# Решения Cisco Secure Data Center для защиты виртуальных и частных облачных сред

## Требования заказчика

**В.** Почему важно обеспечить безопасность виртуальной и облачной инфраструктуры?

**О.** Виртуализация и облачные вычисления изменили способы передачи и потребления информации и сервисов. Гибкое и более результативное использование ресурсов повысило эффективность и конкурентоспособность бизнеса, ускорив достижение организациями своих целей. Одновременно эти новые технологии привели к возникновению новых рисков в области безопасности и проблем, связанных с изменением рабочих процессов. Для достижения успеха организациям необходимо решить вопросы обеспечения безопасности.

**В.** С какими проблемами в области безопасности, связанными с виртуализацией и облачными вычислениями, сталкиваются заказчики?

**О.** Можно выделить четыре основные группы таких проблем:

- **Защита от угроз:** сетям необходима защита от внешних и внутренних угроз. Снаружи надо защищать инфраструктуру и приложения от потерь данных, атак на сети и приложения, а также других современных атак. Для этого используются такие передовые технологии, как выявление и анализ угроз, пассивный контроль признаков ОС, анализ репутации и контекста совместно с глобальной корреляцией, обеспечивая высокий уровень безопасности. Изнутри требуется защита от угроз, вызванных общими атаками на службу доменных имен, порты и протоколы со стороны недовольных работников.
- **Проблемы, вызванные новыми технологиями.** Хорошим примером является работа с большим числом пользователей. Вместо физического выделения инфраструктуры (серверов, коммутаторов, хранилищ) для каждого приложения, подразделения или функции, в больших виртуальных и облачных средах используется логическое разделение для групп пользователей, требующих защищенной и надежной виртуальной вычислительной среды. Защита обмена данными между виртуальными средами обеспечивается посредством контроля доступа к данным пользователей, входящих в состав выделенных групп с необходимыми правами доступа.
- **Прозрачность:** соблюдение норм и обеспечение прозрачности в виртуальных и облачных ЦОД является важнейшей задачей. Заказчики хотели бы работать в виртуальной среде с теми же средствами контроля, что и в физической среде. Детальная прозрачность является необходимым предварительным условием соблюдения внутренних, отраслевых и государственных стандартов.
- **Проблемы виртуализации серверов.** Решение VMware vMotion обеспечивает перемещение виртуальных машин между физическими портами, заданная сетевая политика должна следовать за виртуальной машиной. Администраторам необходима возможность анализа и применения политик сетевой безопасности к локально коммутируемому трафику. Администраторы должны поддерживать разделение функциональных обязанностей, одновременно обеспечивая бесперебойность эксплуатации. Организациям необходимо решение, независимое от виртуальных сетей, для снижения сложности и повышения возможности масштабирования.

## Подход Cisco к созданию защищенных ЦОД

**В.** О чем нужно подумать сначала при изучении безопасного перехода к виртуальной среде и к облаку?

**О.** В этом случае проблемы безопасности решаются на уровнях технологии и бизнеса. Организациям необходимо включить меры безопасности в общий процесс планирования работы ЦОД и облачных вычислений с первого дня, введя их в состав корпоративной культуры управления. При выборе сроков и объектов для виртуализации и переходу к облачной среде заказчикам надо оценить свои планы с точки зрения требований бизнеса, изучив цели, процессы и приложения. Необходимо выстроить равновесие между целями бизнеса, факторами риска, требованиями и ограничениями архитектуры. Организациям нужен стратегический план внедрения средств безопасности в виртуальную и облачную архитектуру с одновременным сохранением гибкости и устойчивости. После внедрения решения по обеспечению безопасности для такой архитектуры важно обеспечить соответствие процессов учета и совершенствования изменяющимся угрозам и развивающимся технологиям.

**В.** Как Cisco создает защищенный ЦОД?

**О.** Решения Cisco для защищенного ЦОД - это полный набор проверенных функций, которые, не влияя на важные для бизнеса сервисы и приложения, обеспечивают гибкость интеграции со сложными распределенными сетями при предоставлении возможности масштабирования и надежности. Продукты Cisco в области безопасности полностью интегрированы в архитектуру Cisco Unified Data Center и прошли комплексные испытания в условиях, моделирующих работу инфраструктуры заказчиков. Совместное использование рекомендованных дизайнов Cisco и архитектуры Cisco, охватывающей сеть, вычисления и средства обеспечения безопасности, позволяет выполнить развертывание решений и сервисов надежно и с предсказуемыми последствиями. Кроме того, такие проверенные решения позволяют инфраструктуре развиваться вместе с потребностями заказчика.

**В.** Каковы основные цели и требования для ЦОД в отношении безопасности?

**О.** Решения Cisco для защищенного ЦОД обеспечивают **сегментацию** сети, вычислений и виртуальных границ в рамках политики, учитывающей особенности функций, устройств и организации. И, наконец, они предоставляют постоянный доступ к сетевым ресурсам и приложениям. Они **блокируют** внешние и внутренние **угрозы** на границе ЦОД, в выделенных зонах, а также угрозы для приложений, в соответствии с внедренными четко определенными политиками. При этом достигается **прозрачность** элементов и информационных потоков в сети, что позволяет обеспечить соблюдение политики вне зависимости от модели развертывания.

**В.** Каковы требования в области архитектуры для решений по обеспечению безопасности виртуализированных и облачных инфраструктур?

**О.** Решение должно отвечать следующим требованиям в области архитектуры:

- **Логическое разделение:** средства защиты устанавливаются в рамках логических единиц (физических и виртуальных элементов инфраструктуры).
- **Единство политики:** важно, чтобы политика в области безопасности одинаково работала и для физической, и для виртуализированной среды.
- **Автоматизация:** в облачной вычислительной среде с динамическим использованием общих ресурсов, действуют два требования - виртуальные машины вводятся и перемещаются в автоматическом режиме, политика безопасности перемещается вместе с ними.
- **Аутентификация и контроль доступа:** при доступности облачных сервисов в любое время и в любом месте необходимы четкие политики безопасности для контроля доступа пользователей к ним.

- **Возможность масштабирования и производительность:** внедрение виртуальных и облачных вычислений потребует надежной поддержки больших нагрузок и вспомогательной инфраструктуры, например, виртуальных машин высокой плотности, а также соединений между несколькими ЦОД и мобильности рабочих нагрузок. В соответствии с этим необходима возможность масштабирования межсетевых экранов и средств предотвращения вторжения, чтобы они не стали узким местом для всей системы.

## Обеспечение безопасности виртуальной и частной облачной инфраструктуры

**В.** Как решения для защищенных ЦОД Cisco помогают удовлетворить требованиям к архитектуре физической, виртуальной и многоклиентской среды?

**О.** В решениях Cisco для защищенных ЦОД учтены многие вопросы, касающиеся архитектуры.

**Для физической среды**

- В многофункциональном устройстве обеспечения безопасности Cisco ASA 5585-X реализовано ведущее в отрасли решение MultiScale™, обеспечивающее высокопроизводительную обработку соединений, большое число одновременных сессий, высокую пропускную способность и различные защитные сервисы для исключительной гибкости в работе.
- Сенсоры Cisco IPS 4500 были специально разработаны для использования в ЦОД. Они производят проверку трафика с аппаратным ускорением, обеспечивая производительность, соответствующую реальным условиям эксплуатации, высокую плотность портов и энергетическую эффективность в расширяемом шасси, рассчитанном на будущий рост и защиту инвестиций. Малые размеры и низкое потребление энергии делают сенсоры Cisco IPS 4500 идеальными для ЦОД, предъявляющих жесткие требования к свободному месту.
- Межсетевой экран уровня приложений Cisco ASA CX можно развертывать в ЦОД в качестве межсетевого экрана для подразделений. С помощью ASA CX можно идентифицировать и допускать или не допускать использования внешних (посторонних) серверов в сети подразделения.
- ПО Cisco ASA версии 9.0 для платформы Cisco ASA поддерживает устройства различных размеров, включая широкий диапазон автономных устройств, аппаратных блейд-модулей, которые интегрируются с существующей сетевой инфраструктурой, а также программное обеспечение для защиты общедоступных и частных облаков. В данной версии ПО ASA поддерживается возможностью объединения до 8 устройств Cisco ASA 5585-X или 5580 в единый кластер; интеграция с облачным сервисом безопасности 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 использование технологии меток групп безопасности (SGTs) для решения Cisco TrustSec, что обеспечивает наиболее полную интеграцию средств защиты непосредственно в сеть для расширения политик, созданных 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 распространением соответствующих политик безопасности по всей инфраструктуре ЦОД. Такая классификация использует метки групп безопасности (Security Group Tags, SGTs) для формирования решений о допуске к ЦОД или отказе от допуска на основе интеллектуальной политики. Кроме того, эта технология позволяет снизить стоимость владения системой за счет автоматизации разработки правил межсетевого экрана, и снижения уровня сложности при организации контроля доступа.
- Cisco Security Manager 4.3 - это комплексное решение для управления, обеспечивающее постоянное соблюдение политик, быстрое устранение проблем информационной безопасности и подготовку обобщенных отчетов по объекту управления. Данный продукт управляет защитной средой Cisco, обеспечивая прозрачность операций и совместное использование данных с основными инфраструктурными сервисами. И наконец, оно повышает эффективность работы за счет мощного комплекса средств автоматизации.

 

Программная платформа Cisco Security Manager управляет жизненным циклом таких решений, как: многофункциональные устройства безопасности Cisco ASA серии 5500, сенсоры системы предотвращения вторжений Cisco IPS серии 4500, программное обеспечение Cisco AnyConnect™ Secure Mobility Client, маршрутизаторы Cisco и другими.

**Для виртуальной среды**

- Для сред, не требующих разделения клиентов, можно применять многофункциональное устройство Cisco ASA 5585-X, в котором несколько виртуальных межсетевых экранов (технология контекстов) реализованы в одном аппаратном устройстве. Каждый контекст выполняется в изолированном окружении и имеет собственные интерфейсы и политики.
- Технология Cisco Virtual Machine Fabric Extender (VM-FEX), встроенная в архитектуру системы унифицированных вычислений Cisco (Cisco UCS®), объединяет работу с виртуальными и физическими сетями в рамках единой инфраструктуры. Вместе с решением VMware's vMotion, технология Cisco VM-FEX позволяет перемещать сетевые политики одновременно с перемещением виртуальных машин на новые физические или виртуальные устройства. Объединение мультиконтекстного межсетевого экрана ASA 5585-X с устройством Cisco IPS 4500 и технологией VM-FEX предлагает комплексное решение обеспечения безопасности в виртуальных средах, не требующих высоко масштабируемого разделения клиентских ресурсов.

Если виртуальная среда требует расширенных возможностей гибкости и масштабирования, а также более гибких средств обеспечения безопасности на уровне клиентов, подразделений и зон, можно использовать облачный межсетевой экран Cisco ASA 1000V и виртуальный шлюз безопасности Cisco (VSG). Такое решение интегрируется с виртуальным коммутатором Cisco Nexus® 1000V.

- 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 программируемых сетей Software Defined Networks (SDN).
- Программный виртуальный шлюз безопасности Cisco Virtual Gateway, встраиваемый в виртуальный коммутатор Cisco Nexus® 1000V позволяет создавать большое число сетевых зон с контролем присутствия виртуальных машин. Это обеспечивает детальную безопасность при контакте между виртуальными машинами в пределах контролируемых зон. При этом возможно полное логическое разделение различных серверов, сервисов и приложений, работающих на виртуальных машинах разных пользователей.
- Облачный межсетевой экран Cisco Nexus 1000V позволяет создавать границы зон отдельных пользователей с помощью виртуальных сетей. МСЭ, реализует поддержку протокола DHCP, функционал преобразования сетевых адресов (NAT) и инспектирование протоколов. Для данного продукта предусмотрена интеграция с виртуальным коммутатором для улучшения гибкости при развертывании. По умолчанию, Cisco ASA 1000V функционирует в режиме шлюза, защищающего пользователя от сетевых атак.
- 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 на базе политик с использованием шаблонов и профилей безопасности. Также обеспечивается повышение гибкости управления благодаря интерфейсу API XML, поддерживающему интеграцию со сторонними средствами управления. Центр VNMC предоставляет администраторам средств обеспечения безопасности возможность раздельного управления политиками безопасности приложениями, серверами и сетями в целях обеспечения соответствия нормам.

## Виртуализация и работа с облачными средами

**В.** Какие сервисы предусмотрены у Cisco для виртуализации и работы с облачными средами?

**О.** Cisco предлагает услуги профессиональной технической поддержки для достижения заказчиками успеха в процессах планирования, построения защищенных ЦОД и облачных сред, а также управления ими при одновременном обеспечении безопасности таких инфраструктур. Вне зависимости от решаемой задачи (безопасное соединение различных объектов или физических и виртуальных сред с большим числом пользователей, обеспечение защищенного доступа к рабочим приложениям и данным с любого устройства, защита информации, в том числе личного характера, или обеспечение совместной работы в любом месте), Cisco поможет сформировать политики, выстроить управление, обеспечить соблюдение норм и требований безопасности в рамках инфраструктуры ЦОД, внутри облачных сред и между ними для защиты бизнеса заказчика.

Для получения дополнительных сведений об услугах в области безопасности посетите web-страницу

Для получения дополнительных сведений об услугах в области ЦОД посетите web-страницу

**В.** Как Cisco помогает построить частную облачную среду и обеспечить ее безопасность?

**О.** ПО Cisco для интеллектуальной автоматизации облачных сред позволяет автоматизировать и организовать создание таких сред и управление ими в виртуальном ЦОД. Система позволяет реализовать автоматизированные процессы по выделению виртуальных машин по требованию и закреплению их за разными сетями, политики безопасности в которых уже определены решениями Cisco ASA, ASA 1000V и VSG. Кроме того, центр VNMC (управляющий решениями VSG и ASA 1000V) может использовать интерфейс XML API для интеграции со средствами управления и администрирования других разработчиков для дальнейшей автоматизации политик безопасности в управляемой частной облачной среде.

## Преимущества Cisco по сравнению с конкурентами

**В.** В чем заключаются преимущества Cisco?

**О.**

- Cisco - признанный лидер в области средств обеспечения безопасности, - предлагает самый высокоскоростной межсетевой экран с возможностью масштабирования в соответствии с новыми потребностями ЦОД с использованием решения ASA 5585-X.
- Архитектура Cisco обеспечивает гибкость в обеспечении безопасности архитектур, соединяющих виртуальные машины и многочисленных пользователей (при развертывании внутри и на границах зон) за счет решений Cisco VSG и ASA 1000V.
- Архитектура Cisco использует единые политики и принципы управления в физической, виртуальной и облачной средах, средства обеспечения безопасности с функциями, независящими от размера
- Архитектура Cisco обеспечивает перемещение политик внутри сети, используя такие инновационные технологии, как VM-Fex, решение Cisco для виртуализации транспорта (OTV), протокол Locator/ID Separation Protocol (LISP) и vPath
- Архитектура Cisco предлагает решения, рассчитанные на разные типы контекста, и средства кластеризации для масштабирования виртуальных сред
- Компания Cisco интегрирует продукты в архитектуру Unified Data Center, только после тщательного тестирования

**В.** Что такое виртулизированный мультисервисный ЦОД Cisco (VMDC)?

**О.** В первую очередь, VMDC - это проверенная архитектура Cisco. Cisco предусмотрены интенсивные испытания решений для выполнения требований надежности и устойчивости в работе при обеспечении безопасности физического или виртуального ЦОД, а также частной облачной среды.

Архитектура VMDC обеспечивает защиту унифицированного ЦОД, в котором находятся критически важные приложения и конфиденциальные данные. 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 задач интеграции вводятся дополнительные уровни управляющего программного обеспечения, унифицированный ЦОД Cisco изначально разработан специально для виртуализации, автоматизации задач и предоставления ресурсов по запросу из общих пулов инфраструктуры для физических и виртуальных среда. В случае использования архитектуры Cisco ИТ больше не является центром затрат, а становится направлением по предоставлению сервисов для получения конкурентных преимуществ.

С унифицированным ЦОД тесно интегрированы средства управления безопасностью, включенные в лидирующий в отрасли межсетевой экран, функционал VPN, комплекс 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.

## Дополнительные вопросы

**В.** Где можно найти дополнительные сведения?

**О.** Защищенный центр обработки данных

Защищенный центр обработки данных VMDC

Безопасная многоклиентская среда

Архитектура Унифицированного центра обработки данных Cisco

Многофункциональное устройство обеспечения безопасности Cisco ASA 5585-X

Система предотвращения вторжений Cisco IPS 4500

Виртуальный межсетевой экран Cisco ASA 1000V

Виртуальный коммутатор Cisco Nexus 1000V.

Виртуальный шлюз безопасности Cisco Virtual Gateway

Центр управления виртуальными сетями Cisco

Cisco ASA CX

Решение Cisco TrustSec

Система управления Cisco Security Manager

**Головной офис в США**
Cisco Systems, Inc.
Сан-Хосе, штат Калифорния, США

**Центральное представительство в Азиатско-Тихоокеанском регионе**
Cisco Systems (USA) Pte. Ltd.
Сингапур

**Центральное представительство в Европе**
Cisco Systems International BV Амстердам, Нидерланды

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 C67-714776-00 09/12

 