

Технология безтуннельного шифрования:

Group Encrypted Transport VPN

Константин Павлов

Ведущий преподаватель

pavlovkn@specialist.ru

CCSI

CCIE:RS

CCIE:SEC

Введение в технологию MPLS

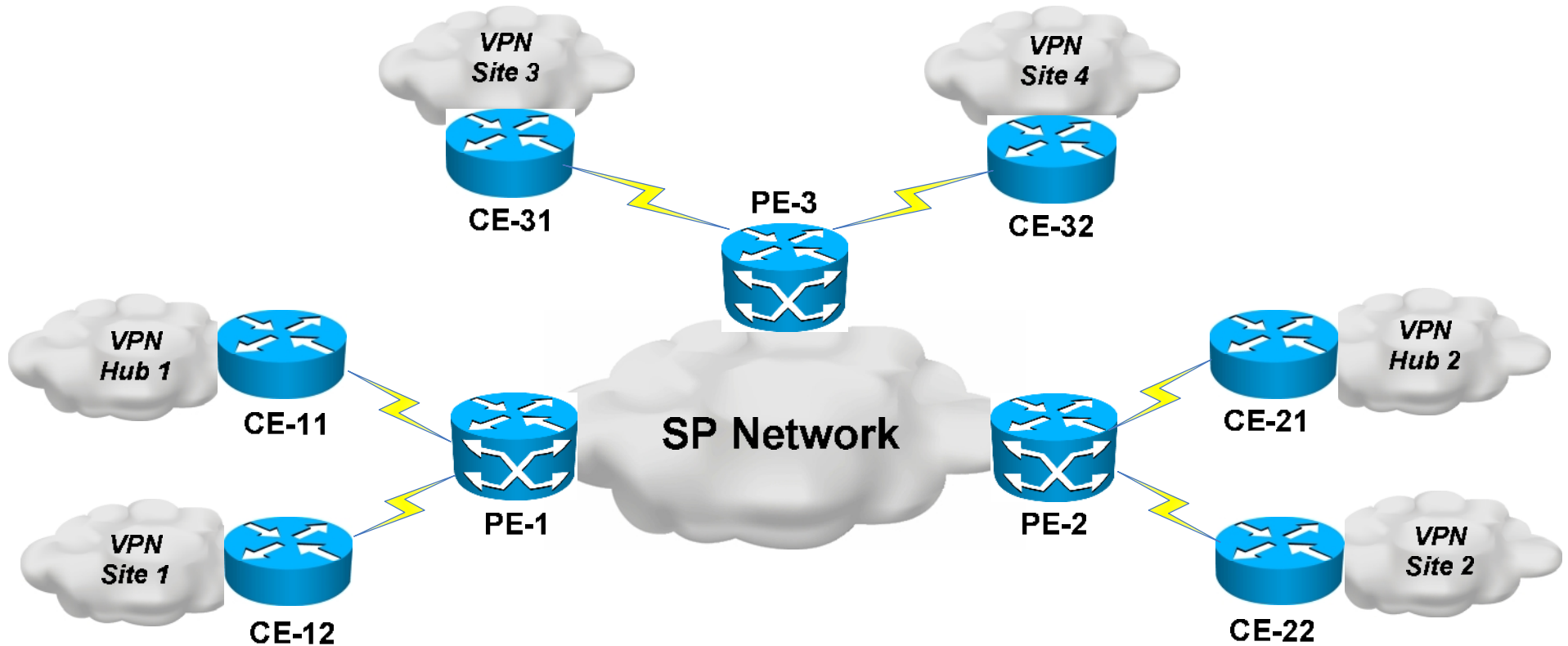
MPLS (label table forms
from routing table)
**Scalability,
Efficiency and Speed**

Switching
(looking L2 and find in mapping table)
Efficiency and speed

Routing
(looking L3 addressing)
Scalability

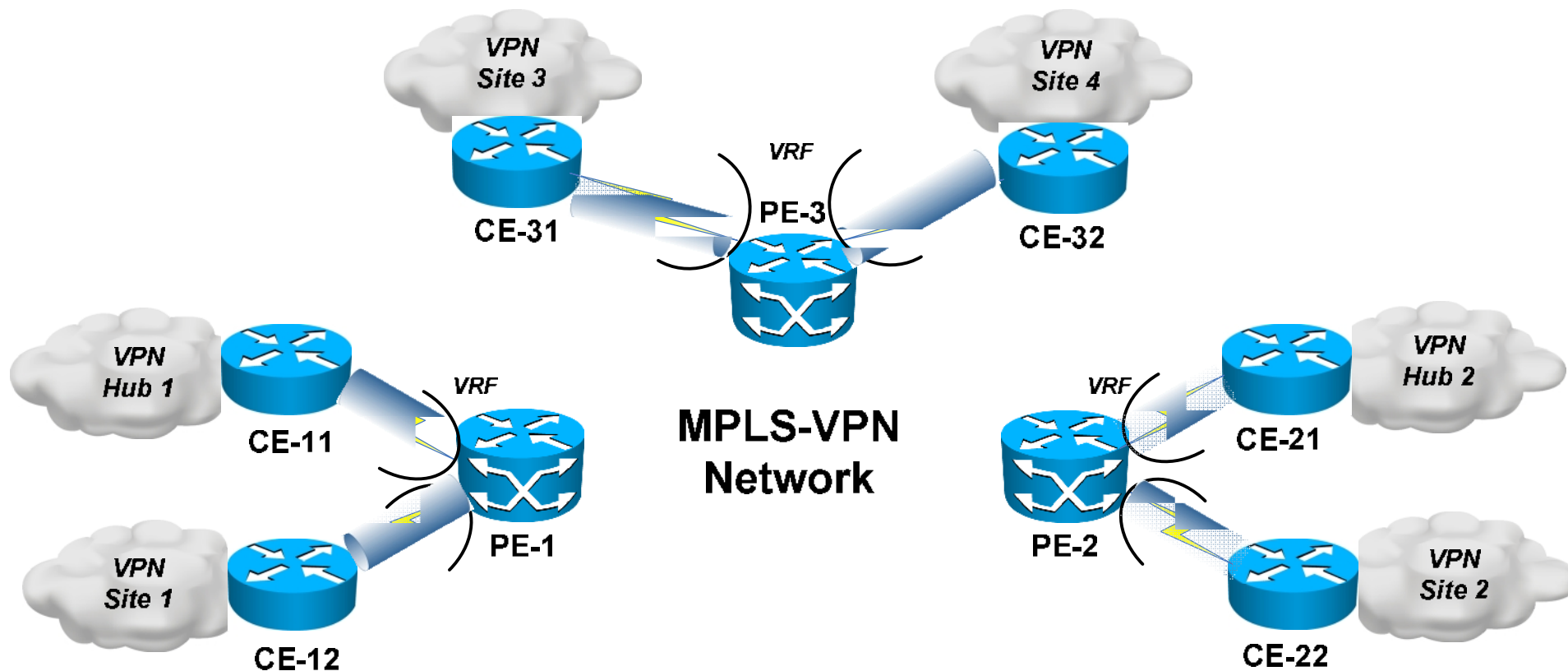
Недостатки существующих решений

www.specialist.ru



- Необходимо реализовать end-to-end шифрование

Недостатки существующих решений: MPLS VPN + IPSec-aware



- Альтернативный вариант – использование DMVPN или Easy VPN на CE-устройствах (недостатки решения)

Сравнение существующих методов VPN

www.specialist.ru

	Easy VPN	DMVPN	Cisco GET VPN
	Туннельные VPN		Безтуннельный VPN
Сетевая инфраструктура	Публичный интернет транспорт	Публичный интернет транспорт	Приватный интернет транспорт
Сетевая топология	Hub-and-Spoke (Клиент-Сеть)	Hub-and-Spoke и Spoke-to-Spoke (Сеть-Сеть)	Все-со-всеми (Сеть-Сеть)
Маршрутизация	Reverse-route injection	Динамическая маршрутизация на туннельных интерфейсах	Динамическая маршрутизация в IP WAN сети
Отказоустойчивость	Stateless hub crypto failover	Модель распространения маршрутов	Модель распространения маршрутов
Топология шифрования	Шифрование точка-точка	Шифрование точка-точка	Групповая защита
Работа Multicast	Не поддерживается	Репликация Multicast со стороны центрального узла (протокол NHRP)	Репликация Multicast в IP WAN сети

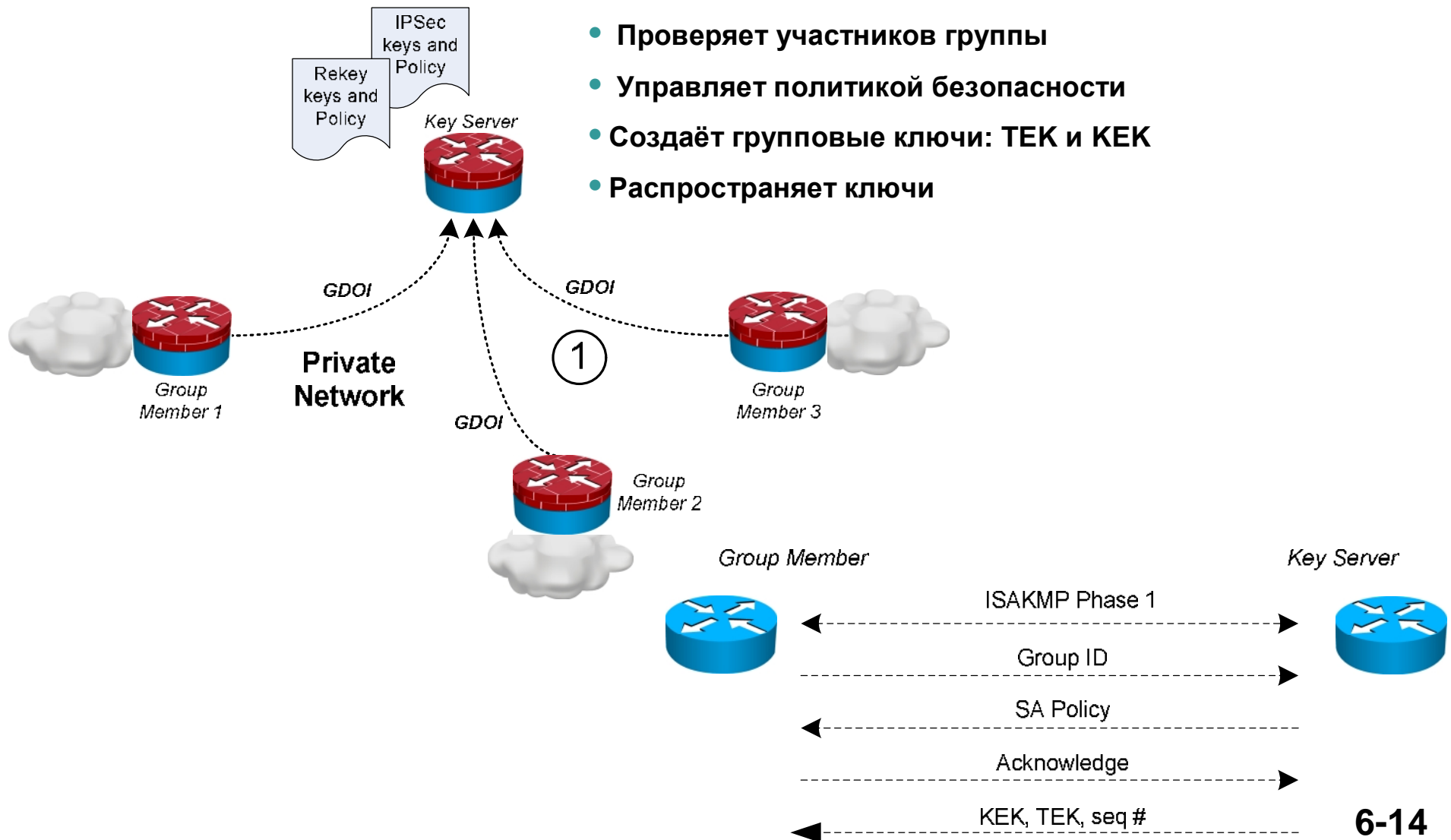
Преимущества внедрения GET VPN

www.specialist.ru

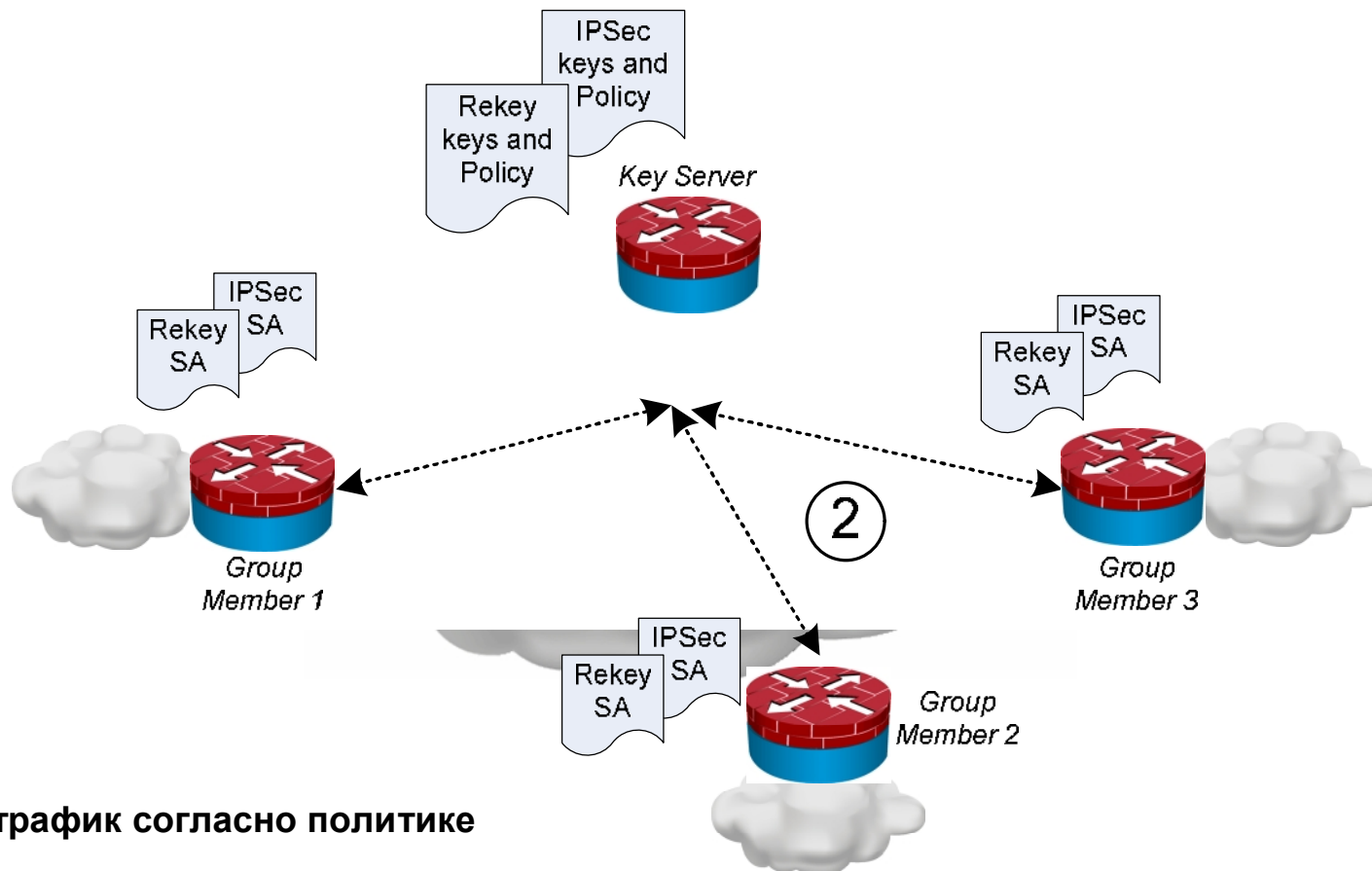
- Упрощает интеграцию модели шифрования в существующую IP WAN сеть
- Упрощает шифрованием на сотнях узлов благодаря концепции «доверенных» групп
- Добавляет масштабируемость и лёгкость управления для сетей any-to-any требованиями связи
- Поддерживает QoS, Multicast и маршрутизацию

Концепция сети GET VPN: Этап 1

- Проверяет участников группы
- Управляет политикой безопасности
- Создаёт групповые ключи: ТЕК и КЕК
- Распространяет ключи



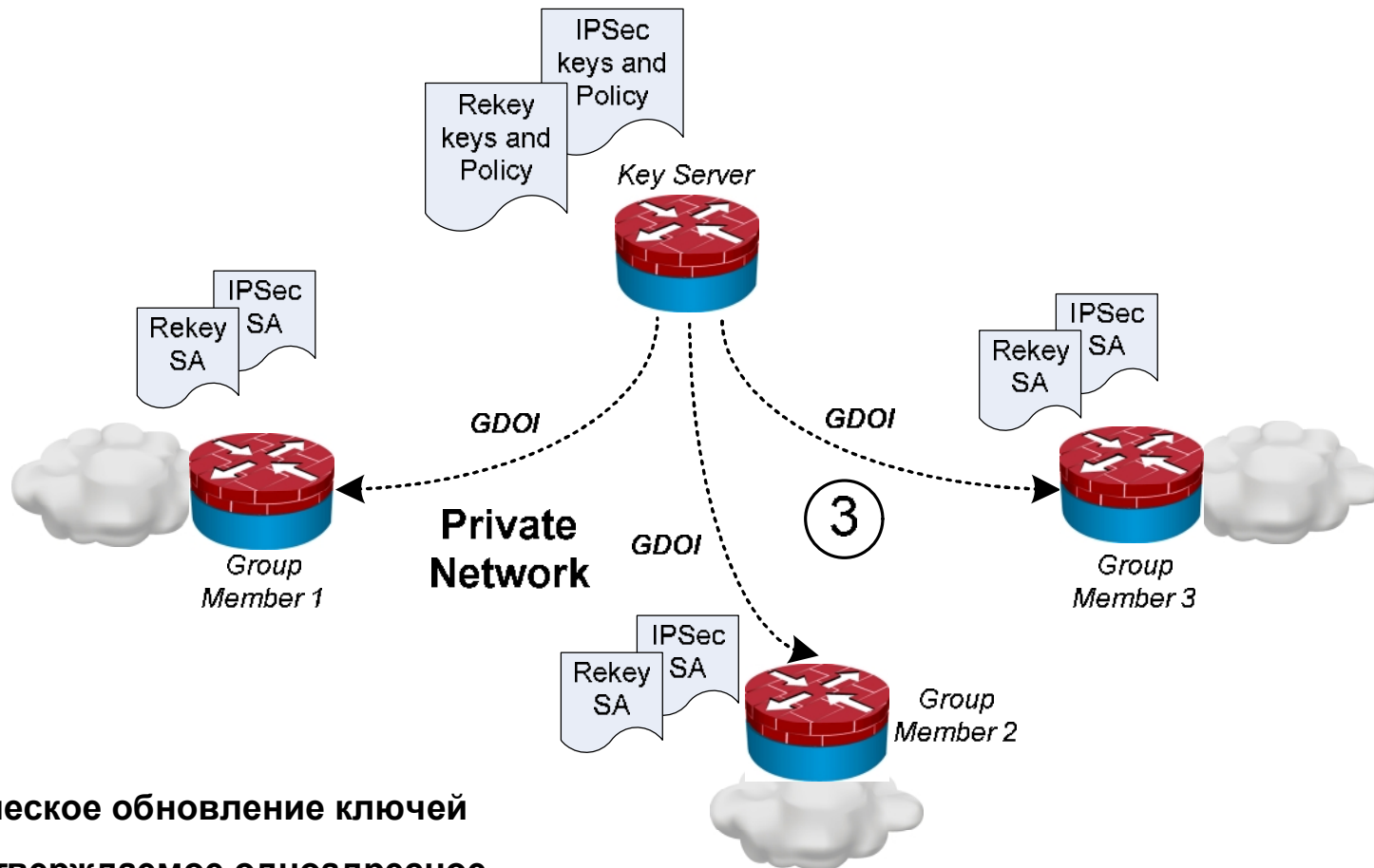
Концепция сети GET VPN: Этап 2



- Шифрует трафик согласно политике
- Маршрутизирует между защищёнными и незащищёнными участками сети
- Участвует в репликации Multicast

Концепция сети GET VPN: Этап 3

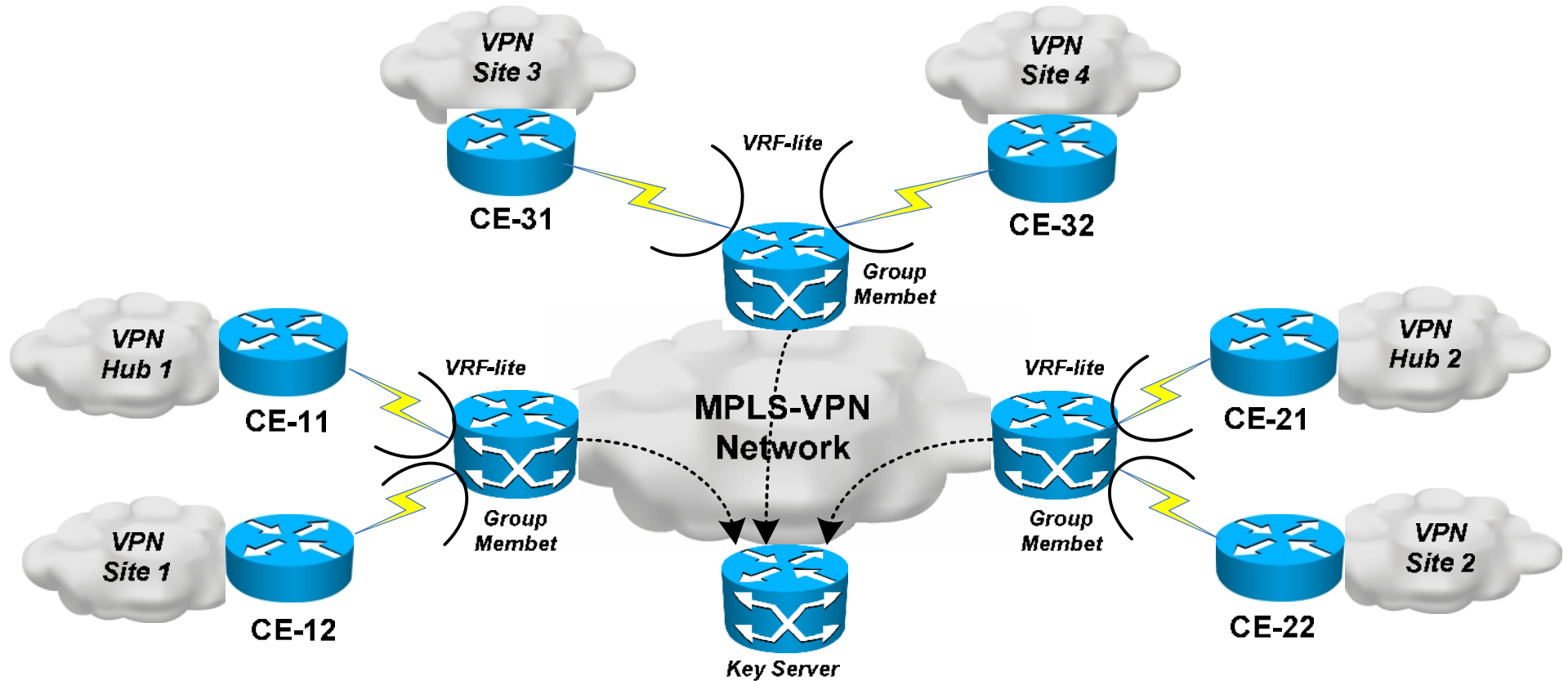
www.specialist.ru



- Периодическое обновление ключей
 - Подтверждаемое одноадресное
 - Неподтверждаемое многоадресное

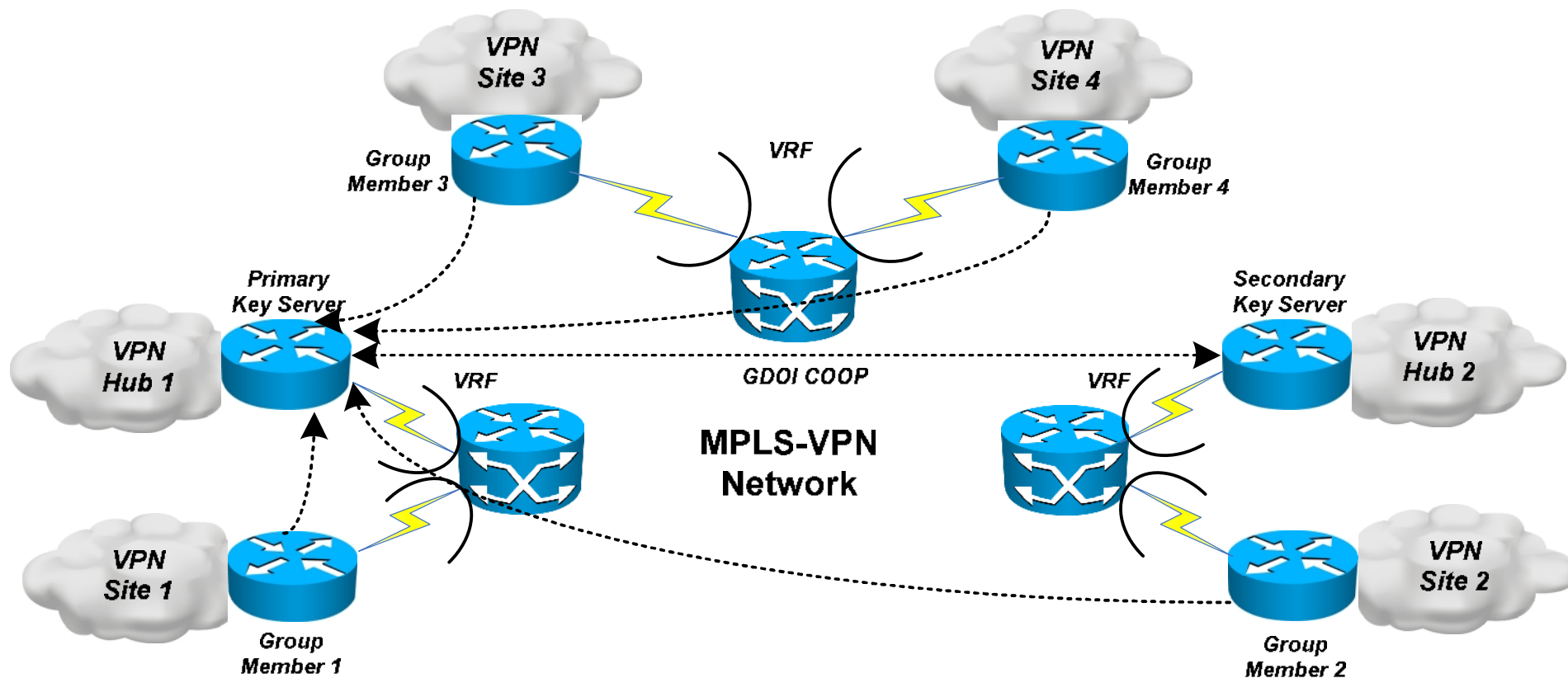
Варианты решений GET VPN: VRF-lite

www.specialist.ru



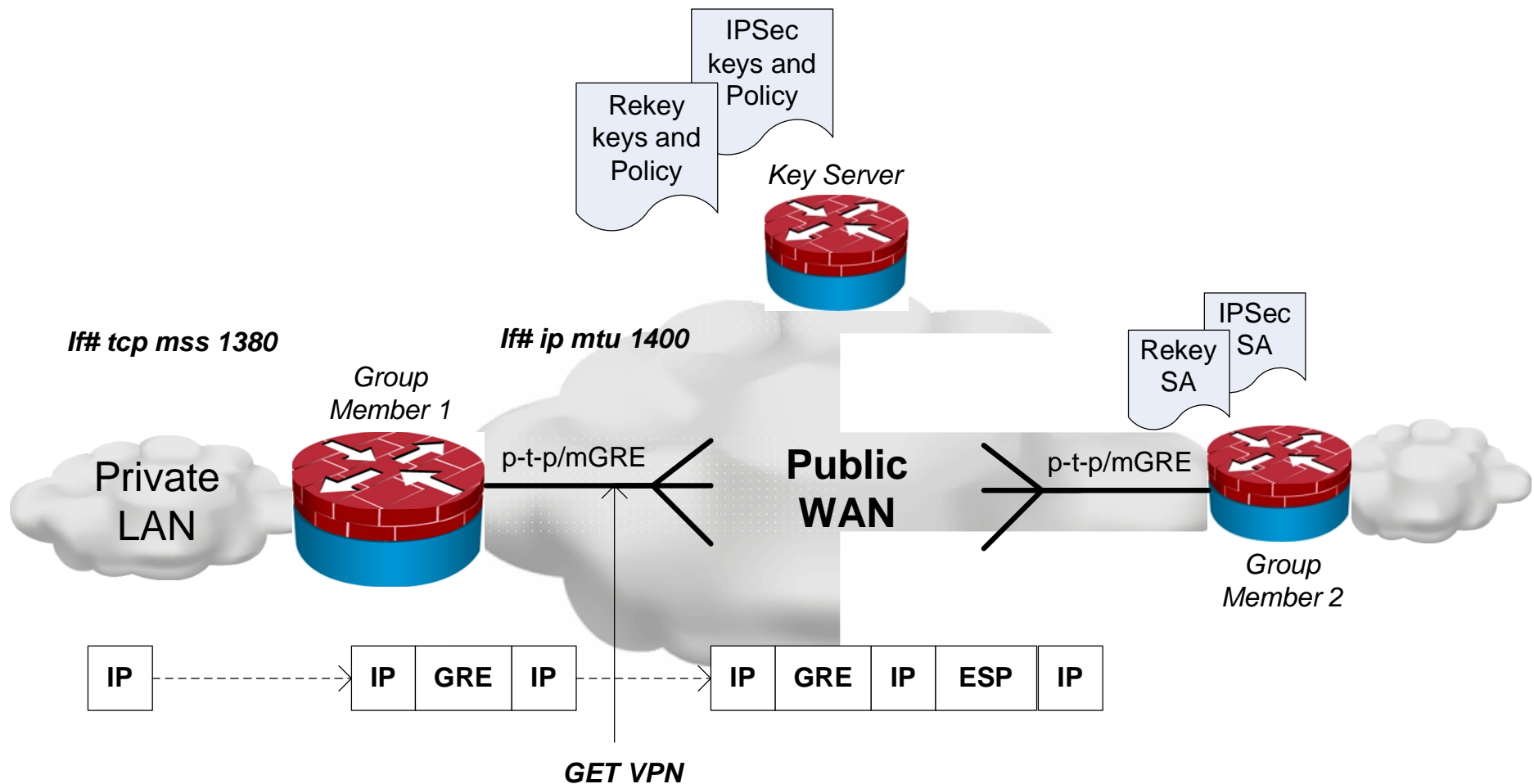
- Нагрузка на шифрование ложится на PE-устройства (поддержка VRF-lite)

Варианты решений GET VPN: защита сетей клиента



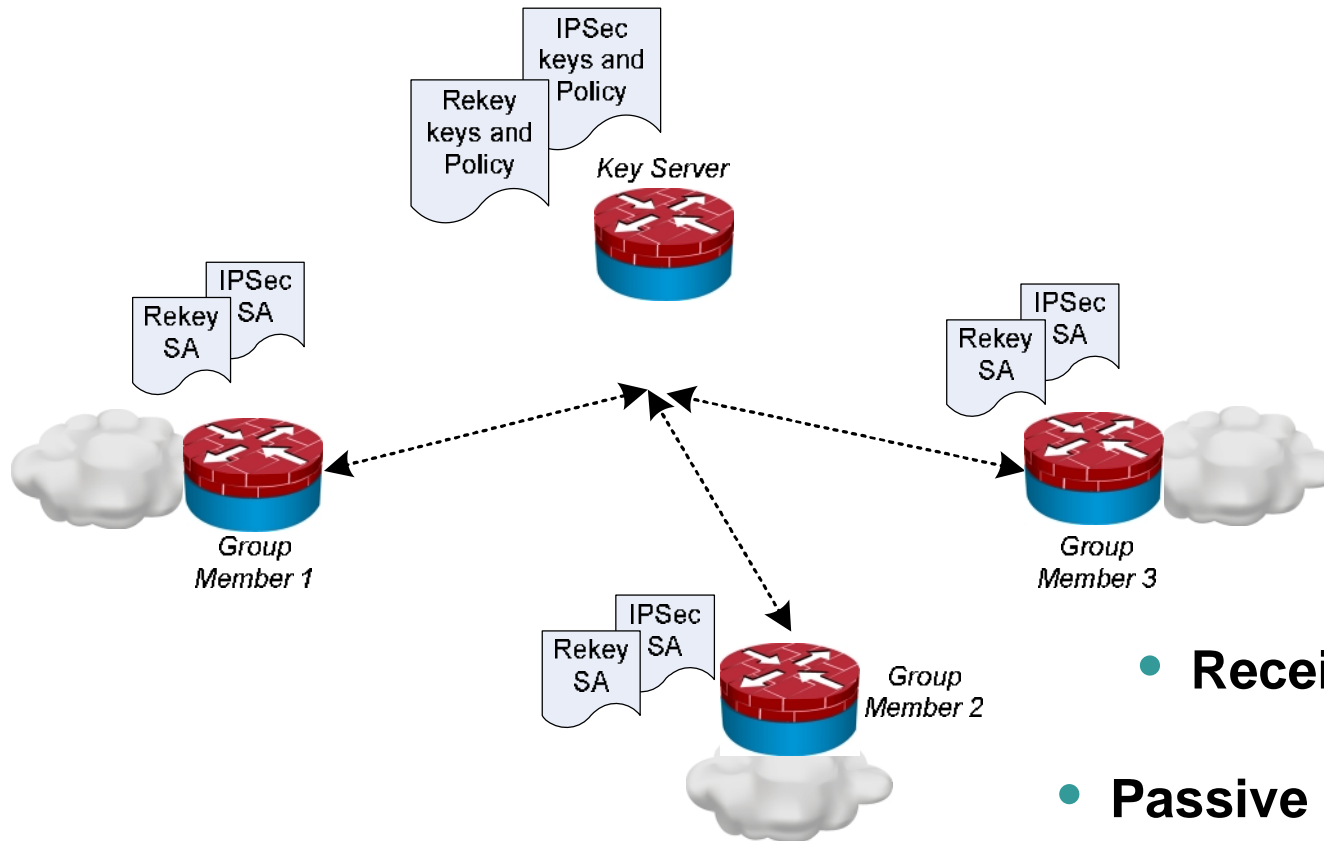
- Нагрузка на шифрование ложится на CE-устройства

Варианты решений GET VPN: замена туннельных VPN сеть-сеть



Дополнительные функции GET VPN

www.specialist.ru



- Receive only SA Feature
- Passive SA Feature
- Fail Close mode
- Local Exception Policy on GM 12-14

Поддерживаемые устройства

- **Key Servers: Cisco 18xx, Cisco 28xx, Cisco 3845, Cisco 7200, Cisco ASR1004**
- **Group Members: Cisco 8xx, Cisco 18xx, Cisco 28xx, Cisco 38xx, Cisco 7200**
- **IOS image version: 12.4(15)T8 and 12.4(22)T2**
- **IOS-XE image version: 12.2(33)XNC**
- **Следующие модули аппаратного шифрования доступны:**
 - **Cisco AIM-VPN/SSL Module for Cisco integrated services routers**
 - **Cisco VPN acceleration Module 2+ for Cisco 7200 series routers and 7301 routers**
 - **Cisco VSA (high-performance crypto engine) for Cisco 7200VXR/NPE-G2 routers**

Выводы: GET VPN

- **Высокомасштабируемая технология безтуннельного шифрования**
- **Нет необходимости в дополнительной маршрутизации**
- **Поддержка существующей QoS архитектуры**
- **Оптимальная передачи multicast-трафика**
- **Повышенная сетевая производительность**
- **Гибкость и простота управления**