

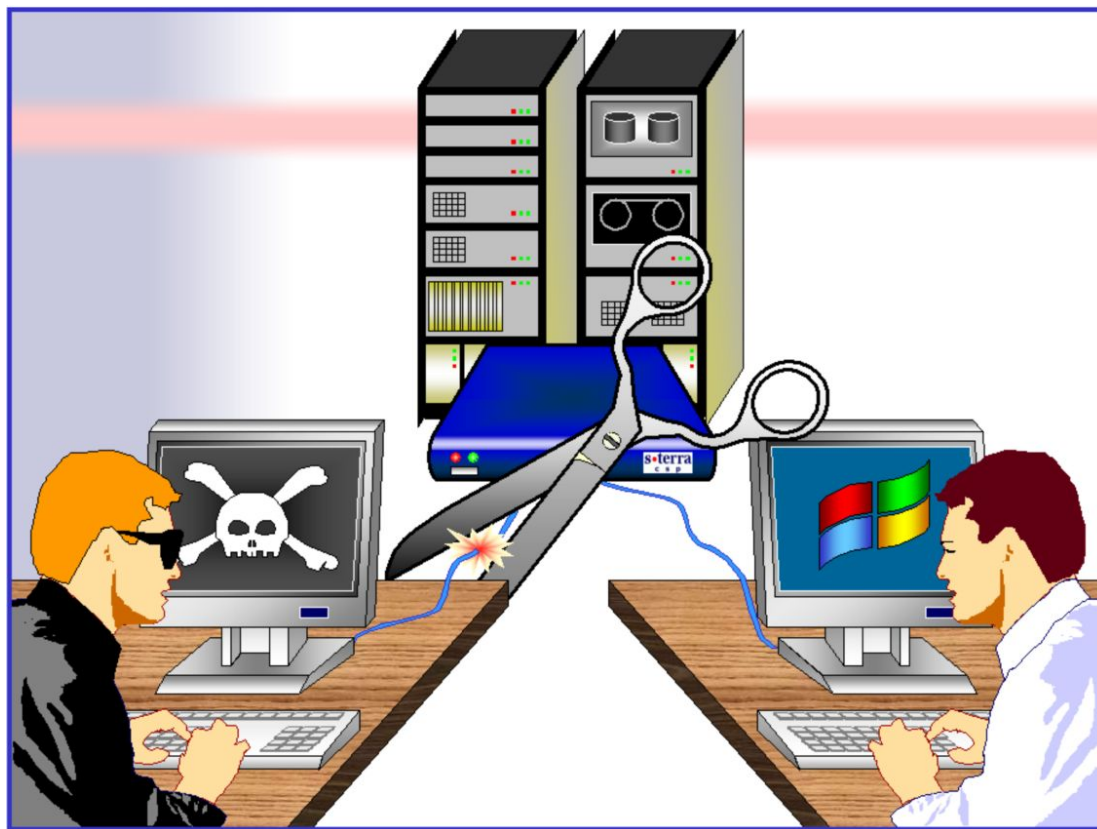


Сетевая безопасность для вертикальных рынков

Решения

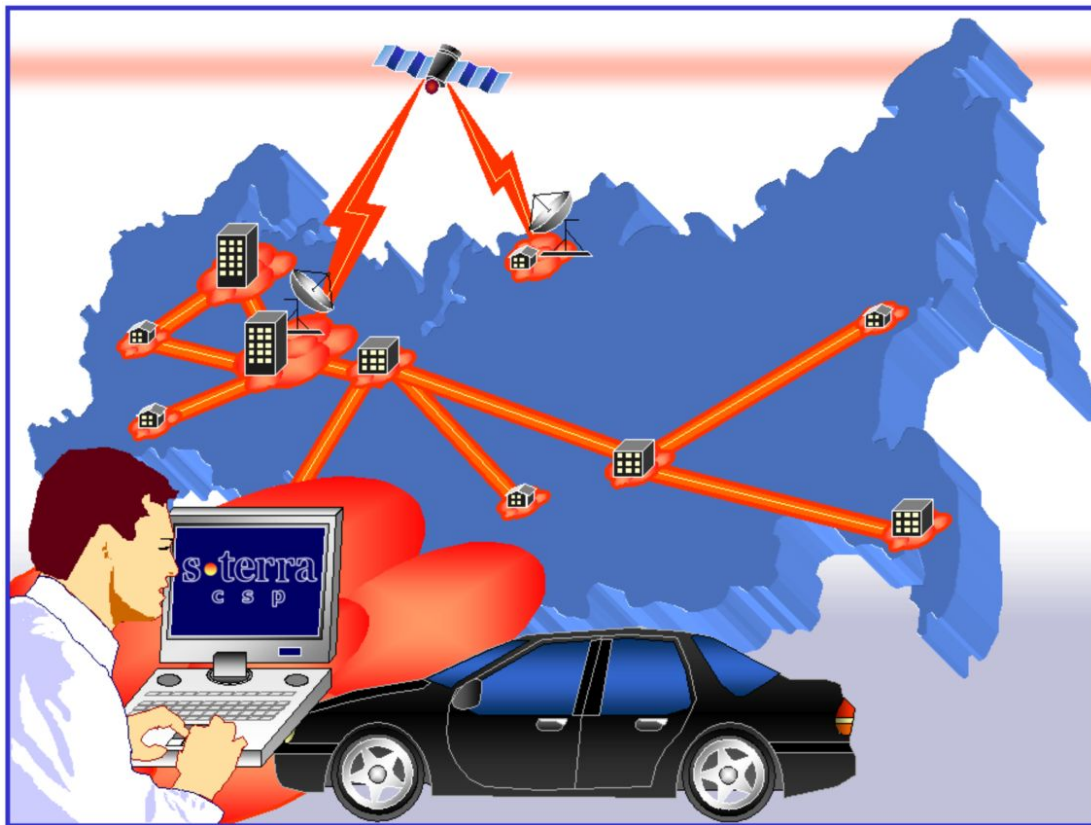
для коммуникационных провайдеров

● Как работает сетевая защита?



- * Стандарты сетевой безопасности применительно к каждому сетевому пакету обеспечивают свойства:
 - Конфиденциальности
 - Целостности
 - Аутентификации источника данных
- * Внедрение системы сетевой безопасности прозрачно для приложений и не требует реорганизации сети и информационной инфраструктуры

● Преимущества защищенной сети



- * Открытый трафик не подвержен перехвату
- * В сеть может войти только легитимный пользователь
- * Поток пакетов целостен, в него нельзя «подмешать» не только посторонний пакет, но и ранее принятый сетью (перехваченный и повторно переданный) легитимный пакет
- * Внутренняя топология сети полностью скрыта от злоумышленника
- * ... таким образом, корпоративное информационное пространство полностью изолировано

● Продукты сетевой защиты



CSP VPN Client
(защита индивидуального рабочего места)

CSP VPN Server
(защита сервера)



NME-RVPN
(модуль сетевой защиты для Cisco ISR 2800, 3800)

CSP VPN Gate 1000
(канал xDSL, до 10 Мбит/с)



CSP VPN Gate 100
(канал до 2 Мбит/с, малый офис)

CSP VPN Gate 3000
(канал до 100 Мбит/с)

CSP VPN Gate 7000
(субгигабитный канал)

CSP VPN Gate 10000
(гигабитный канал)

● Требования законодательства



- ✦ Федеральные законы «Об информации, информационных технологиях и защите информации», «О коммерческой тайне», «О персональных данных» (и конкретизирующие его Постановления Правительства), требования ФСТЭК и ФСБ России

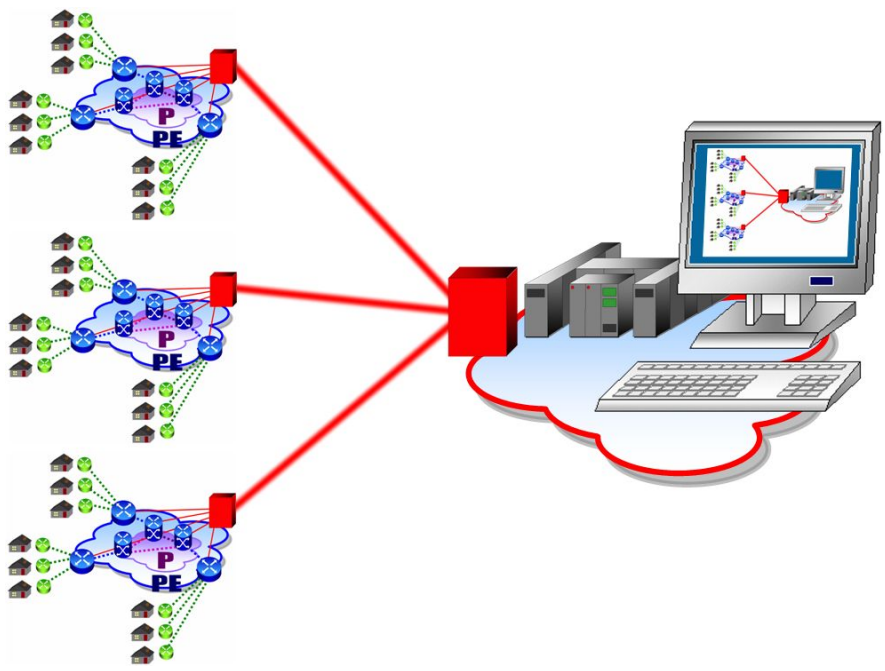
определяют меры ответственности за безопасность информационных активов

- ✦ ФСТЭК России, «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»

«Для передачи информации по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации. Применяемые средства защиты информации должны быть сертифицированы»

● Защита инфраструктуры и систем управления

ВЫДЕЛЕННАЯ ЗАЩИЩЕННАЯ СЕТЬ УПРАВЛЕНИЯ



- * Сложная коммуникационная инфраструктура провайдера может быть полностью защищена от воздействий из внешних сетей
- * Для систем управления, мониторинга, биллинга могут быть организованы выделенные защищенные подсети, высоко изолированные друг от друга

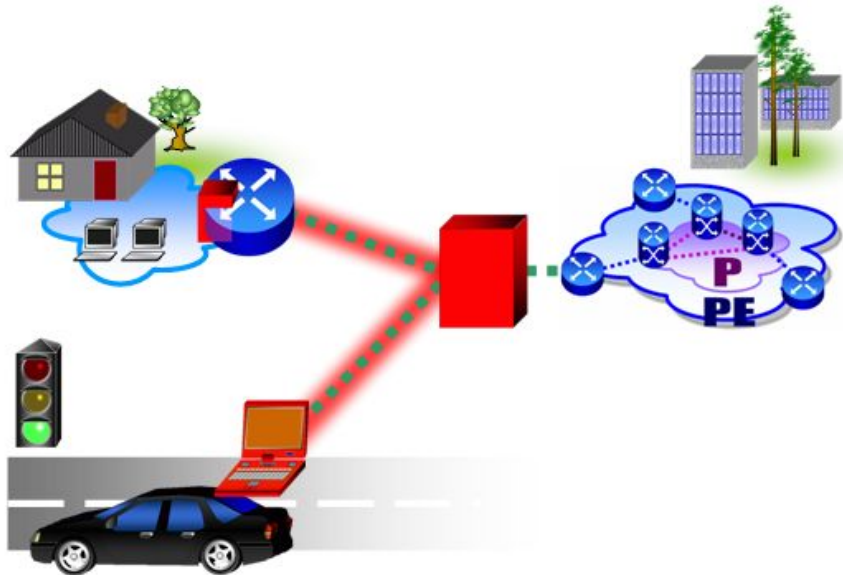
Сервис защиты информации для клиентов



IPsec VPN может быть включен в состав дополнительных услуг, предоставляемых провайдером для клиентов



● Изоляция сети клиента на последней миле



- ✱ IPsec VPN мало требователен к инфраструктуре доступа
- ✱ Там, где трудно организовать прямое подключение клиентов к MPLS VPN, IPsec VPN позволит «подобрать» клиента где угодно (в том числе – в точке временного пребывания мобильного пользователя) и подвести его по защищенному туннелю на «последней миле» к инфраструктуре MPLS

Это существенно расширяет зону предложения базового сервиса MPLS

● Услуга сквозной конфиденциальности трафика

- ✦ Для тех клиентов, которые не готовы доверять провайдеру, можно предложить сервис, обеспечивающий конфиденциальность данных



Для этого достаточно отдать клиенту процесс управления ключами шифрования

В результате при предложении любой услуги (включая MPLS, где данные клиента от провайдера не закрыты) можно привлечь к пользованию услугой новых клиентов, не доверявших провайдеру ранее

● Модель сервиса MSSP

- ✦ Эта модель сервиса получила широкое распространение в мире
- ✦ Тенденция к аутсорсингу безопасности объективна, поскольку:

Безопасность дорога в эксплуатации

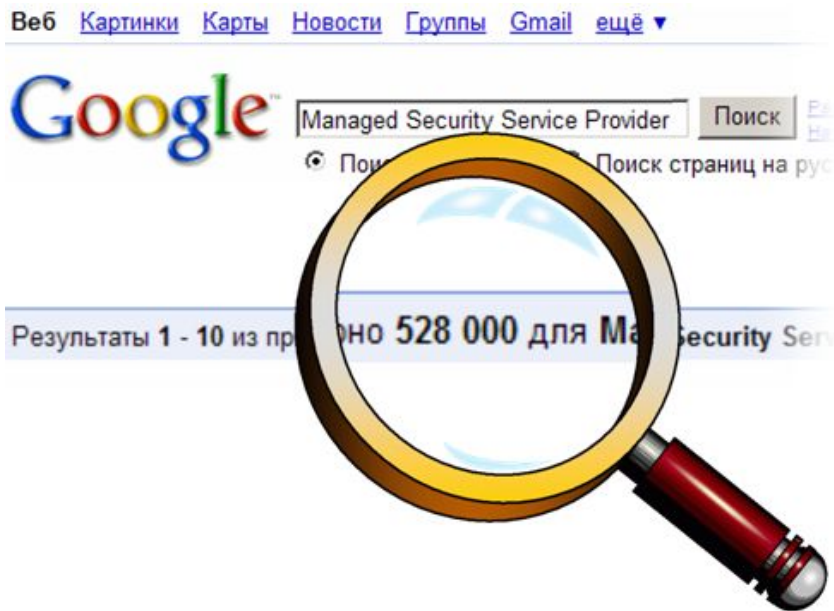
Массовый клиент не может позволить себе инфраструктуру того же масштаба и качества, что и крупный поставщик услуг

Профессиональный опыт службы эксплуатации провайдера всегда будет превосходить опыт и знания, оперативность и качество сервиса команды корпоративного заказчика

- ✦ **Дополнительный рыночный фактор: закон о персональных данных**

Миллионы операторов персональных данных к 2010 году должны будут применять предписанные государством меры защиты

- Большинство из них к этому не готовы – поэтому придут к поставщику услуг



● Реализация сервиса MSSP



✳ Конечному заказчику (клиенту) провайдер может предоставлять следующий сервис:

1. интеграция защищенной сети с соблюдением требований заказчика по политике безопасности
2. управление системой защиты
3. обеспечение ключевым материалом и услугами удостоверяющего центра
4. мониторинг системы защиты (осуществляется клиентом совместно с провайдером сервиса)
5. техническую поддержку и сопровождение

✳ Для решения задач проектирования «под ключ», внедрения и технического сопровождения решения может, при необходимости, привлекаться специализированный системный интегратор (на подряде у провайдера)

КОНТАКТЫ

e-mail: 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