Решения Cisco для защищенного центра обработки данных

БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ, ГИБКОСТЬ И ВОЗМОЖНОСТЬ МАСШТАБИРОВАНИЯ ЦОД

Безопасное преобразование ЦОД

При увеличении требований к ЦОД предприятиям необходимо искать пути снижения капитальных инвестиций, повышения эффективности своей деятельности, оптимизации ИТ-ресурсов, достижения гибкости и возможности масштабирования, а также создания условий для новых моделей работы, обеспечивающих рост выручки. Для достижения этого предприятия совершенствуют архитектуру ЦОД, переходя от традиционных решений к виртуализированной, а затем и к облачной среде.

При переходе к новым моделям вычислений возникают проблемы обеспечения безопасности, как технического, так и делового характера. Это является основным барьером на пути перехода от виртуализированного ЦОД к использованию облачной среды. В ответ на этот вызов необходимо пересмотреть подходы к обеспечению безопасности и разработать новые средства защиты при передаче информации.

Оптимизация безопасности для новых ЦОД

Решение Cisco® для защищенного ЦОД обеспечивает возможность безопасной сегментации сети, а также позволяет задать политики безопасности для виртуальных машин и пользователей. При реализации политик это решение блокирует внутренние и внешние угрозы на границах зон ЦОД и приложений. Так достигается прозрачность элементов и информационных потоков в сети, что позволяет обеспечить соблюдение политики вне зависимости от модели развертывания.

Ключевые элементы решения Cisco® для защищенного ЦОД:

- безопасная сегментация
- защита от угроз
- прозрачность

Безопасная сегментация

Большие предприятия используют сегментацию для организации данных в ЦОД. Однако безопасность сегментированной структуры зависит от того, где, для кого и кем она была внедрена. По мере сегментации и визуализации организации, а также перевода приложений в облачную среду увеличивается сложность сети. Средства безопасности должны быть встроены в саму сеть, работая в ней для обеспечения устойчивости политики и прозрачности во время передачи важной информации по сети.

- Многофункциональные устройства безопасности Cisco ASA 5585-X рассчитаны на удовлетворение требований к работе критически важных ЦОД. В них используется технологии проверенного во всем мире межсетевого экрана и системы предотвращения вторжений, наиболее широко распространенной в отрасли, которые ориентированы на работу с учетом контекста. В результате получилось самое эффективное решение в отрасли, позволяющее существенно снизить риски делового характера и обеспечить соблюдение нормативных требований. И все это в компактном варианте исполнения высотой 2 RU.
- ПО Cisco ASA версии 9.0 поддерживает устройства платформы ASA различного форм-фактора, включая широкий диапазон автономных устройств, блейд-модулей, которые интегрируются с существующей сетевой инфраструктурой, и программное обеспечение для защиты общедоступных и частных облаков. Версия 9.0 отличается возможностью кластеризации; интеграцией с решением Cisco Cloud Web Security (прежнее название - ScanSafe), что позволяет обеспечить детализацию контроля доступа в Интернет и политики работы с веб-приложениями с одновременной защитой от вирусов и вредоносных программ. При этом поддерживается технология меток групп безопасности (Security Group Tags, SGTs) 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 или пользователей на основе контекста при их подключении с последующим преобразованием порядка внедрения политики безопасности во всей инфраструктуре ЦОД. Такая классификация использует метки групп безопасности для формирования решений о допуске или отказе от допуска на основе интеллектуальной политики. Кроме того, эта технология автоматизирует разработку правил работы межсетевого экрана, снижая уровень сложности при организации контроля доступа.
- Межсетевой экран для облачной среды Cisco ASA 1000V обеспечивает безопасность периметра сетей пользователей внутри ЦОД, разделяя физическую и виртуальную среду. Этот экран, созданный с использованием технологий ASA, позволяет сформировать интеллектуальные границы с использованием технологий VPN для связи между объектами, реализует функционал трансляции адресов (NAT), протокола DHCP и предотвращения сетевых атак. Многопользовательский ЦОД или частная облачная среда, естественно, требуют изоляции трафика приложений для различных клиентов, приложений и групп пользователей в зависимости от принятой политики. Архитектура Cisco ASA 1000V предусматривает интеграцию с коммутатором Nexus 1000V для улучшения гибкости при развертывании.
- Виртуальный шлюз безопасности Cisco Virtual Security Gateway вместе с коммутатором Cisco Nexus® 1000V обеспечивает детальную безопасность при контакте между виртуальными машинами в пределах одной клиентской зоны. Он работает в качестве сетевого шлюза и обеспечивает разграничение доступа на основе зон безопасности и контекстно-зависимую защиту виртуальных машин. Шлюз использует технологию Virtual Path (vPath), являющуюся частью функционала коммутатора Cisco Nexus 1000V.

- Технология Cisco vPath обеспечивает управление как внутренним трафиком с помощью облачного межсетевого экрана ASA 1000V, так и потоками данных между виртуальными машинами с помощью шлюза Virtual Security Gateway. Это обеспечивает возможность связи между собой встроенных виртуальных сервисов, развернутых в составе решения (включая виртуальный шлюз безопасности и облачный межсетевой экран). Помимо того, технология vPath предусматривает возможность использования виртуальных расширяемых сетей LAN (VXLAN) для улучшения масштабирования.
- Коммутаторы Cisco Nexus 1000V обеспечивают высокий уровень безопасности многоклиентских сервисов, добавляя интеллектуальные средства виртуализации к возможностям сети ЦОД. Эти программные коммутаторы расширяют границы сети к гипервизорам и виртуальным машинам, предусматривая возможность масштабирования для облачных сетей. Коммутаторы Nexus 1000V поддерживают различные варианты гипервизоров, включая VMware vSphere и Microsoft Windows 2012 Server Hyper-V. Коммутатор Nexus 1000V формирует фундамент архитектуры виртуальных наложенных сетей – ключевой технологии концепции Software Defined Networks (SDN).

Защита от угроз

В исследовании утечек данных компании Verizon 2011 г. указано, что 92 % сетевых угроз являются внешними: их источники - это хакеры, организованные преступные сообщества и государственные организации; а цели таких атак - конкретные организации. Решения Cisco защищают инфраструктуру и приложения от передовых постоянных угроз и прочих сложных внешних атак с помощью анализа угроз, пассивного контроля признаков OS, анализа репутации и контекста.

- Устройство Cisco IPS 4500 обеспечивает проверку с аппаратным ускорением, производительность, соответствующую реальным условиям эксплуатации, высокую плотность портов и энергетическую эффективность в расширяемом шасси, рассчитанном на будущий рост и защиту инвестиций. Его малые размеры и низкое потребление энергии делают его идеальным для ЦОД, предъявляющих жесткие требования к свободному месту.
- Решение Cisco ASA CX можно развертывать в ЦОД в качестве межсетевого экрана для подразделений. Что позволяет идентифицировать, разграничивать доступ с учетом контекстной информации и вести учет доступа к внешним серверам из сети подразделения.

Прозрачность

Заказчики желают иметь идентичный уровень контроля как в физически-выделенной среде, так и в виртуальной. Решения Cisco упрощают работу и формирование отчетности о соблюдении норм, обеспечивают прозрачность элементов защиты сети и учитывают особенности основной деятельности организации в работе сети.

- Cisco Security Manager 4.3 - это комплексное решение для управления, обеспечивающее постоянное соблюдение политик, устранение проблем и подготовку обобщенных отчетов по объекту управления. Данный продукт управляет инфраструктурой средств защиты Cisco, обеспечивая прозрачность на объекте управления и совместное использование данных важными сетевыми службами. И наконец, повышает эффективность работы за счет 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.
- 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. Cisco VNMC - это прозрачное масштабируемое решение для управления объектами на основе политик для обеспечения комплексной безопасности виртуальных и облачных сред. Оно обеспечивает быстрое развертывание на основе динамического управления и на базе политик с использованием шаблонов и профилей безопасности. Центр Cisco VNMC обеспечивает повышение гибкости управления благодаря интерфейсу API XML, поддерживающему интеграцию со сторонними средствами управления. Также VNMC предоставляет администраторам безопасности возможность раздельного управления политиками безопасности приложениями, серверами и сетями в целях обеспечения соответствия нормам.

Эффективная интегрированная безопасность

Архитектура Cisco SecureX Architecture™ — это ориентированный на сеть подход к безопасности с учетом контекста, который обеспечивает единообразную реализацию политик безопасности в масштабах всей организации, более высокий уровень согласованности политик безопасности с потребностями бизнеса, интегрированные глобальные интеллектуальные ресурсы и упрощение доставки сервисов. Поддержка задач основной деятельности организации за счет оптимизации управления рабочей средой, выходящей за рамки обычного безопасного ЦОД, является основой этого похода. В результате получается комплексная автоматизированная система обеспечения безопасности, прозрачная для конечного пользователя и более эффективная для ИТ-организации.

Отличительные особенности продуктов Cisco:

- Полный комплект проверенных функций обеспечения безопасности, не влияющих на работу критических сервисов делового назначения
- Высокопроизводительный межсетевой экран с возможностью масштабирования в соответствии с новыми потребностями ЦОД
- Гибкость интеграции со сложными распределенными сетями
- Эффективная поддержка архитектур, связывающих виртуальные машины и группы пользователей (развертывание в зонах и на границах)
- Единые политики и принципы управления в физической, виртуальной и облачной средах, средства обеспечения безопасности с функциями, независящими от размера сетей

- Прозрачность интеграции внедрения политик в сетевые структуры за счет использования таких инновационных решений, как VM-Fex, OTV, LISP и vPath
- Мультиконтекстный дизайн и масштабируемость виртуальной инфраструктуры
- Интеграция продуктов в прошедший тщательную проверку типовой дизайн архитектуры Cisco Unified Data Center

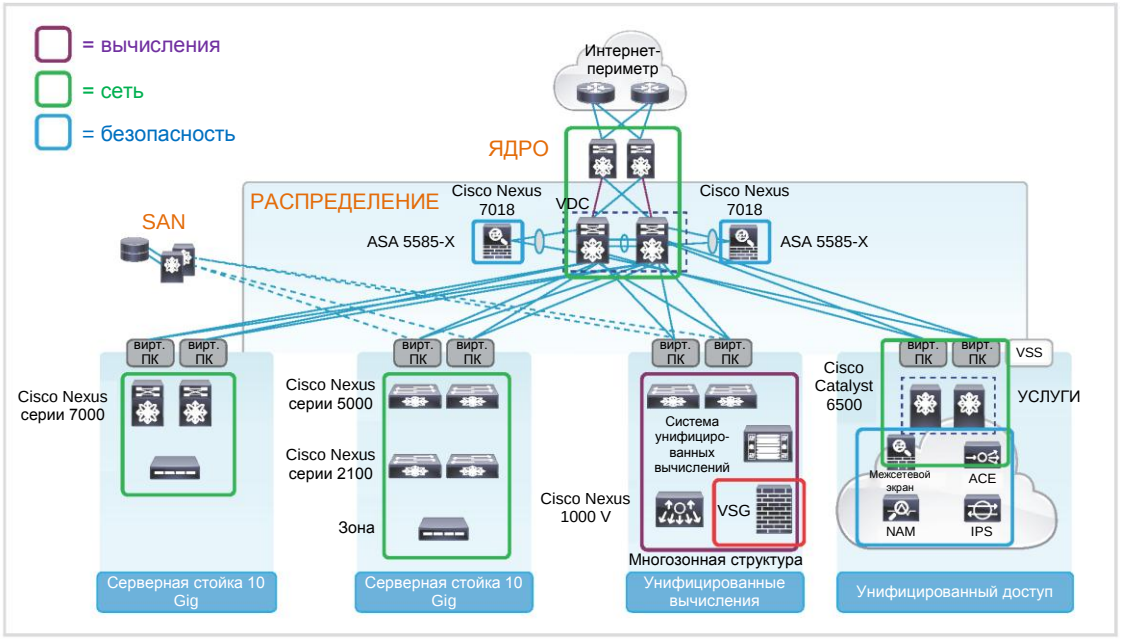
Интеграция функций безопасности в унифицированный ЦОД

Cisco предусмотрены интенсивные испытания решений для выполнения требований надежности и устойчивости в работе при обеспечении безопасности физического или виртуального ЦОД, а также облачной среды. Виртуализированный мультисервисный ЦОД Cisco (VMDC) построен путем интеграции защитных функций в проверенное решение для унифицированных 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.

С унифицированным ЦОД тесно интегрированы средства управления безопасностью, включенные в лидирующий в отрасли межсетевой экран, функционал VPN, систему IPS с аппаратным ускорением и устройства и приложения для виртуальной среды. Эта безопасное и проверенное решение обеспечивает надежность передачи трафика от физических к виртуальным сетям, повышая гибкость работы и упрощая управление. Такое решение позволяет создать несколько зон безопасности, логически разделяющих ресурсы пользователей в виртуальной сети, и выполнение отказоустойчивого перемещения 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 комплекса средств - новейшей системы IPS с глобальной корреляцией, межсетевых экранов и шлюзов Web-приложений, а также технологией VPN.

На рис. 1 показана архитектура решения Cisco VMDC.

Рис. 1. Архитектура решения Cisco VMDC Solution



Почему именно Cisco?

Cisco - лидер в области безопасных сетей с признанным опытом инноваций в этой сфере. Архитектура Cisco SecureX уникальным образом объединяет три основных элемента: сеть, предоставляющую контекстную информацию и реализующую выполнение политик безопасности; средства сбора данных о глобальных угрозах и один из самых больших портфелей с решениями в области безопасности в отрасли.

Дополнительная информация

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

C45-647419-02 09/12