимся на определенных этапах развития — начиная с выделенной инфраструктуры и до перехода в частную облачную среду:

1. Организация с единой общей инфраструктурой и несколькими приложениями, которой требуется безопасное разделение между приложениями и подразделениями.
   - Выделенная инфраструктура для критически важных приложений, которая является распространенным требованием для приложений, например от Oracle и SAP.
2. Крупные организации с общей инфраструктурой и требованиями к безопасному разделению ресурсов.
   - Несколько отделов с разными требованиями к качеству обслуживания (QoS) на основе соглашений SLA или бизнес-приоритетов (например, трафик системы управления отношениями с клиентами [CRM] имеет более высокий гарантированный уровень, чем видеотрафик).
   - Базовое условие для виртуализации: общие ресурсы с виртуальными контейнерами для различных программных приложений.
3. Одна организация, которая разрослась до нескольких организаций, требующих дополнительного разделения и добавления виртуализации, а также развертывания частного облака и облачных ресурсов для интеграции в процессе приобретения.
   - Соответствие административным требованиям к разделению, позволяющее исключить перекрытие трафика. Например, защита группы, занимающейся управлением информации о кредитных картах должна осуществляться иначе, чем защита инженерной группы.
   - Исключительная необходимость сегментирования отдельных виртуальных сред.
4. Ситуации с гарантиями по соглашениям SLA. Например, в организациях здравоохранения, где ИТ-отделы являются поставщиками услуг с соответствующими гарантиями.
   - Создание границ и гарантированное разделение.
   - Координация и упрощение.

Разработка модели безопасности для сегментации

Одной из самых серьезных проблем, стоящих перед ИТ-специалистами, является безопасность центра обработки данных. Клиентам необходимы решения по защите ценных объектов и конечных результатов, обеспечению доступности и соблюдению нормативных требований. Кроме того, они хотят получить высокопроизводительную систему безопасности ЦОД, которая будет способна обрабатывать большие объемы рабочих нагрузок, поддерживать множество различных типов данных и сетевых транзакций. При изучении возможностей перехода во многоклиентскую или частную облачную среду ИТ-специалистам необходимо учитывать следующие принципы и вопросы безопасности:

Многоклиентская модель и сегментация

- Многоклиентская модель. 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 арендуют разные ресурсы разные компании, 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.

- Сегментация. В крупных организациях может быть развернуто несколько тысяч приложений, которые можно сегментировать по типам бизнес-задач, степени важности (критически важное или не имеющее высокой важности), функции и т. д. Каждый из этих сегментов должен быть защищен с помощью согласованных механизмов безопасности, которые применяются как в физической сети, так и в облаке, и предотвращают потерю данных в результате действия внешних и внутренних угроз. Организации все больше придерживаются принципов сегментирования, внедряют технологию виртуализации и переносят приложения в облако, сеть становится все более сложной средой. Это особенно заметно при вводе средств для автоматизации и координации процессов.

Безопасный доступ к 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 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.

Прозрачность и соответствие требованиям в облаке

- Сложность системы и многокомандный подход к управлению. Многие компании замечают потерю прозрачности при переходе к облачным технологиям. Традиционные межсетевые экраны и системы предотвращения вторжений, расположенные за границами 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.
- Частное или общедоступное облако. 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.

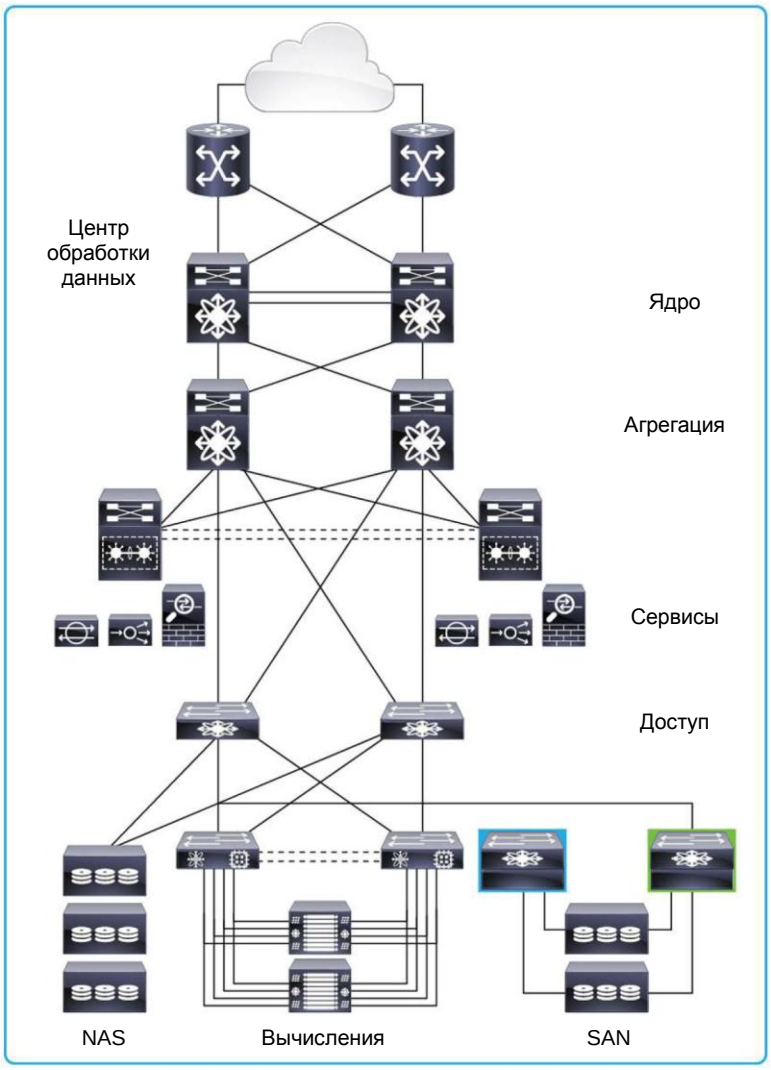
Сценарии использования сегментации

Сегментация инфраструктуры многоклиентского центра обработки данных является базовой технологией безопасности, предоставляющей возможность создания виртуальных контейнеров в архитектуре ЦОД. Сегментация гарантирует разделение рабочих нагрузок и виртуальных машин в соответствии с требованиями по разделению клиентов, безопасности, соблюдения норм и соглашений SLA для предоставляемых сервисов.

В пяти сценариях использования, представленных в этом документе, рассматриваются различные уровни сегментации ЦОД по мере развития организации. Начиная от перехода с традиционной модели сегментации в сценарии 1, до добавления гарантированной безопасности и изоляции для многоклиентской модели. Сценарии использования показывают варианты изменения существующей архитектуры для адаптации к новым требованиям, в связи с изменениями требований организации к безопасности в результате приобретений, роста, добавления новых приложений и появления новых административных норм.

Описанные сценарии основаны на стандартной иерархической платформе ЦОД, изображенной на рис. 1. Иерархический дизайн обычно использовался в сетевых инфраструктурах для обеспечения масштабируемости и высокой доступности. И теперь иерархическая модель аналогичным образом применяется в архитектуре унифицированного центра обработки данных Cisco для создания надежной сетевой инфраструктуры. В иерархическом представлении сеть Cisco формирует уровни ядра, агрегации и доступа.

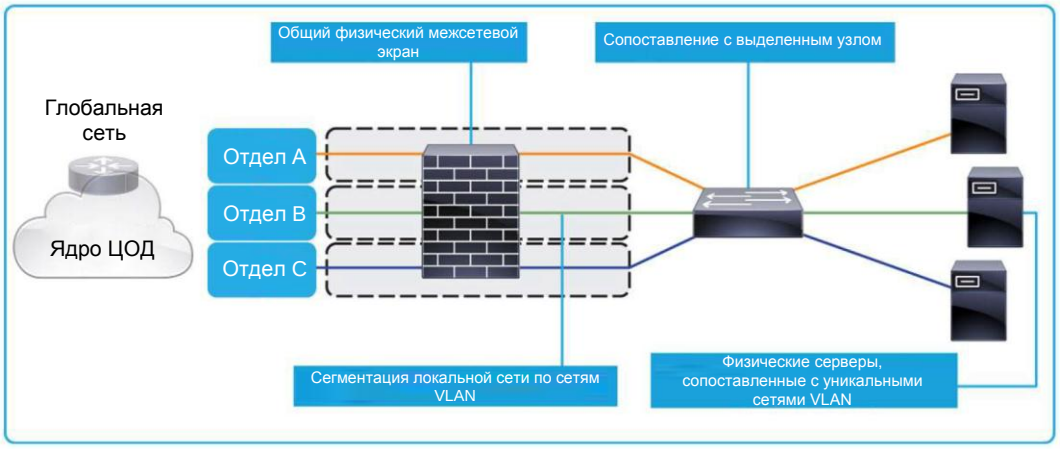
Рис. 1. Иерархическая структура сети



Сценарий использования 1. Организация с единой общей инфраструктурой и несколькими приложениями, которой требуется разделение между приложениями и отделами

На рис. 2 показан сценарий использования 1.

Рис. 2. Сценарий использования 1



Требования организации в области безопасности

- Отделам A, B и C требуется разделение доступа к приложениям в целях обеспечения безопасности и соблюдения норм.
- Организации необходимы некоторые элементы физической и виртуальной сегментации.

Продукты для сценария использования 1

- Многофункциональные устройства безопасности Cisco ASA 5500, коммутаторы Cisco Nexus®.

Интернет-периметр

Реализация политики безопасности осуществляется на периметре глобальной сети, который является границей общей инфраструктуры на сетевом уровне (L3) и обеспечивает контроль доступа к корпоративной сети и ЦОД. Как правило, на этом уровне реализованы следующие возможности:

- правила политик безопасности применяются с помощью списков контроля доступа маршрутизаторов (ACLs);
- между физической сетью и несколькими виртуальными сетями находится сетевой МСЭ;
- используется контекстная виртуализация;
- топология, процессы подготовки и мониторинга изолированы для каждого подразделения.

Общий физический межсетевой экран

Общий физический МСЭ на платформе Cisco ASA5500 для подразделений A, B и C и используется для фильтрации внешнего трафика, одновременно обеспечивая защиту доступа к сетям VPN и нейтрализацию угроз. Технология VLAN обеспечивает изоляцию потоков данных и сопоставление с доменами безопасности каждого пользователя.

Контейнеры подразделений

Семейство коммутаторов Cisco Nexus обеспечивают изоляцию между контейнерами подразделений A, B и C. Технология VLAN позволяют разделить физическую сеть на несколько логических оптимального использования ресурсов.

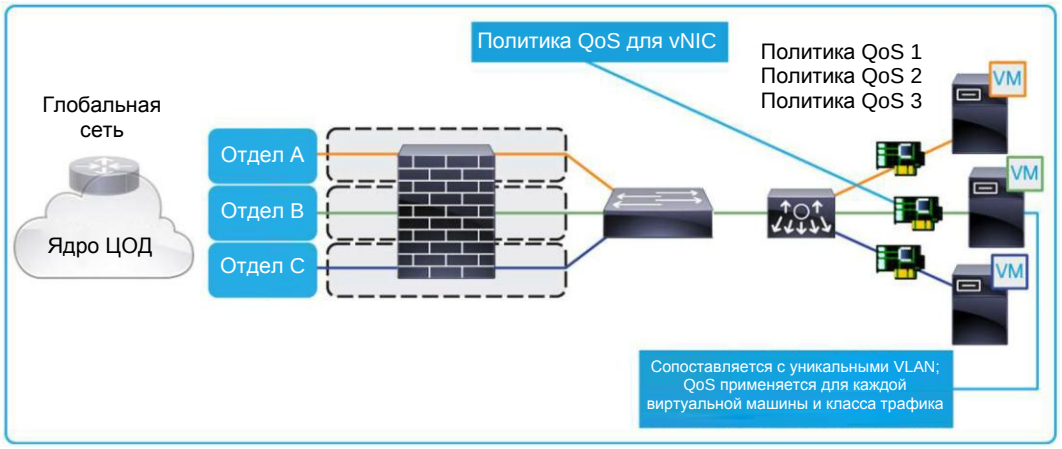
Серверы

Эту модель дополняют выделенные физические серверы. Отдельные физические серверы обрабатывают определенные приложения, которые, в свою очередь, сопоставляются с набором политик VLAN и политик безопасности.

Сценарий использования 2. Организация с единой общей инфраструктурой и несколькими приложениями, которой требуются элементы физического и виртуального сегментирования ресурсов

На рис. 3 показан сценарий использования 2.

Рис. 3. Сценарий использования 2



Требования организации в области безопасности

- В организации есть несколько отделов с разными требованиями к качеству обслуживания.
- Базовым условием для виртуализации являются общие ресурсы с виртуальными контейнерами для различных приложений.
- Организации необходимо выполнить разделение виртуальных машин и рабочих нагрузок для соответствия требованиям по разграничению доступа для подразделений и соблюдения норм и соглашений SLA

Продукты, добавленные в сценарий использования 1

- Виртуализированный коммутатор Cisco Nexus 1000V, гипервизор виртуализации и виртуальные машины на физических серверах, виртуальные сетевые карты (vNIC для виртуальной сети Ethernet в Cisco Nexus 1000V).

Серверы

Виртуализация внедряется на серверы для создания безопасных контейнеров для сервисов.

Виртуальный коммутатор Cisco Nexus 1000V позволяет сегментировать потоки трафика на уровне виртуальных машин и реализует сервисы безопасности.

Cisco Nexus 1000V и технология Cisco VN-Link предоставляют возможности контроля отдельных виртуальных машин. Теперь настройку политик для виртуальных машин и их реализацию можно выполнять в Cisco Nexus 1000V.

Трафик от виртуальной машины можно отправлять на физические устройства (например, с помощью VLAN), для реализации различных сетевых сервисов. С помощью виртуальных контекстов можно организовать многоклиентский режим работы.

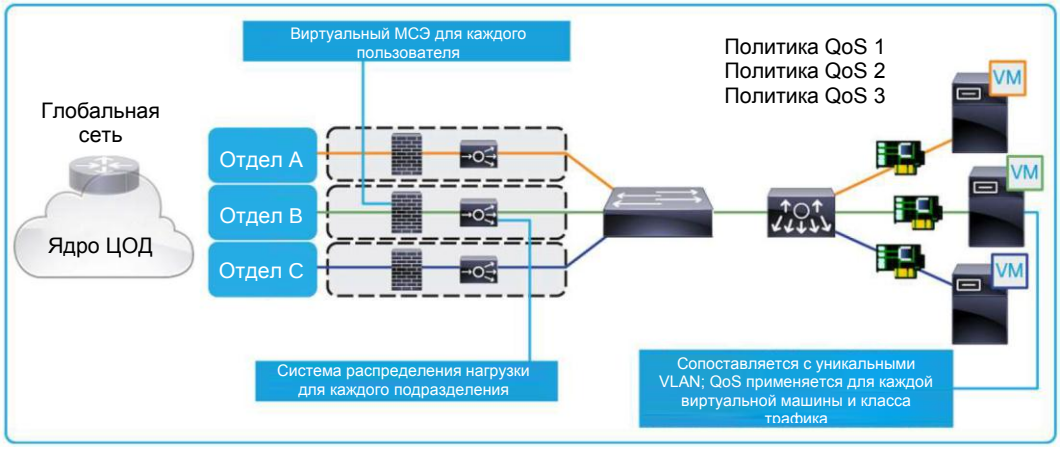
Политика QoS для каждого подразделения

Cisco Nexus 1000V предоставляет широкие возможности реализации и контроля политик для каждой конкретной виртуальной машины. Коммутатор Cisco Nexus 1000V поддерживает типы очередей CBWFQ и LLQ. Политики QoS применяются персонализировано к каждой виртуальной машине пользователя (то есть для каждой карты NIC) для каждого класса трафика. Классифицированный и промаркированный трафик обслуживается в соответствии с заданными политиками QoS на всех узлах коммутации на базе Cisco Nexus в сетевой инфраструктуре.

Сценарий использования 3. Одна организация, которая трансформировалась в несколько организаций, требующих сегментирования и виртуализации, а также внедрения частного облака и облачных ресурсов для интеграции при приобретениях

На рис. 4 показан сценарий использования 3.

Рис. 4. Сценарий использования 3



Требования организации в области безопасности

- Организации требуются дифференцированные уровни качества обслуживания для каждого приложения в соответствии со сценарием использования.
- Для обеспечения соответствия административным требованиям к разделению необходима дополнительная изоляция для каждого подразделения (МСЭ и сервисы), позволяющая исключить перекрытие трафика.
- Важное значение имеет сегментация на уровне виртуальных сред.

Продукты, добавленные в сценарий использования 2

- Виртуальный МСЭ и система балансировки нагрузки для каждого подразделения.

Выделенные виртуальные контексты для каждого подразделения

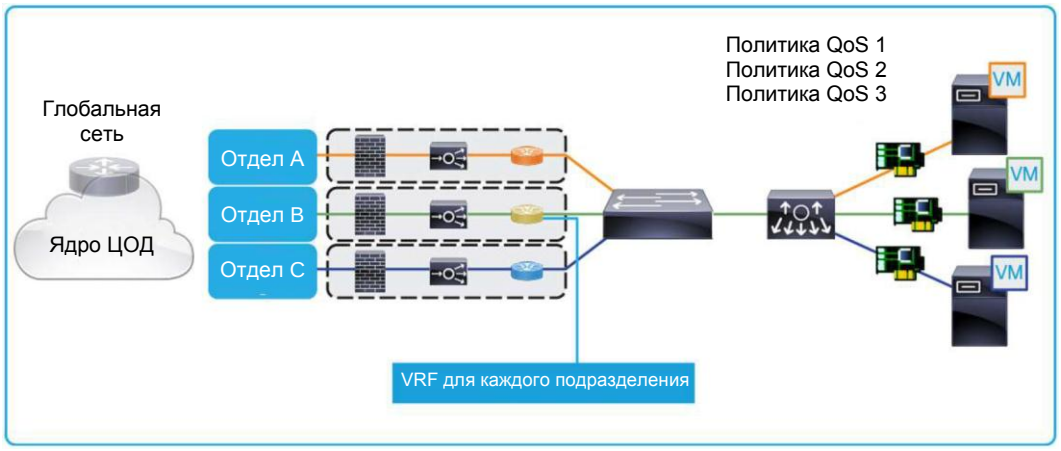
- Виртуализация используется в узлах инфраструктуры.
- Сервисы МСЭ и балансировки нагрузки выделяются логически для каждого подразделения.

- Система балансировки Cisco Application Control Engine (ACE) предоставляет виртуальные контексты, которые выделяются для каждого подразделения с целью изоляции трафика, передаваемого между узлами сервиса.
- Коммутатор Cisco Nexus 1000V реализует виртуальные контексты МСЭ для каждого подразделения.

Сценарий использования 4. Ситуации с гарантированным SLA. Например, организации здравоохранения, которым необходим высочайший уровень разделения и изоляции пользователей для соответствия нормативным требованиям

На рис. 5 показан сценарий использования 4.

Рис. 5. Сценарий использования 4



Требования организации в области безопасности

- Организации требуются дифференцированные уровни качества обслуживания для каждого приложения в соответствии со сценарием использования.
- Например, сценарий использования в клинике позволит гарантировать, что клиент соблюдает закон о передаче данных и отчетности в медицинских учреждения (HIPPA).

Продукты, добавленные в сценарий использования 2

- Функционал виртуальной маршрутизации (VRF) для каждого подразделения.

Функционал виртуальной маршрутизации, технология VRF

Некоторым организациям необходим очень высокий уровень безопасности. Часто для обеспечения дополнительной защиты требуется создание выделенной наложенной сети. Одним из способов реализации такого решения является использование функции VRF в семействе коммутаторов Cisco Nexus. За счет добавления выделенного экземпляра VRF для каждого подразделения происходит изоляция серверов back-end приложений (например, серверов приложений и баз данных).

Технология VRF позволяет реализовать нескольких экземпляров таблицы маршрутизации в одном маршрутизаторе. Поскольку экземпляры маршрутизации являются независимыми, они позволяют гибко разделять информационные потоки в многоклиентской среде.

Глобальный экземпляр VRF представляет собой виртуальную сетевую инфраструктуру, объединяющую общие ресурсы и виртуальные машины. В число общих ресурсов может входить демилитаризованная зона DMZ (с прокси-серверами, IPS и системой распределения серверной нагрузки [SLB] для ускорения обработки сессий SSL).

С помощью шлюза безопасности Cisco Virtual Security Gateway VSG возможно дополнительно обеспечить гибкую сегментацию для общей внешней зоны и серверных зон для каждого подразделения, таким образом, обеспечивая более комплексную поддержку требований к безопасности и разделению многоуровневых приложений.

Преимущества решений Cisco для безопасности ЦОД

Комплекс решений Cisco для безопасности ЦОД формирует контролируемую политиками среду для реализации новых бизнес-инициатив и развертывания различных приложений. Универсальный и эффективный подход Cisco к безопасности ЦОД позволяет организациям улучшить качество и сократить время предоставления сервисов. Вместе с решениями Cisco по защите ЦОД Вы сможете:

- Обеспечить высокую доступность ЦОД, реализовав защиту от угроз;
- Защитить сервисы ЦОД на уровне приложений и предоставления контента;
- Предотвратить потери для бизнеса за счет реализации безопасного доступа;
- Обеспечить соответствие нормативным требованиям как для физической, так и для виртуальной инфраструктур

Решения Cisco по защите ЦОД предоставляют следующие преимущества:

- Компания Cisco располагает необходимыми технологиями и богатым опытом, а также ответственно относится к работе с заказчиками.
- Продукты безопасности Cisco разработаны в том объеме и полноте, которые необходимы для решения проблем, связанных с защитой ЦОД клиентов.
- Инновации и архитектура Cisco вместе с рекомендованными дизайн-решениями поддерживают клиентов на стадиях внедрения и обслуживания, помогая повысить эффективность работы и сократить совокупную стоимость владения (TCO).

Рекомендованный дизайн Cisco для виртуализированного многоклиентского ЦОД

Эксперты Cisco проводят тщательное тестирование, необходимое для того, чтобы надежность и стабильность архитектуры соответствовала требованиям к безопасному центру обработки данных, безопасному виртуальному центру обработки данных и безопасному частному облаку в виртуальной среде.

Архитектура Cisco Virtualized Multiservice Data Center (VMDC) обеспечивает защиту критически важных приложений и конфиденциальных данных, обрабатываемых в ЦОД. Решение Cisco Unified Data Center изменяет экономику центра обработки данных путем объединения вычислений, систем хранений, сетей, виртуализации и управления в единую платформу на основе инфраструктуры коммутации, что позволяет повысить операционную эффективность, упростить ИТ-процессы и обеспечить гибкость 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.

С унифицированным ЦОД тесно интегрированы средства управления безопасностью, включенные в лидирующий в отрасли межсетевой экран, технологии VPN, система IPS с аппаратным ускорением, а также устройства и приложения для виртуальной среды. Защищенная апробированная архитектура Cisco VMDC обеспечивает прозрачную передачу сетевого трафика из физической сети в виртуальную, повышая гибкость операций и упрощая управление. Она позволяет создавать несколько зон безопасности, логически разделяющих ресурсы пользователей в виртуальной сети, и выполнять отказоустойчивое перемещение виртуальных машин. Система безопасности периметра сети защищает ЦОД от внешних угроз и предоставляет надежный контекстно-зависимый доступ к ресурсам центра обработки данных. Cisco VMDC является интуитивно понятной, мощной и безопасной платформой, которая обеспечивает исключительную защиту важных информационных активов в реальном времени с помощью новейшей системы IPS с глобальной корреляцией, МСЭ и МСЭ веб-приложений (WAF) и технологией VPN.

В связи с переходом заказчиков в многоклиентские среды организации, отвечающие за ЦОД должны выполнить дополнительные требования:

- Упрощенное развертывание и масштабирование вычислительных ресурсов, безопасная установка и функционирование виртуальных машин.
- Поддержка виртуальными машинами возможностей разделения рабочих нагрузок по уровням доверия и логическим группам.
- Наличие средств запроса безопасного самостоятельного построения виртуальных машин для создания клиентами новых виртуальных машин для временных или постоянных рабочих нагрузок, а также для развертывания и тестирования.
- Шаблоны соответствия требованиям и средства автоматизации политик для связи политики безопасности с координацией сети.

Компания Cisco поможет выполнить эти дополнительные требования с помощью реализации политики зонирования на основе ролей путем виртуального управления и с помощью виртуальных шлюзов, предоставить защищенные прозрачные каналы для мобильности виртуальных машин и обеспечить защищенную автоматизацию за счет рекомендованных дизайн-решений с шаблонами для соблюдения норм и политик.

Многоуровневая комплексная безопасность за счет Cisco VMDC

Успешное развертывание облачной архитектуры зависит от комплексной безопасности инфраструктуры ЦОД и виртуализованных сред, в которых выполняются приложения и сервисы потребителей облачных услуг. Архитектура Cisco VMDC позволяет справляться с проблемами безопасности за счет предоставления универсальной платформы для обеспечения сквозной защиты на нескольких уровнях сети.

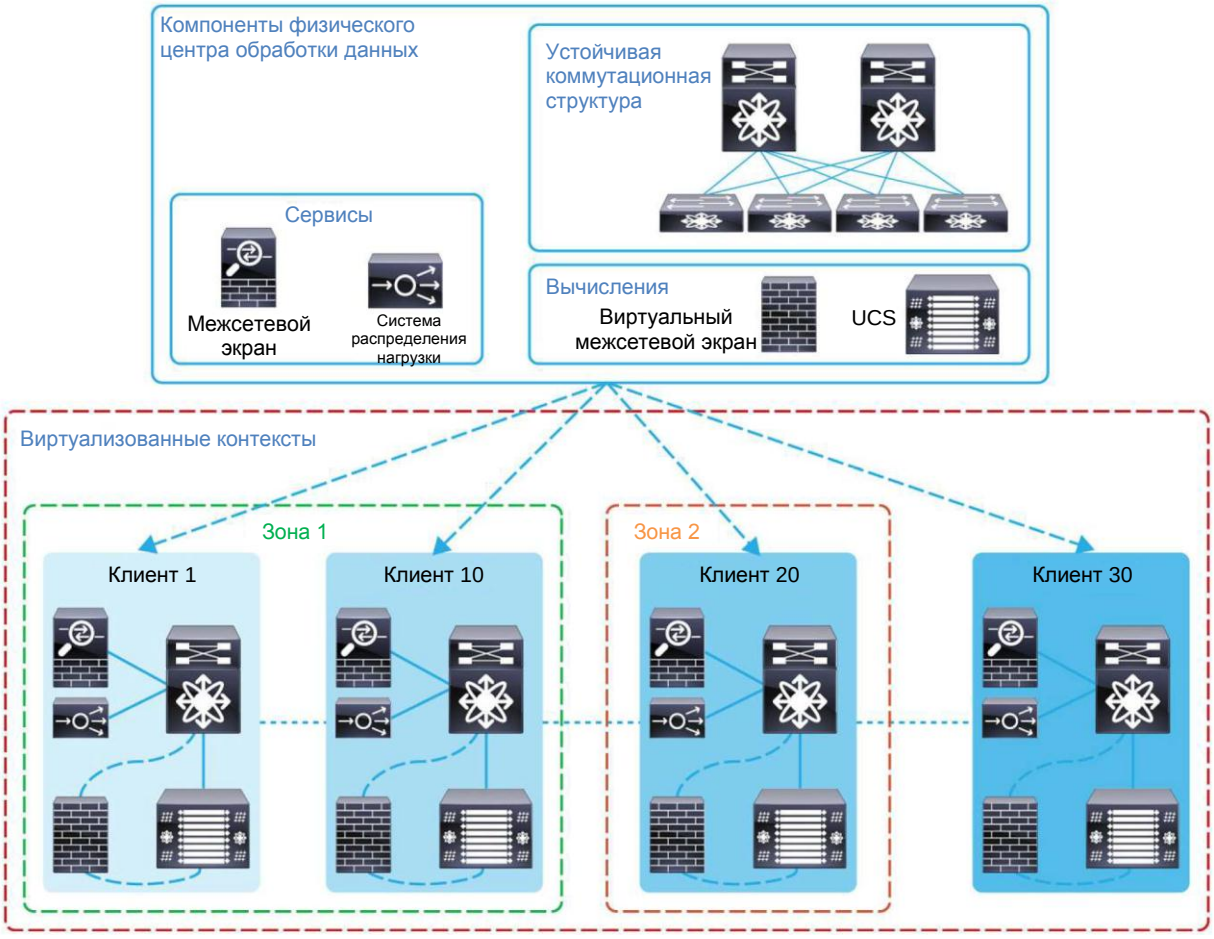
Для реализации эффективного подхода по обеспечению безопасности в соответствующих точках сети ЦОД необходимо развернуть ряд взаимодействующих сервисов безопасности. К основным требованиям безопасности ЦОД относятся:

- Защита ЦОД от неавторизованных пользователей и атак извне
- Предотвращение вторжений и данных, содержащих вредоносное программное обеспечение
- Защита периметра сетей заказчиков с помощью проверенного МСЭ для обеспечения безопасности виртуальной и облачной инфраструктуры
- Назначение виртуальных машин сегментированным доверенным зонам в виртуальной сети и реализация политик доступа на уровне виртуального сервера
- Предоставление централизованного управления многоклиентскими политиками
- Поддержка мобильности виртуальных машин
- Защита доступа к виртуализированным ЦОД и приложениям
- Предоставление решения защиты, масштабируемого в соответствии с остальной частью инфраструктуры, готовой к переносу в облако
- Разделение обязанностей администраторов безопасности, сетевой и серверной инфраструктур

В архитектуре Cisco VMDC используется набор физических и виртуальных средств безопасности Cisco, в который входят многофункциональное устройство Cisco ASA 5585-X, облачный межсетевой экран Cisco ASA 1000V Cloud Firewall, виртуальный шлюз Cisco VSG, виртуальные коммутаторы Cisco Nexus серии 1000V и ПО управления Cisco Virtual Network Management Center (VNMC), предназначенные для согласованного управления безопасностью и политиками физического периметра сети клиентов ЦОД, а также взаимодействиями между пользователями внутри клиентских зон. Решение Cisco VNMC совместно с технологией Cisco vPath, представленной в коммутаторах Cisco Nexus серии 1000V, повышают гибкость и эффективность функций безопасности за счет реализации возможности динамической контекстно-зависимой защиты.

Для поддержки многоклиентской модели для каждого клиента традиционно развертывается выделенная инфраструктура. Однако этот подход имеет определенные трудности масштабирования, связанные с затратами, сложностями управления и неэффективным использованием ресурсов. В архитектуре VMDC несколько клиентов в общей инфраструктуре могут рационально использовать общие ресурсы, добиваясь тем самым снижения затрат. Каждый клиент может рассчитывать на изоляцию своих вычислительных ресурсов от остальных при использовании общей вычислительной инфраструктуры. Логическое разделение или виртуализация, являющееся основополагающим принципом многопользовательской среды, комплексно реализуется в архитектуре Cisco VMDC на уровнях сети, вычислений и систем хранения (рис. 7).

Рис. 6. Многоклиентская структура



Заключение

Решения Cisco для защищенного центра обработки данных для частного облака обеспечивают безопасную многоклиентскую работу в средах частных облаков и предоставляют возможности контроля сетевого трафика и работы сети, необходимые клиентам для поддержки процессов управления в облаке. Клиентам, выбравшим переход на облачные вычисления, компания Cisco поможет сократить риски благодаря согласованным политикам и их скоординированному внедрению, более высокому уровню масштабируемости и улучшенной производительности. Продукты безопасности Cisco наряду с унифицированным центром обработки данных Cisco призваны упростить переход к облачным технологиям независимо от того, выполняется ли обновление ЦОД или создается новый, позволяя надежными и безопасными способами получить экономию от масштаба и достичь эффективности облачных вычислений.

Дополнительная информация

- Безопасность ЦОД Cisco: http://www.cisco.com/en/US/partner/netsol/ns340/ns394/ns224/ns376/index.html
- Устройство Cisco ASA 5585-X и сервисный модуль Cisco Catalyst® серии 6500 ASA Services Module: http://www.cisco.com/en/US/partner/products/ps11621/index.html
- Сенсоры Cisco IPS серии 4500 и процессор Cisco ASA 5585-X IPS Security Services Processor: http://www.cisco.com/go/ips
- Коммутаторы Cisco Nexus серии 1000V: http://www.cisco.com/en/US/partner/products/ps9902/index.html
- Cisco VSG: http://www.cisco.com/en/US/partner/products/ps11208/index.html
- Облачный межсетевой экран Cisco ASA 1000V Cloud Firewall: http://www.cisco.com/en/US/partner/products/ps12233/index.html
- Cisco VNMC: http://www.cisco.com/en/US/partner/products/ps11213/index.html
- Унифицированный центр обработки данных Cisco: http://www.cisco.com/en/US/partner/netsol/ns340/ns394/ns224/architecture.html
- Рекомендованная архитектура Cisco VMDC: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html

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 C11-722425-00 12/12