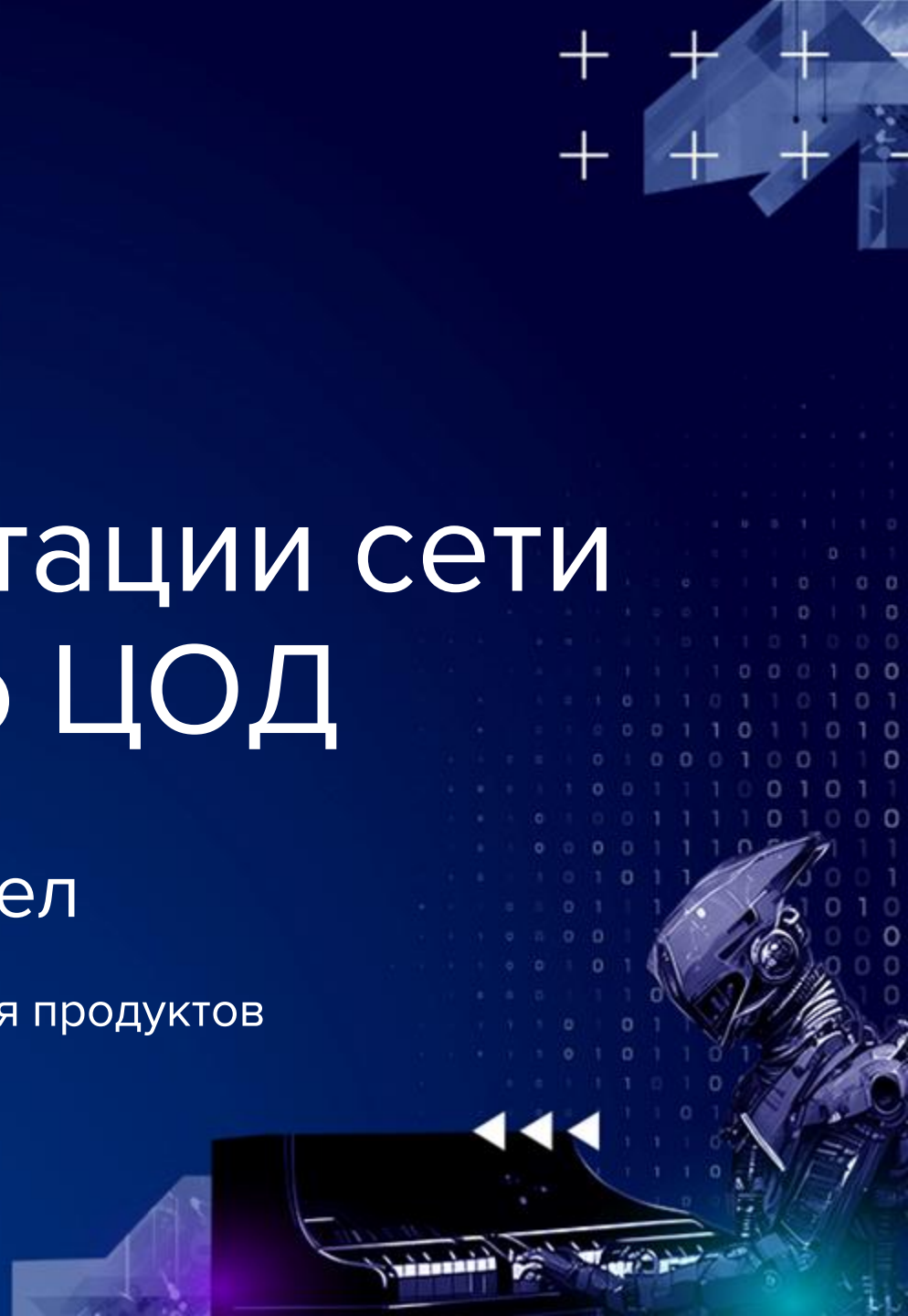
GIS DAYS

Подходы к сегментации сети современного ЦОД

Коростелев Павел

Руководитель отдела продвижения продуктов

Код Безопасности



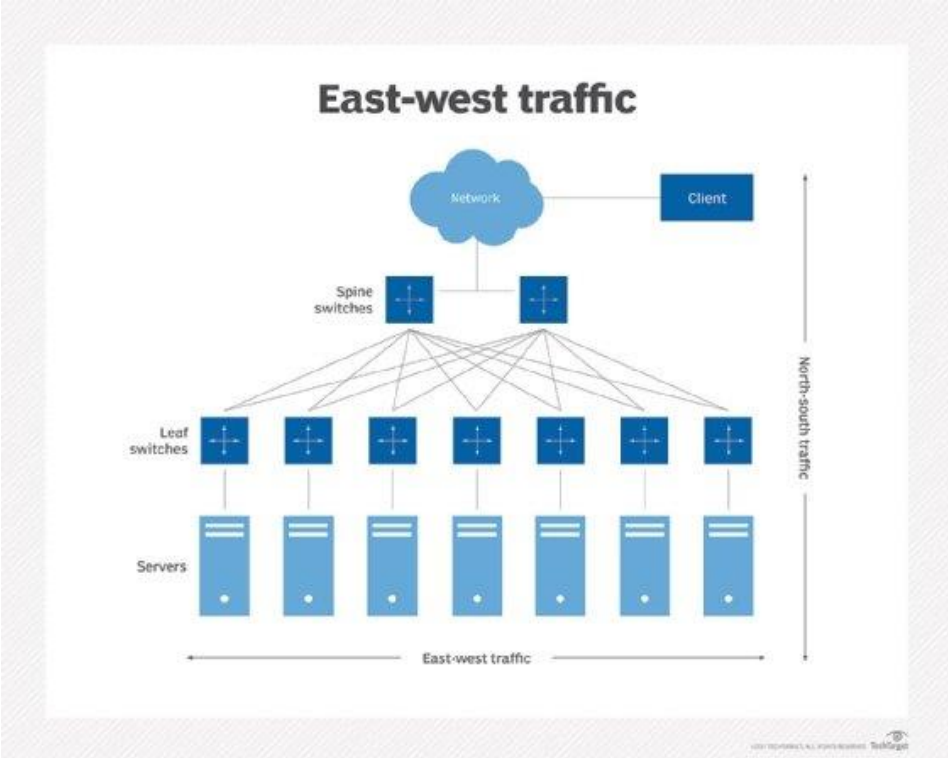
Импортозамещение в сетевой безопасности идет на всех парах

Успешные сценарии:
- Периметровый МЭ
- Территориально-распределенный МЭ
- МЭ для среднего и малого бизнеса

Сложные сценарии:
- Сегментация ЦОД
- Защита АСУ ТП

Нюансы защиты сети ЦОД

- **Два разных паттерна движения трафика**
- **Высокие требования производительности и отказоустойчивости под нагрузкой**
- **Поддержка VXLAN и других сетевых технологий**
- **Переход на отечественную виртуализацию**



Задачи фильтрации трафика для защиты ВМ

Передача трафика внутри виртуальной сети

- Контроль трафика между ВМ разного уровня чувствительности
- Контроль подключений к приложениям
- Контроль трафика по подразделения предприятия

Фильтрация трафика ВМ

- Фильтрация трафика входящего и исходящего от конкретной ВМ

Различные варианты межсетевых экранов для задачи

- Физический МСЭ
- Виртуальный МСЭ
  - Виртуальное устройство
  - МЭ уровня ядра гипервизора

vmware NSX

Использование физических МЭ

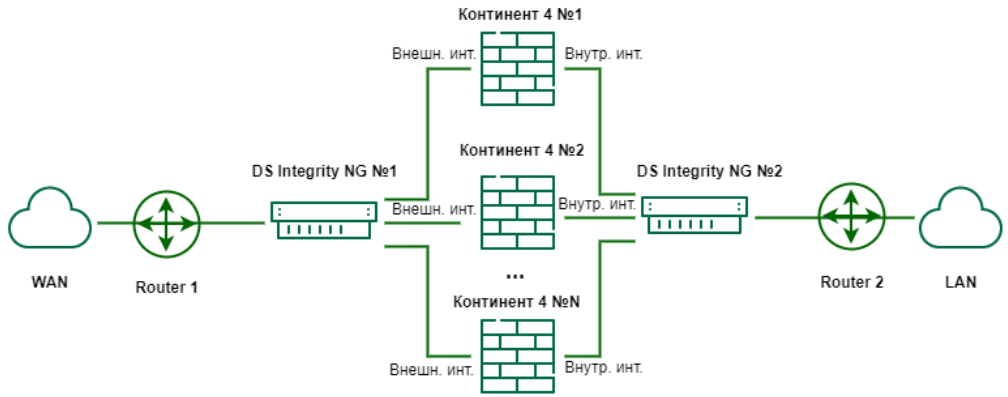
Преимущества:

1. Реализация «Наложенной» безопасности
2. Разделение полномочий

Недостатки:

1. Избыточная сложность конфигурации сети
2. Дополнительные задержки при обработке трафика
3. Отсутствие «коробочных» решений на рынке

Использование физических МЭ



Как происходит:

1. Используется функционал Континент 4 NGFW для фильтрации сетевого трафика с анализом на уровне:
   - Системы предотвращения вторжений
   - Механизмов контроля приложений
   - Контентной фильтрации
2. Используется функционал брокера сетевых пакетов для балансировки трафика на устройства

Использование виртуальных устройств МЭ

Преимущества:

1. Трафик не покидает виртуальную среду
2. Просто развертывается
3. Реализует функции NGFW
4. Стоит дешевле

Недостатки:

1. Нет вертикального масштабирования производительности
2. Нестабильная работа кластера отказоустойчивости
3. Сложности при переезде виртуальной машины на другой хост

Использование МЭ уровня гипервизора

Преимущества:

1. Неограниченная пропускная способность*
2. Прозрачность состояния ВМ, распределенного коммутатора, трафика
3. Мониторинг обоих паттернов трафика

Недостатки:

1. Нет сертифицированных решений от российских вендоров виртуализации
2. Нельзя «приземлить» сервисы NGFW (контроль приложений, IPS, Антивирус)

Рекомендации по выбору для East-West сегментации:

Есть чувствительные к задержкам приложения?

- Проектируем виртуальный МЭ или МЭ уровня гипервизора

Есть высоконагруженные приложения?

- Проектируем МЭ уровня гипервизора

Нужна интеграция с платформой управления виртуализацией (получение имен виртуалок)

- Проектируем МЭ уровня гипервизора

Подробности: NIST 800-125B

www.securitycode.ru

Код Безопасности – Единственный вендор на рынке, реализующий все три варианта сертифицированными средствами

СПАСИБО ЗА ВНИМАНИЕ

p.korostelev@securitycode.ru
www.securitycode.ru
Tg: @Kodnaprovode

КОД безопасности