

Основы безопасности информационных технологий

Виртуальные частные сети

Содержание лекции

- Введение
- Туннелирование
- Протоколы VPN канального уровня
- Протокол IPSec
 - Ассоциации обеспечения безопасности (Security Association, SA)
 - Протокол обмена Интернет-ключами
 - Первая фаза протокола IKE
 - Вторая фаза протокола IKE
 - Протокол аутентификации заголовка
 - Протокол безопасной инкапсуляции содержимого пакета
- Протоколы VPN транспортного уровня
- Цифровые сертификаты
- Примеры отечественного построения VPN



Введение

Виртуальные частные сети (Virtual Private Network, VPN) — это подключение, установленное по существующей общедоступной инфраструктуре и использующее шифрование и аутентификацию для обеспечения безопасности содержания передаваемых пакетов.

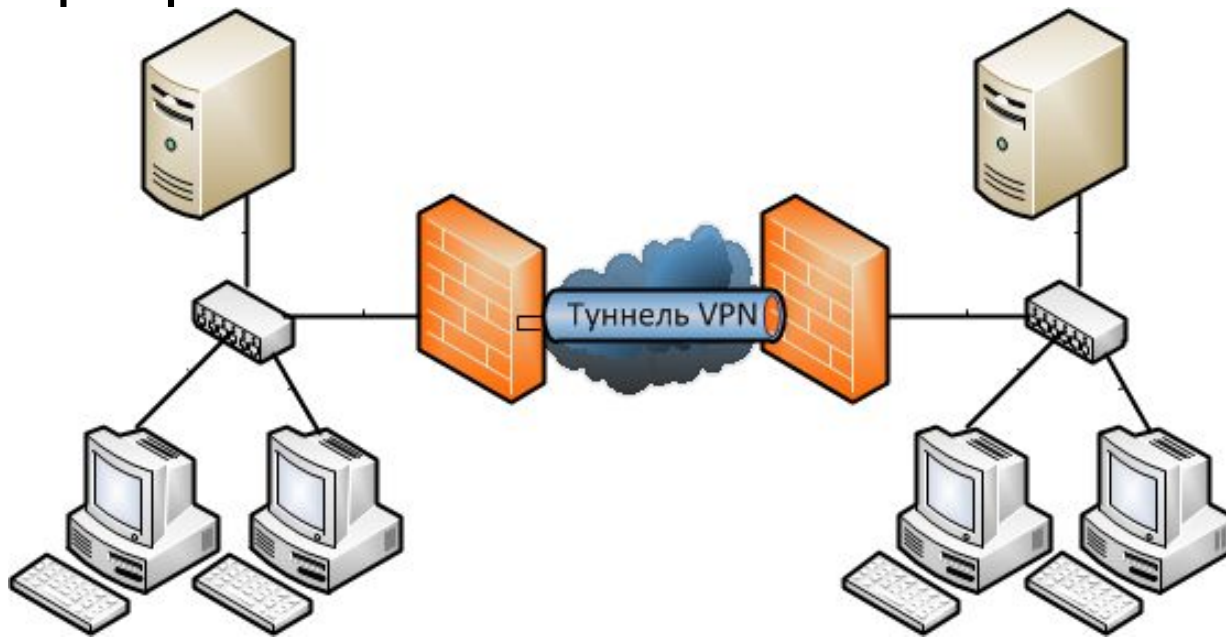
Типы VPN по конфигурации:

- узел-узел (host-to-host)
- узел-шлюз (host-to-gateway)
- шлюз-шлюз (gateway-to-gateway)



Туннелирование

Туннелирование — это процесс инкапсуляции одного типа пакетов внутри другого в целях получения некоторого преимущества при транспортировке.



Протоколы VPN канального уровня

- Протокол туннелирования типа «точка-точка» (Point-to-point Tunneling Protocol, PPTP)
- Протокол туннелирования второго уровня (Layer Two Tunneling Protocol, L2TP)



Протокол IPSec

IPSec (IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

IPSec имеет два основных режима:

- транспортный (transport)
- туннельный (tunnel)



Ассоциации обеспечения безопасности (Security Association, SA)

- ❑ База данных политики безопасности (Security Policy Database, SPD)
- ❑ База данных ассоциации обеспечения безопасности (Security Association Database, SAD)
- ❑ Уникальный индекс параметра обеспечения безопасности (Security Parameter Index, SPI)

- ❑ Выборка из базы данных ассоциации обеспечения безопасности маршрутизатора Cisco:

inbound esp sas:

spi: 0x71BB425D (1908097629)

transform: esp-des esp-md5-hmac,

in use settings={ Tunnel,}

slot: 0, conn id: 2000, flow_id: 1, crypto map: mode

sa timing: remaining key lifetime (k/sec) : (4600800/ 3500)

IV size: 8 bytes

replay detection support: Y



Протокол обмена Интернет-ключами

Протокол обмена интернет-ключами (Internet Key Exchange, IKE) предназначен для аутентификации и согласования параметров обмена протокола IPSec.

Протокол IKE представляет собой комбинацию двух протоколов:

- протокола управления ассоциациями
- протокола управления ключами обеспечения безопасности в сети Интернет (Internet Security Association and Key Management Protocol, ISAKMP)



Первая фаза протокола IKE

Функции первой фазы:

- аутентификация удаленного пользователя
 - предварительно распространяемые ключи, pre-shared keys
 - цифровые сертификаты, digital certificates
- обмен информацией об открытых ключах
 - основной режим (main mode)
 - агрессивный режим (aggressive mode)



Вторая фаза протокола IKE

- согласовываются конкретные параметры ассоциации обеспечения безопасности IPSec
- согласование подобно агрессивному режиму обмена информацией первой фазы
- по завершению второй фазы формируется ассоциация обеспечения безопасности, пользователь получает подключение к VPN
- возможен единственный режим согласования — быстрый режим (quick mode)



Протокол аутентификации заголовка

- Поддерживает возможности аутентификации и проверки целостности
- Значение проверки целостности (Integrity Check Value, ICV)
- Несовместим с использованием NAT

Следующий заголовок	Длина содержимого пакета	Зарезервировано
Индекс параметра обеспечения безопасности (SPI)		
Порядковый номер		
Информация аутентификации (переменная длина, кратная 32 байтам)		



Протокол безопасной инкапсуляции содержимого пакета

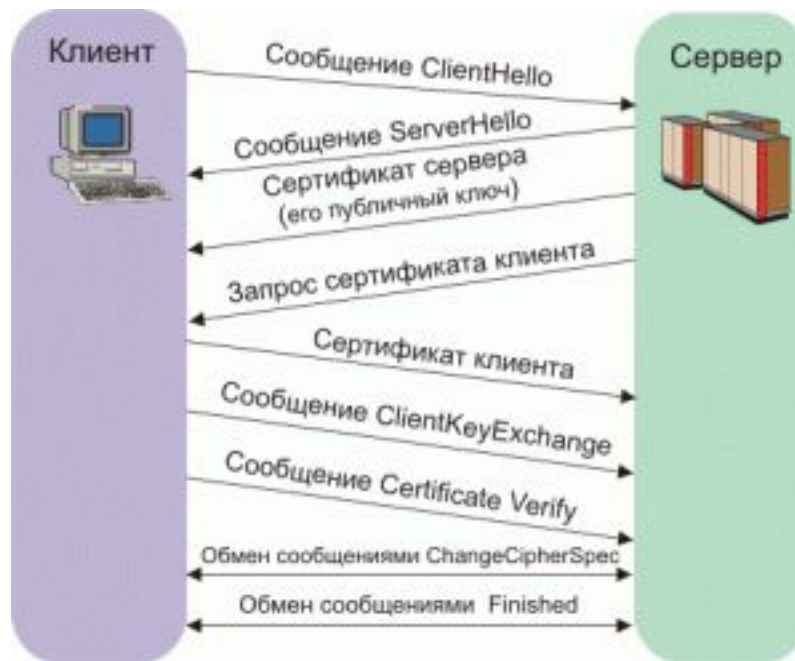
- обеспечивает конфиденциальность при помощи полного шифрования содержимого IP-пакетов
- модульность, может использовать любое количество доступных симметричных алгоритмов шифрования
- при работе в туннельном режиме можно использовать NAT

Индекс параметра обеспечения безопасности (SPU)		
Порядковый номер		
Содержимое пакета (переменная величина, кранная 32)		
Заполнение (опционально) (переменная величина, кранная 32)		
	Длина заполнения	Следующий заголовок
Информация аутентификации (опционально)		



Протоколы VPN транспортного уровня

□ Протокол SSL



□ Протокол SOCKS



Цифровые сертификаты

Цифровой сертификат — выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов.

Проблема управления ключами:

- генерацию ключей
 - проверку ключей
 - распространение ключей
 - использование ключей
 - хранение ключей
 - резервирование ключей
 - обновление ключей
 - уничтожение ключей
-
- установление времени жизни ключа

Цифровые сертификаты

Формат X.509

Версия
Номер сертификата
Идентификатор алгоритма шифрования и параметры алгоритма подписи
Имя объекта, выдавшего сертификат
Срок действия сертификата
Имя субъекта
Открытый ключ субъекта, идентификатор алгоритма и параметры алгоритма
Идентификатор объекта, выдавшего сертификат
Идентификатор объекта, получившего сертификат
Расширения
Алгоритм подписи, параметры алгоритма, цифровая подпись сертификата



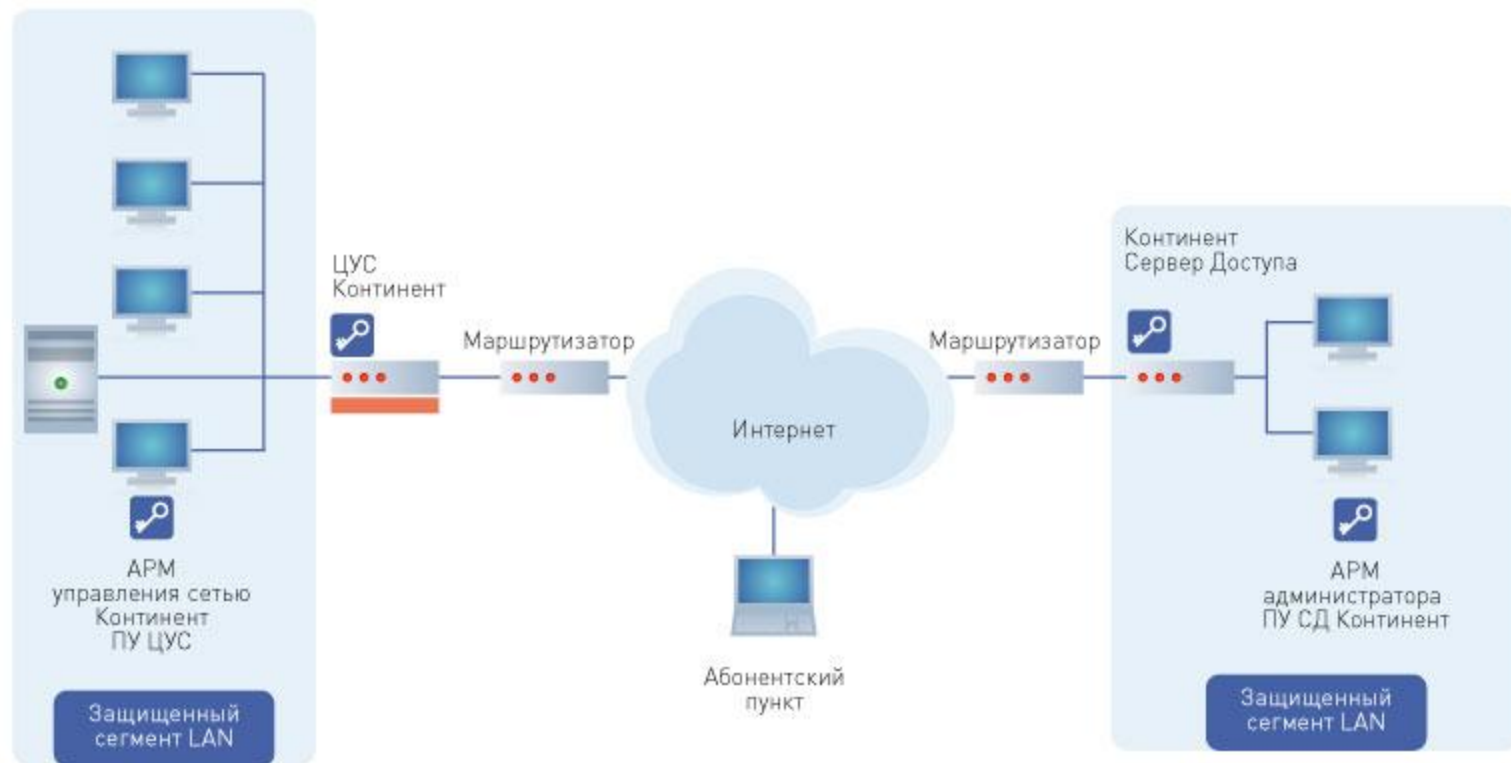
Примеры отечественного построения VPN



Информзащита
Системный интегратор



Аппаратно-программный комплекс шифрования "Континент"



ViPNet

