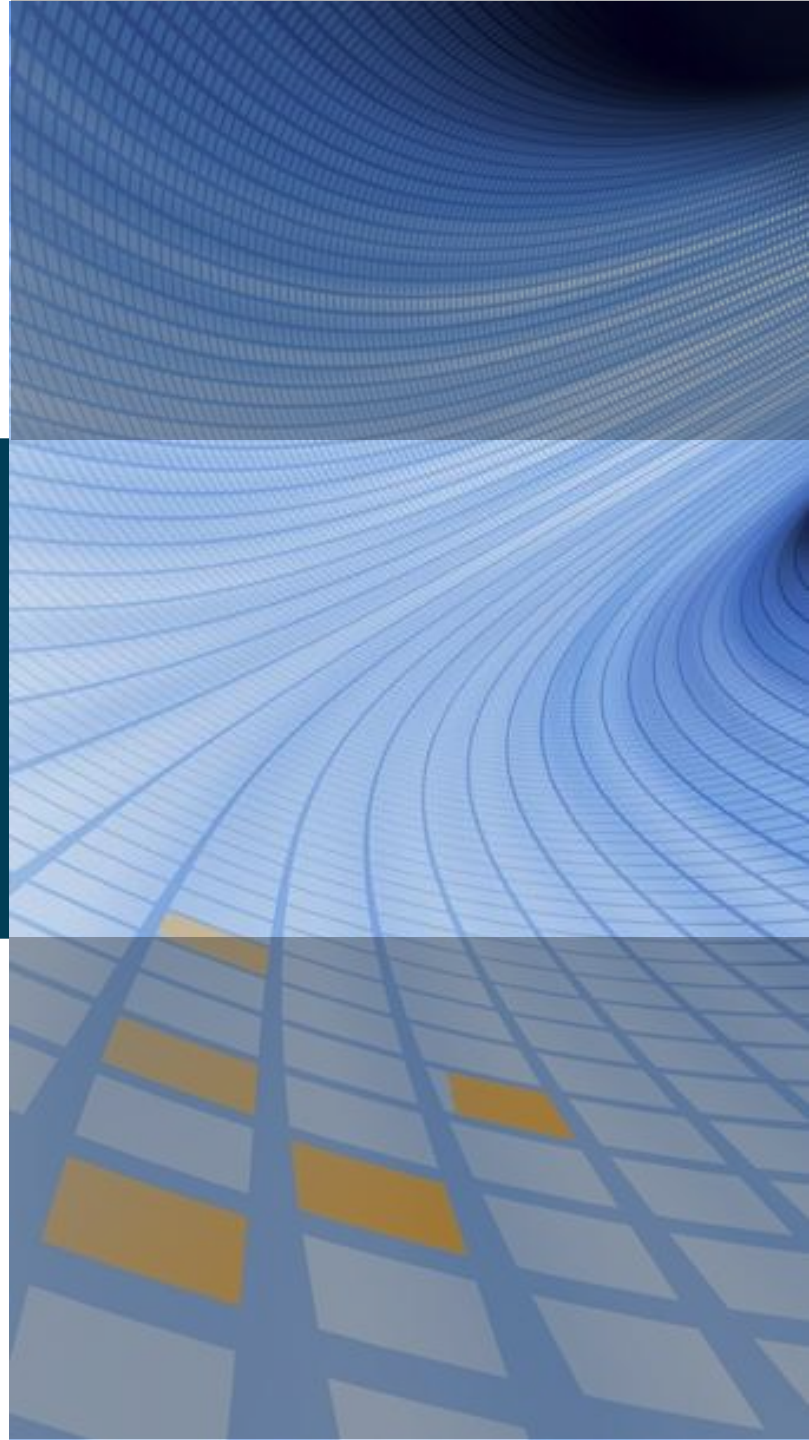
Защищенный центр обработки данных без границ



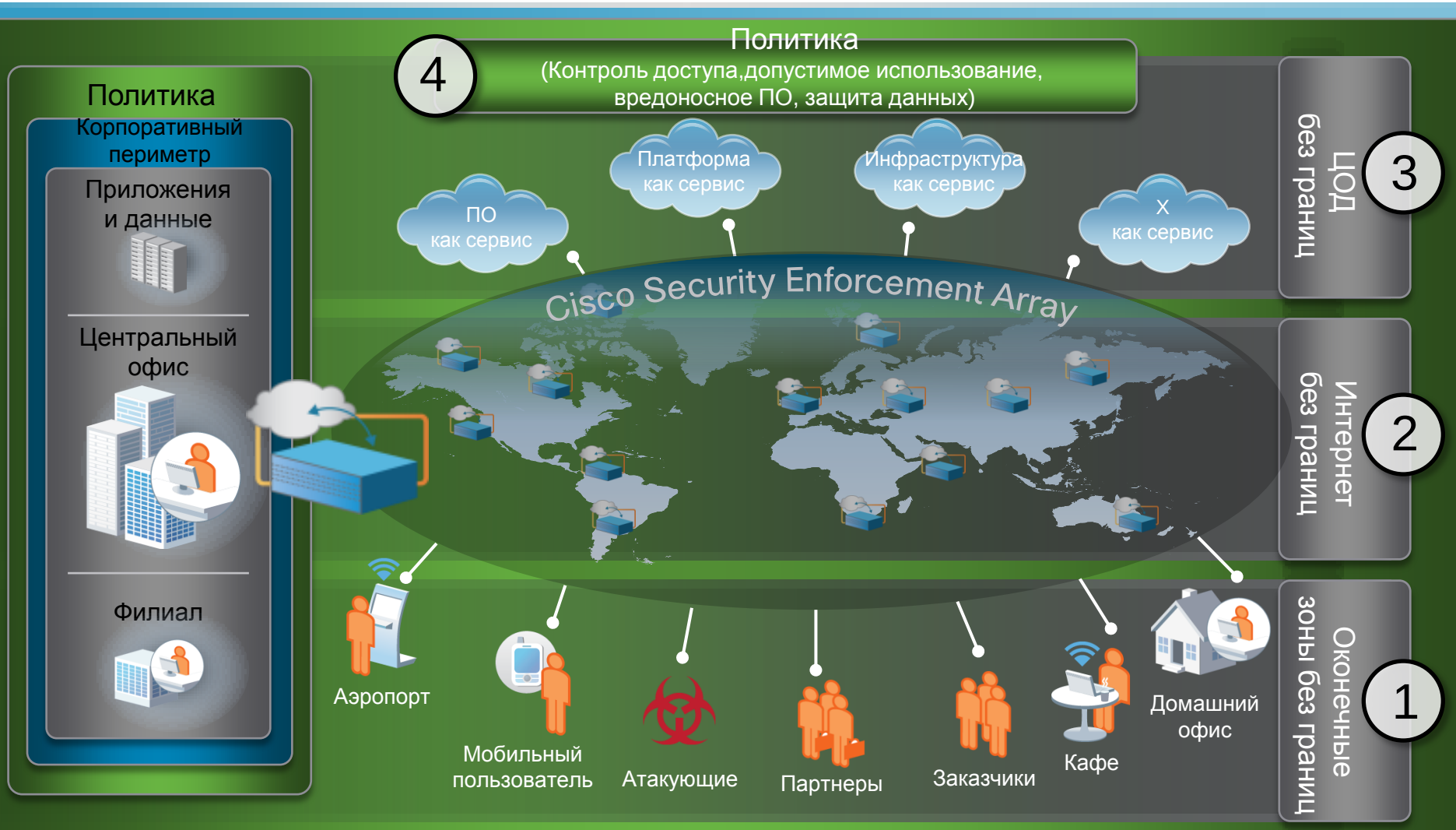
Оговорка о намерениях

Многие из продуктов и функций, упомянутых в данной презентации, находятся на различных стадиях разработки. План их выпуска может изменяться по собственному усмотрению корпорации Cisco, при этом Cisco не будет нести ответственность за задержки с выпуском или отказ от выпуск продуктов и функций, описанных в настоящей презентации.

Основные предпосылки

1. Давление, оказываемое на современные ЦОД, приводит к пересмотру границ ЦОД
2. "Без границ" не значит "без периметра" — напротив, это значит "динамический, интеллектуальный, контекстно-зависимый периметр"
3. Масштабируемость и простота, открытость, виртуализация и распределенные сетевые сервисы — основные элементы архитектуры защищенного ЦОД "без границ"

Архитектура системы безопасности сети без границ



Современный ЦОД

Давление со всех сторон

Эволюция ЦОД

Новые тенденции влияют на архитектуру ЦОД

Задачи по созданию защищенного ЦОД без границ

Масштабируемость и простота

- Производительность сервисов безопасности
- Простота развертывания
- Масштабируемые процедуры эксплуатации

Открытость

- Сегментация и контроль доступа
- Авторизация с учетом контекста для пользователей и приложений
- Сквозная поддержка механизмов идентификации

Виртуализация

- Обеспечение связности виртуальной сети
- Уровень защищенного доступа к виртуальным ресурсам
- Гибридный режим: физические и виртуальные ресурсы

Распределенные сервисы

- Формирование доверительных отношений в рамках инфраструктуры
- Защищенные подключения к распределенным сервисам
- Эксплуатация физических, виртуальных и распределенных ресурсов

Концепция ЦОД без границ: простота и масштабируемость

Масштабируемость, гибкость и простота

Безопасность и производительность

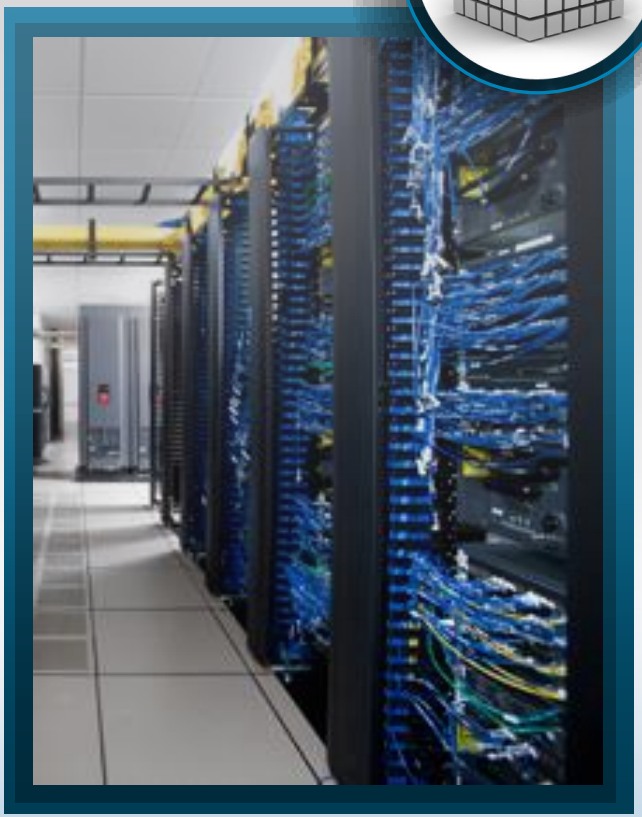
- Не только пропускная способность
- Возможности настройки, количество подключений, количество правил

Гибкость для упрощения развертывания

- Автономные решения и решения для интеграции в сетевые устройства
- Устройства, модули, виртуальные компоненты и элементы распределенных сетевых сервисов

Согласованность сервисов независимо от форм-фактора решения

- Согласованные функциональные возможности и процедуры эксплуатации

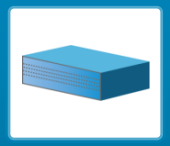


Presentation_ID © 2009 Cisco Systems, Inc. All rights reserved.

Cisco Confidential

Гибкость сегодня, масштабируемость для решения будущих задач

Согласованные функциональные возможности
обеспечивают согласованный набор сервисов и простоту эксплуатации



Устройства

ASA 5580

IPS 4270

План
“Spyker”
10–15 Гбит/с, МСЭ и IPS в шасси 2RU

Модули

FWSM

IDSM2

План:
“Bennu” - 15 Гбит/с, Cat 6500
“Osiris” - 40 Гбит/с, Nexus 7000 –

Виртуальные компоненты

Nexus 1000v

250 вирт. контекстов

План:
1000 виртуальных контекстов
Виртуальный МСЭ – план

Распределен-ные сетевые сервисы

В разработке:

расширение средств безопасности ЦОД на платформы распределенных сетевых сервисов

Кластеризация для масштабирования - план

9

Концепция ЦОД без границ : открытость

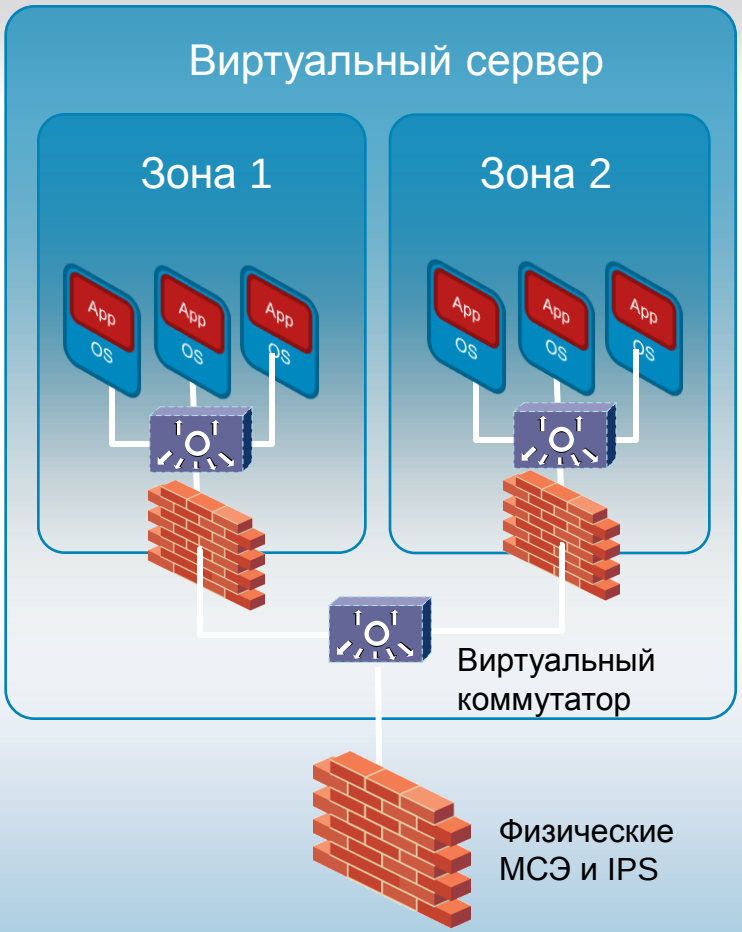
Предоставление доступа при сохранении контроля

	Вчера	Сегодня	Потребности
Кто?	Все пользователи в корпоративной сети	Внутренние и внешние пользователи, виртуальные ПК	Реализация политик с учетом сведений о пользователе
Что?	Простые приложения в ЦОД	Комплексные приложения у заказчика и в рамках распределенных сетевых сервисов	Реализация политик с учетом сведений о приложении
Как?	Надежный периметр; открытая внутренняя среда	Несколько зон рисков и приложений	Сегментация на зоны доверия

Защищенные открытые ЦОД Cisco

Концепция ЦОД без границ: виртуализация

Защита виртуальной среды



Контроль виртуальной сети

- Контроль трафика между ВМ

Безопасность виртуального уровня доступа

- Сохранение контроля за уровнем доступа

Обеспечение выполнения виртуальных политик

- Обеспечение выполнения политик контроля доступа в виртуальной среде
- Выполнение политик в физической и виртуальной средах

Эксплуатация и управление

- Единая среда для управления физической и виртуальной ИТ-инфраструктурами

Согласованное обеспечение выполнения политик

Плавный переход к виртуальной ИТ-инфраструктуре

Физическая реализация

Виртуальная реализация

CSM
Выделение ресурсов, мониторинг, устранение неполадок

Единая среда управления

Уровни 2–4

Nexus 1000v

Контроль трафика между ВМ

Защита на уровне вирт. порта

Поддержка списков ACL

Уровни 4-7

План:
Средства Service Chaining для связи инфраструктур

Виртуальная платформа ИБ ("виртуальный МСЭ") - план

Эксплуатация

Совместная: физической и виртуальной инфраструктур (L2–4)

План:
Совместная: физической и виртуальной инфраструктур (L4–7)

Концепция ЦОД без границ: распределенные сетевые сервисы

Безопасное расширение в среды XaaS

Формирование доверительных отношений

- Защищенная инфраструктура распределенных сетевых сервисов

Защищенные подключения и доступ

- Защищенное увеличение емкости
- Защищенный доступ для пользователей, работающих в офисе, и мобильных пользователей

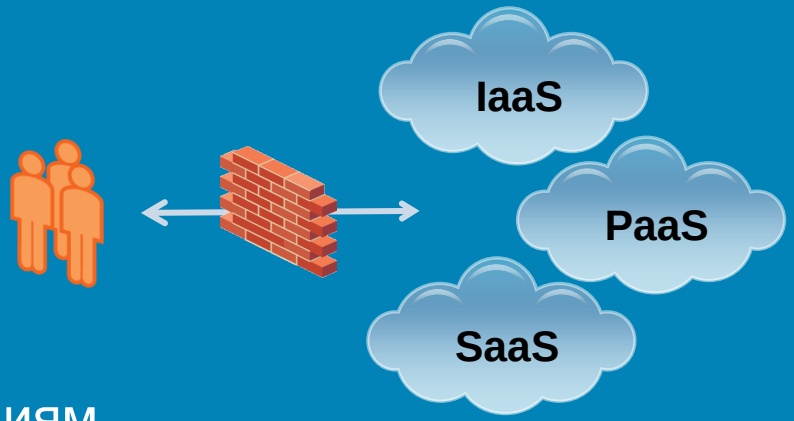
Защищенные приложения на распределенной платформе

- Защита от угроз
- Подтверждение соответствия нормативным требованиям

Могу ли я безопасно использовать сервисы "по запросу"?

Точка зрения корпорации

- Возможность подключения
- Сегментация и безопасность
- Учет мобильности приложений
- Соответствие нормативным требованиям



Точка зрения поставщика распределенных сетевых сервисов

- Доверенная инфраструктура
- Предоставление сервисов безопасности
- Масштабируемая среда для абонентов
- Управление и эксплуатация

Современный ЦОД: сквозная архитектура

Периметр ЦОД и корпоративной сети

Шлюз SaaS в рамках WSA

- Контроль доступа для приложений SaaS

Межсетевой экран

- Глубокая фильтрация входящего трафика

Управление

Уровень сервисов безопасности

Межсетевой экран

- Обеспечение сегментации зон для серверов
- Виртуальные контексты обеспечивают масштабирование

IPS

- Отражение угроз и защита гипервизора

Защищенный уровень доступа к серверам

Сегментация сети

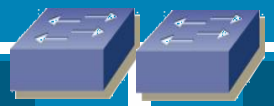
- На зоны (на уровне сервисов)

Связность на виртуальном уровне доступа

- Контроль трафика через виртуальный коммутатор

Безопасность на уровне 2

- Постоянная защита вирт./физич. коммутатора

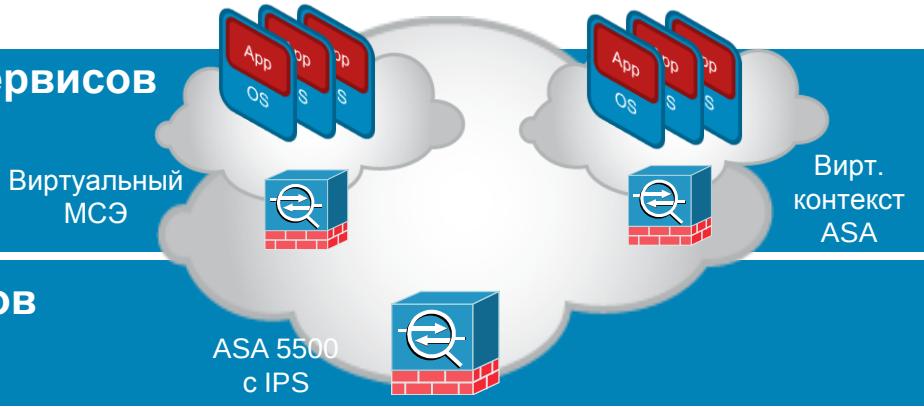


Защищенный ЦОД без границ: архитектура будущего

Уровень защиты распределенных сетевых сервисов

В корпоративной сети или в сети сервисов

- Защита приложений, предоставляемых с помощью сервисов



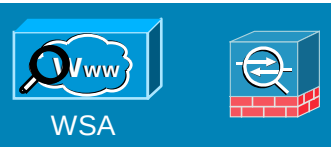
Периметр распределенных сетевых сервисов

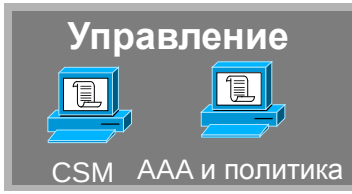
Защита сети поставщика сервисов

Периметр корпоративной сети и ЦОД

Шлюз SaaS – в рамках WSA

МСЭ — интенсивная фильтрация

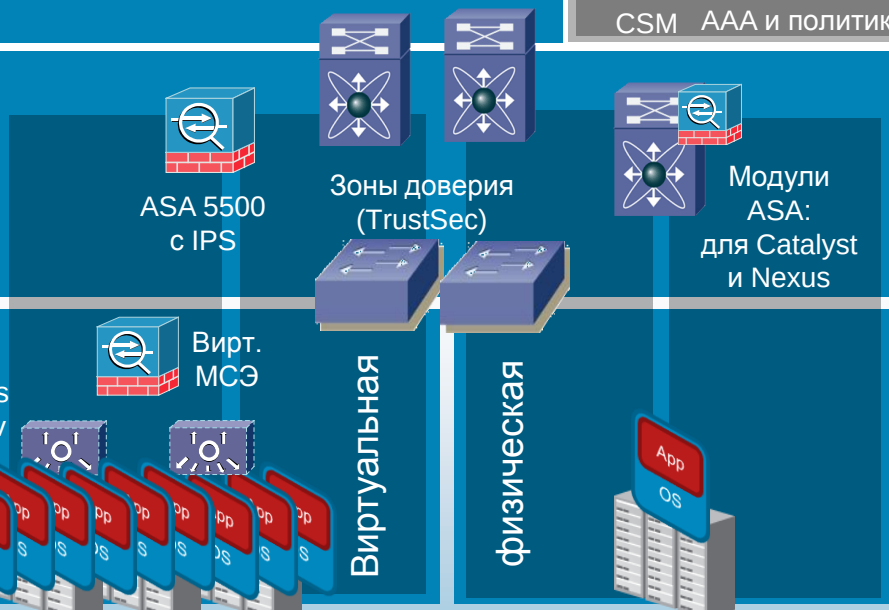




Уровень сервисов безопасности

МСЭ и IPS

- Политики с учетом идентификационных данных
- Service Chaining (связь виртуальной и физической инфраструктуры)



Защищенный виртуальный уровень доступа

Защита виртуальных уровней 2 — 7

- Nexus 1000v и платформа виртуального межсетевого экрана

Защищенный ЦОД без границ: архитектура

Масштабируемость и простота

- Производительность, гибкость и интеграция в сеть

Открытость

- Доступ и контроль доступа

Виртуализация

- Согласованность сервисов и процедур

Распределенные сетевые сервисы

- Гибкость и масштабируемость

Основные результаты

1. Структура ЦОД меняется
   Эти изменения сильно сказываются
   на системе обеспечения безопасности

2. Cisco располагает долговременной стратегией
   создания защищенных ЦОД без границ

3. Обеспечьте соответствие целям заказчика по
   созданию ЦОД, чтобы развивать свой бизнес


CISCO