



Сетевая безопасность для вертикальных рынков

# **Сетевая безопасность платежных систем**

СТАНДАРТ СЕТЕВОЙ БЕЗОПАСНОСТИ ДЛЯ РОССИЙСКОГО БИЗНЕСА

Область применения

Требования

CSP VPN Gate 100B

Дизайн VPN

Критерии выбора продуктов

# Область применения

# ● **Необходимость защиты**

- ✦ **Платежные сети передают и обрабатывают критичную информацию**
  - потенциальный объект атаки
  - идеальный вариант – изолированная сеть
  - проблема: сегодня на рынке отсутствуют специальные средства защиты для банкоматов
- ✦ **Банкомат защищен на прикладном уровне, но желательны дополнительные средства защиты:**
  - защита от несанкционированного доступа из сети
  - защита от denial-of-service attack
  - конфиденциальность в открытой сети, защита от недобросовестного провайдера выделенной линии

# ● Подключение через Интернет

- ✦ **Значительно дешевле, чем выделенная линия IP или X.25**
- ✦ **Дешевле, надежнее и удобнее, чем коммутируемая линия**
- ✦ **Легко диверсифицируется (надежность коммуникаций)**
- ✦ ***В регионах часто отсутствуют выделенные коммуникационные ресурсы и подключению через Интернет нет альтернативы***

**НО:**

- ✦ **При работе платежной сети через Интернет требуется решение проблемы сетевой информационной безопасности**

# ● Решение существует

- ✦ **Технологии VPN (IKE/IPsec) позволяют практически полностью изолировать платежную сеть**
  - сеть настраивается в режим работы только с шифрованным трафиком
  - доступ в сеть получает только владелец криптоключа (сертификата)
- ✦ **Стандартные прикладные средства обеспечения информационной безопасности банкомата не используют российских криптостандартов и, таким образом, де-юре не являются средствами защиты**
  - дополнить программное обеспечение банкомата сертифицированными средствами защиты невозможно (состав ПО ограничен)
  - применение сертифицированных средств защиты сетевого уровня легализует систему безопасности платежной системы

Область применения

Требования

CSP VPN Gate 100B

Дизайн VPN

Критерии выбора продуктов

# Требования

s•terra

C S P

Cisco Solution Technology Integrator

# Сетевое окружение банкомата



- ✱ Уединенный банкомат подключается к процессинговому центру при помощи
  - выделенной линии
    - IP
    - X.25
  - коммутируемой линии GPRS
- ✱ Банкомат в подразделении, отделении, сети предприятия – LAN-соединение (X.25 или IP)

# Требования надежности



- ✦ К платежной системе, как с системе массового обслуживания, предъявляются повышенные требования надежности
- ✦ Можно выделить подзадачи:
  1. надежности банкомата
    - надежные платформы не применяют, дешевле установить два банкомата
  2. надежности канала связи
    - применяют резервированные каналы
  3. надежности процессингового центра
    - применяют резервированные и отказоустойчивые решения



Область применения

Требования

**CSP VPN Gate 100B**

Дизайн VPN

Критерии выбора продуктов

# CSP VPN Gate 100B

s•terra





C S P

Cisco Solution Technology Integrator

# ● Системно-технические требования

- ✱ **Компактность**
- ✱ **Пылезащищенность (отсутствие механических компонент)**
- ✱ **Поддержка коммуникационных сред платежных сетей**
  - Ethernet**
  - модем (внешний) на выделенной линии, коммутируемой линии, GPRS**
- ✱ **Поддержка требований надежности коммуникационной инфраструктуры**
  - поддержка резервирования каналов со стороны банкомата (диверсификация доступа)**
  - поддержка резервированной сетевой инфраструктуры процессингового центра (работа в сети с резервированными шлюзами доступа, автоматическая обработка отказа шлюза доступа)**

# Специальные требования

-  **Стойкость защиты**
  - конфиденциальность
  - строгий контроль доступа (изоляция платежной сети)
-  **Защищенность от НСД со стороны обслуживающего персонала**
-  **Стандартизация, управляемость, совместимость с системами сетевого событийного протоколирования и мониторинга, работа с различными криптографическими и ключевыми системами**
-  **Использование российских стандартов и сертификация**

# VPN-шлюз для защиты банкомата



- \* **CSP VPN Gate 100B:**
  - IKE/IPsec VPN-шлюз с использованием российских криптостандартов**
  - полный набор технических характеристик продуктов CSP VPN Gate**  
(<http://www.s-terra.com/CSP/RU/products/products.htm>)
- \* **Удовлетворяет приведенным выше системно-техническим и специальным требованиям**
- \* **Обеспечивает производительность шифрования трафика до 10 Мбит/с, поддерживает до 5 конкурентных VPN-туннелей**
- \* **ОС Linux (пользователь работает в стандартной консоли Cisco)**
- \* **Дистанционное управление по защищенному каналу, централизованное управление с платформы CiscoWorks**

Область применения

Требования

CSP VPN Gate 100B

**Дизайн VPN**

Критерии выбора продуктов

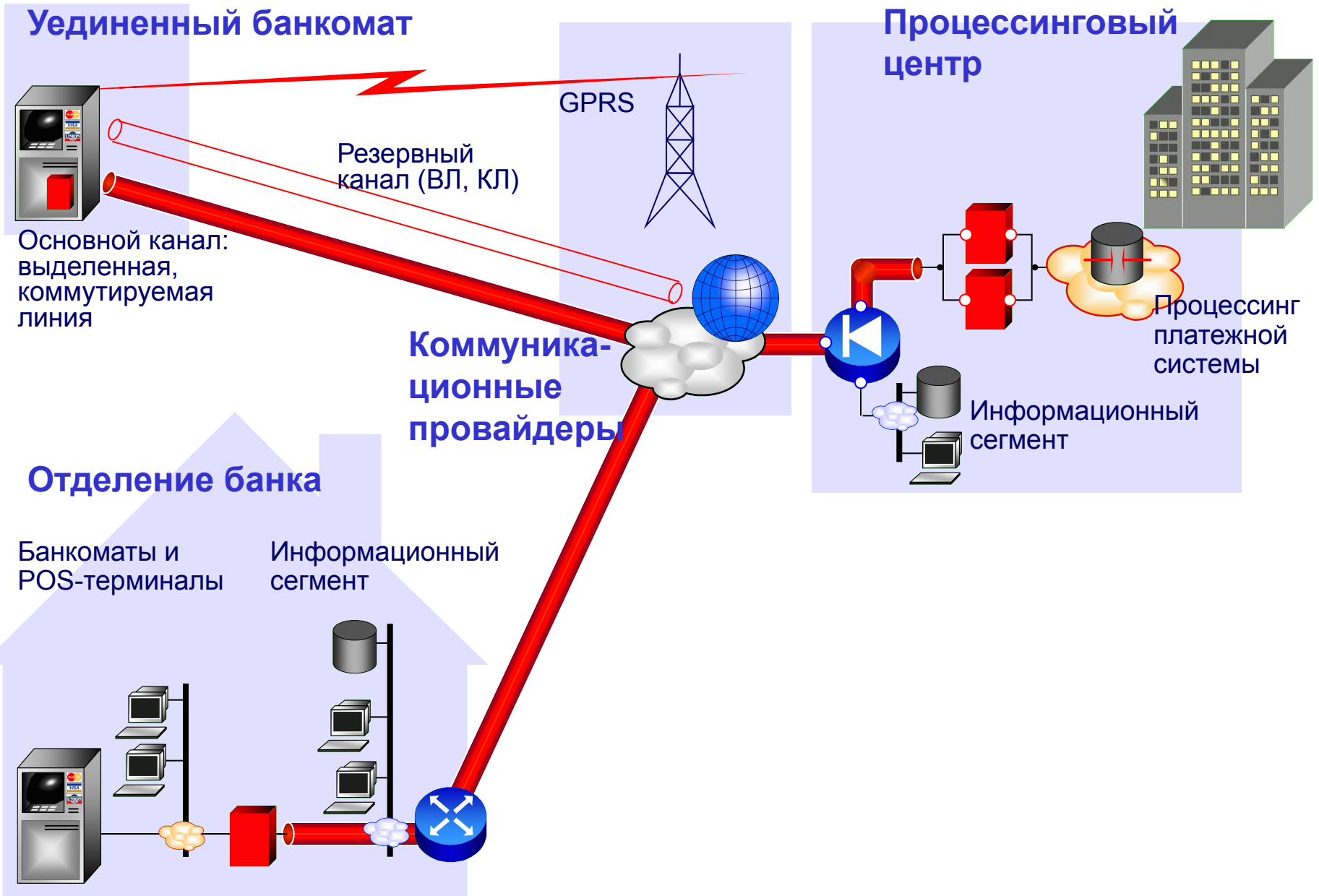
# Дизайн VPN

s•terra

C S P

Cisco Solution Technology Integrator

# ● Базовый сценарий применения



# Выполнение требований безопасности

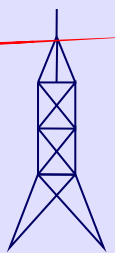
## Уединенный банкомат



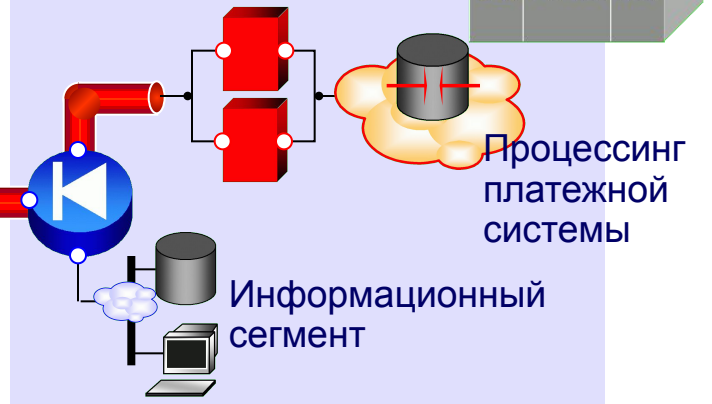
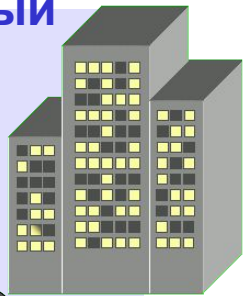
Основной канал:  
выделенная,  
коммутируемая  
линия

Резервный  
канал (ВЛ, КЛ)

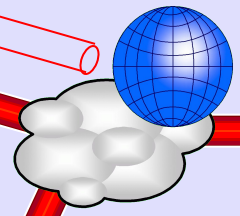
GPRS



## Процессинговый центр



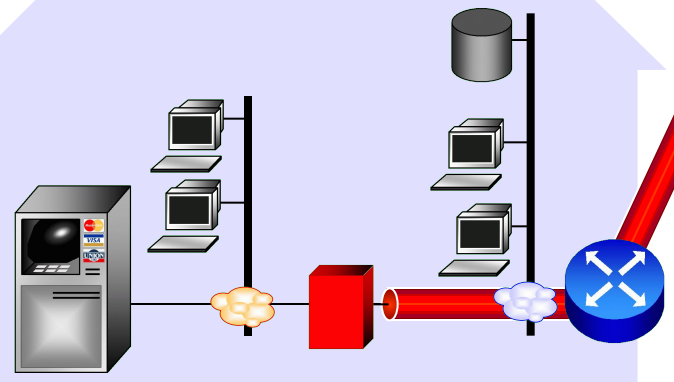
## Коммуникационные провайдеры



## Отделение банка

Банкоматы и  
POS-терминалы

Информационный  
сегмент

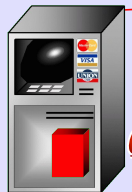


**Весь трафик платежной сети шифрован**

**Платежная сеть изолирована не только от публичных коммуникационных сетей, но и от информационной сети Банка**

# Обеспечение коммуникативности

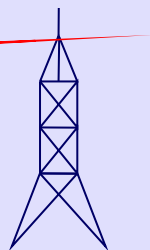
## Уединенный банкомат



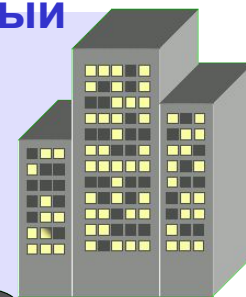
Основной канал:  
выделенная,  
коммутируемая  
линия

Резервный  
канал (ВЛ, КЛ)

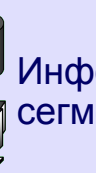
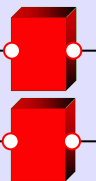
GPRS



## Процессинговый центр



Процессинг  
платежной  
системы



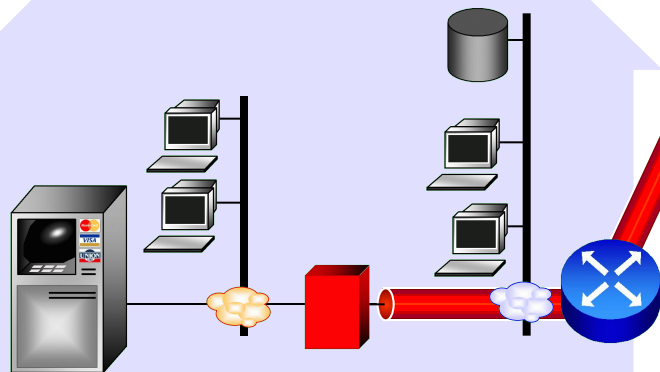
Информационный  
сегмент

Коммуника-  
ционные  
провайдеры

## Отделение банка

Банкоматы и  
POS-терминалы

Информационный  
сегмент



**Число провайдеров не  
ограничено (возможна  
диверсификация)**

**Доверие к провайдерам не  
требуется**

**Используются различные  
среды передачи данных**



# Выполнение требований надежности

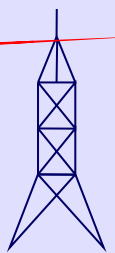
## Уединенный банкомат



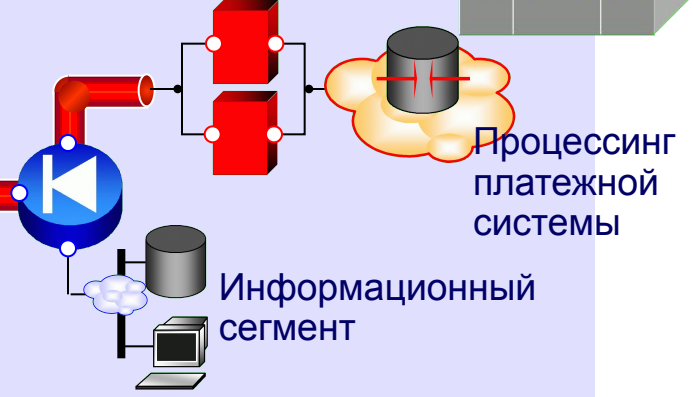
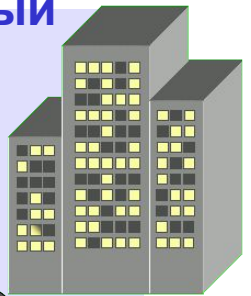
Основной канал:  
выделенная,  
коммутируемая  
линия

Резервный  
канал (ВЛ, КЛ)

GPRS



## Процессинговый центр



Процессинг  
платежной  
системы

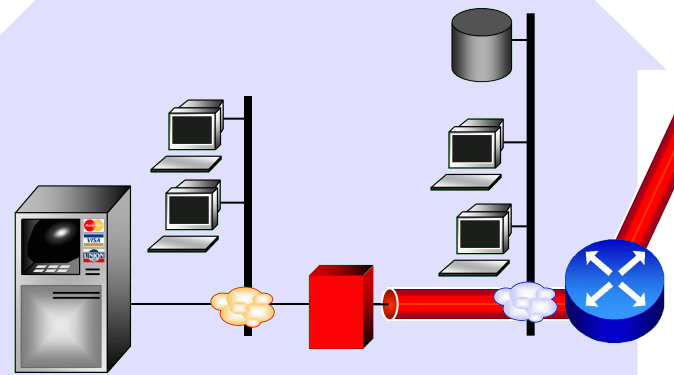
Информационный  
сегмент

Коммуникационные  
провайдеры

## Отделение банка

Банкоматы и  
POS-терминалы

Информационный  
сегмент



**Уединенный банкомат  
использует резервированные  
каналы и автоматически  
переключается на резервный  
канал (шлюз безопасности  
поддерживает эти операции)**

# Выполнение требований надежности

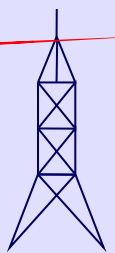
## Уединенный банкомат



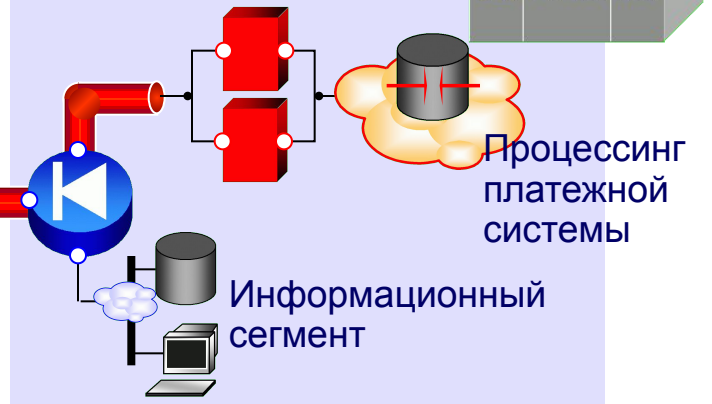
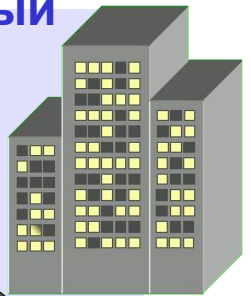
Основной канал:  
выделенная,  
коммутируемая  
линия

Резервный  
канал (ВЛ, КЛ)

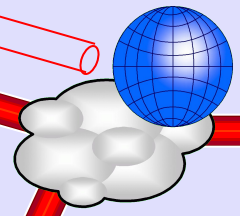
GPRS



## Процессинговый центр



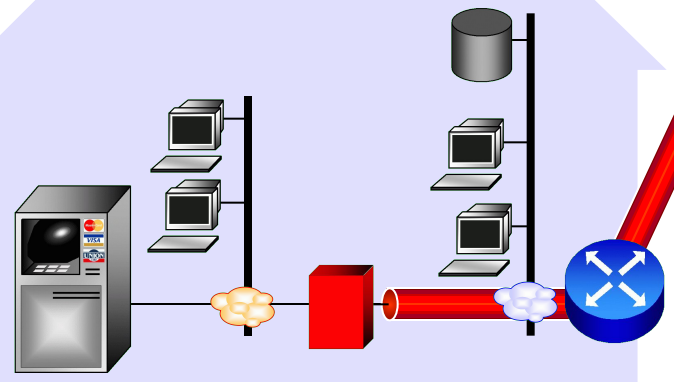
## Коммуникационные провайдеры



## Отделение банка

Банкоматы и  
POS-терминалы

Информационный  
сегмент



**В отделении резервирование каналов и диверсификация доступа обеспечиваются для всей сети отделения (возможен вывод резервной линии со шлюза защиты платежного сегмента)**

# Выполнение требований надежности

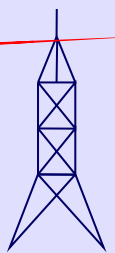
## Уединенный банкомат



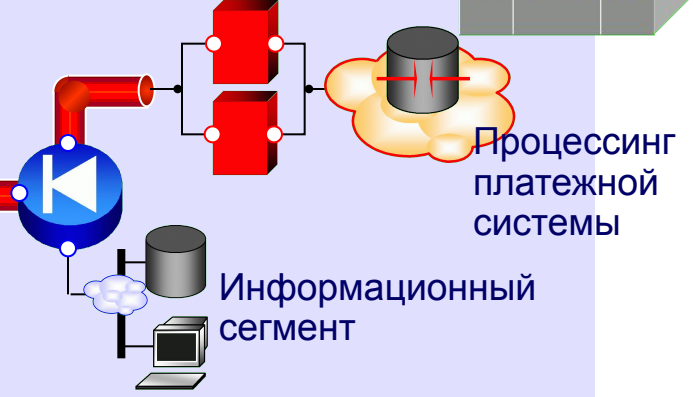
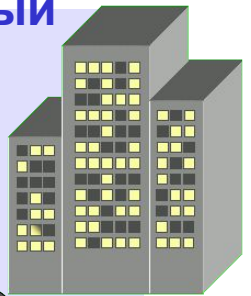
Основной канал:  
выделенная,  
коммутируемая  
линия

Резервный канал (ВЛ, КЛ)

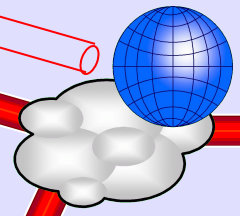
GPRS



## Процессинговый центр



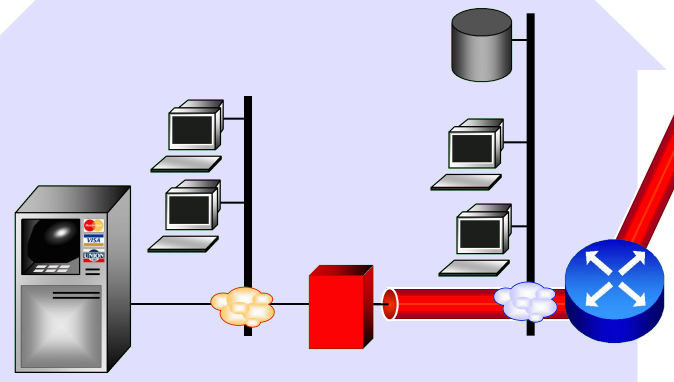
## Коммуникационные провайдеры



## Отделение банка

Банкоматы и POS-терминалы

Информационный сегмент



**В процессинговом центре шлюзы безопасности резервированы и автоматически обрабатывают отказ**

Область применения

Требования

CSP VPN Gate 100B

Дизайн VPN

Критерии выбора продуктов

# Критерии выбора продуктов

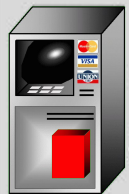
s•terra

C S P

Cisco Solution Technology Integrator

# ● Защита уединенного банкомата

## Уединенный банкомат



- ★ Для защиты отдельно установленного банкомата применяются продукты **CSP VPN Gate 100B** или **CSP VPN Server B**
- ★ По практике наших заказчиков продукт **Server B** часто устанавливается на банкоматы, находящиеся в контролируемой зоне
- ★ В тех случаях, когда регламент эксплуатации платежной системы запрещает установку дополнительного ПО в банкомат персоналу эксплуатации банкоматов нельзя давать доступ к системам защиты информации (часто это требование связывают с тем, что находится вне контролируемой зоны)
- ★ применяется выделенное изолированное средство защиты – **CSP VPN Gate 100B**
- ★ Прочие критерии выбора продуктов (например, скорость линии передачи данных) не имеют значения

Коммуникационные провайдеры

Отдел банка

# ● Защита в отделении банка



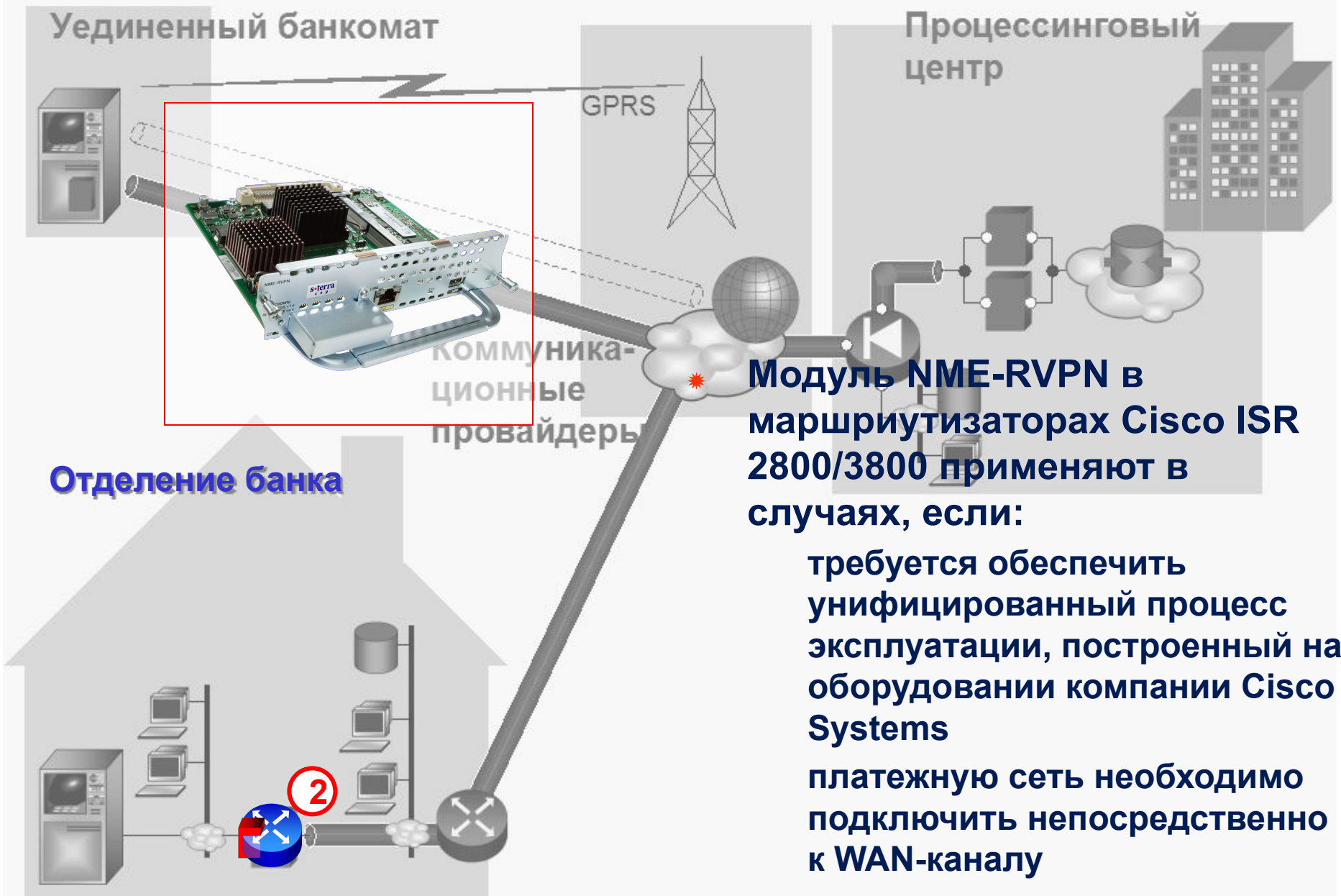
# ● Защита в отделении банка



продукт CSP VPN Client В отличается от продукта Server В тем, что, как клиентская программа, не работает до входа оператора в систему

- ★ Прочие критерии выбора продуктов не устанавливаются

# ● Защита в отделении банка



Уединенный банкомат

Процессинговый центр

GPRS

Коммуникационный провайдер

Отделение банка

**Модуль NME-RVPN в маршрутизаторах Cisco ISR 2800/3800 применяют в случаях, если:**

- требуется обеспечить унифицированный процесс эксплуатации, построенный на оборудовании компании Cisco Systems
- платежную сеть необходимо подключить непосредственно к WAN-каналу

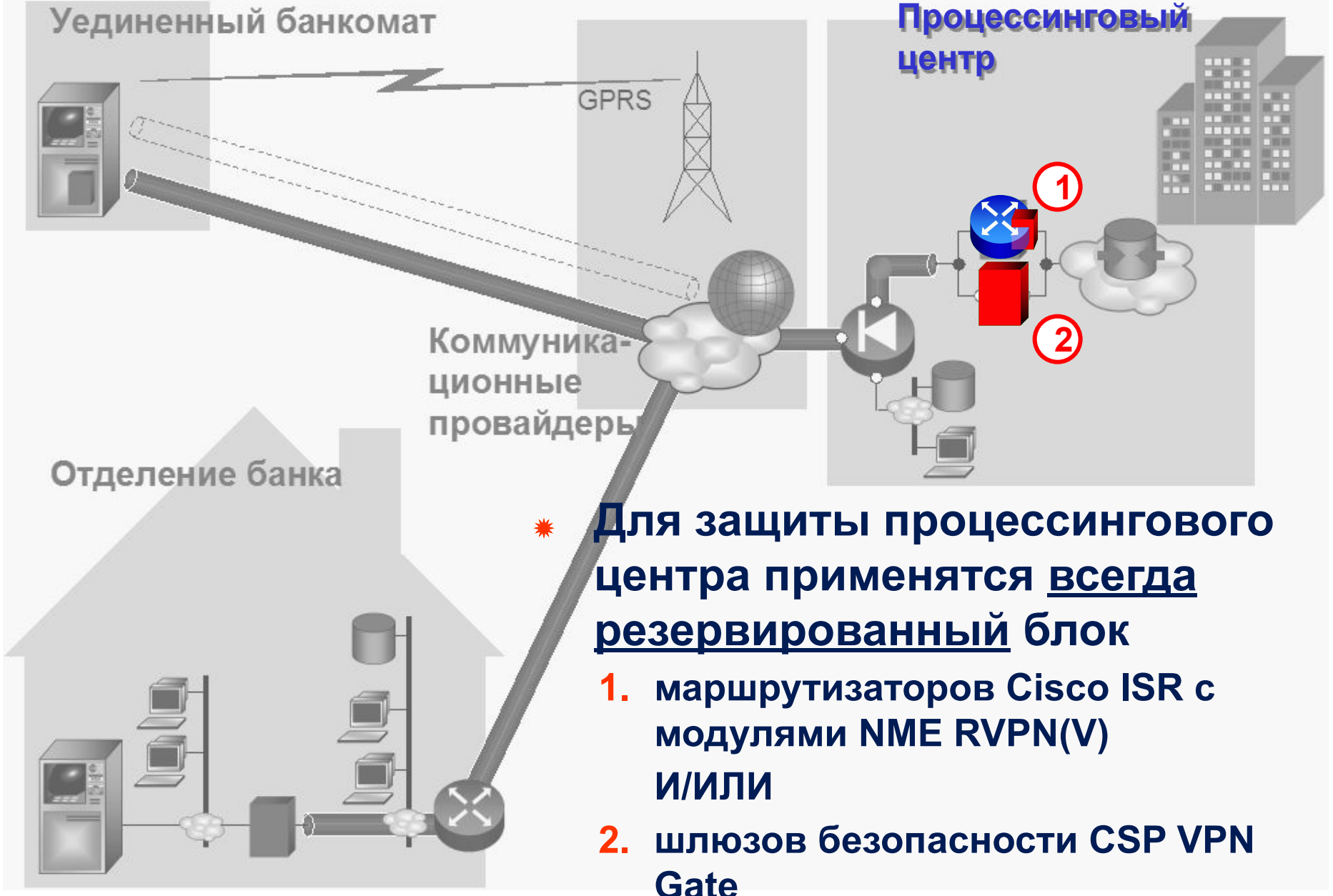


# ● Защита в отделении банка



- ★ Шлюзы безопасности CSP VPN Gate 100B или 1000, реже - 3000 применяют в зависимости от объема трафика сегмента платежной сети в отделении банка
- ★ Иногда применяют схемы с резервированием шлюзов безопасности

# ● Защита процессингового центра



★ Для защиты процессингового центра применятся всегда резервированный блок

- 1. маршрутизаторов Cisco ISR с модулями NME RVPN(V) И/ИЛИ
- 2. шлюзов безопасности CSP VPN Gate

# ● Защита процессингового центра

● Число резервированных маршрутизаторов в блоке – не менее 2х

между маршрутизаторами блока обеспечивается выравнивание нагрузки

система с тремя шлюзами безопасности обеспечивает дублирование систем защиты даже при отказе (профилактике) отдельного маршрутизатора

● Один модуль NME RVPN(V) может обслуживать сеть из 10 000 банкоматов и POS-терминалов

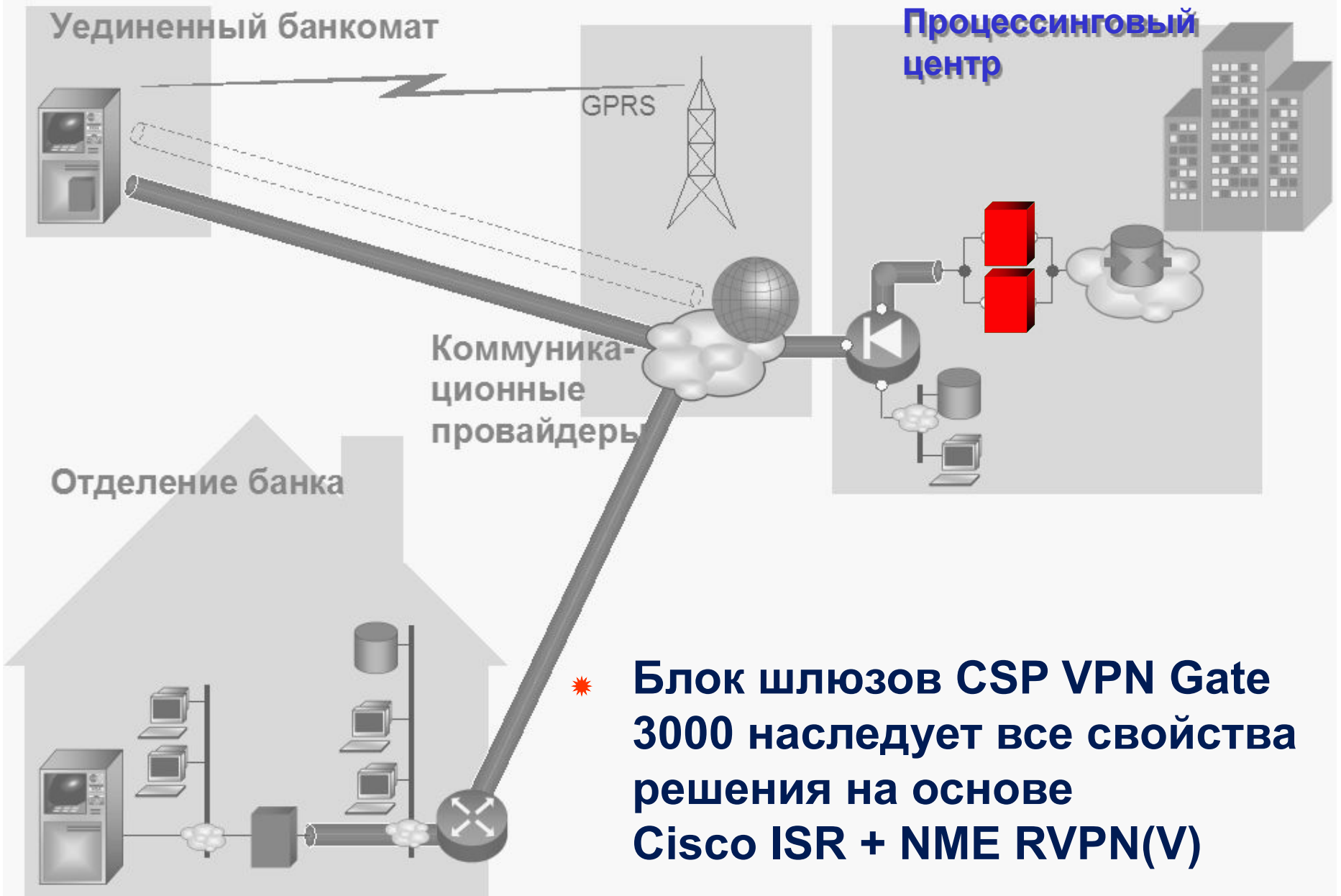
● Масштабируемость системы:

с применением 2х маршрутизаторов Cisco ISR 3845 с 4мя модулями NME RVPN каждый обеспечивается защита платежной сети с 50 000 абонентов установка дополнительных маршрутизаторов может поднять и этот предел

Процессинговый центр



# ● Защита процессингового центра



## КОНТАКТЫ

e-mail: [information@s-terra.com](mailto:information@s-terra.com)

web: <http://www.s-terra.com/>

Тел.: +7 (499) 940 9001

+7 (495) 726 9891

Факс: +7 (499) 720 6928

# Вопросы?

*Обращайтесь к нам!*

s•terra

C S P

Cisco Solution Technology Integrator