s·terra

c s p

Сценарии защиты

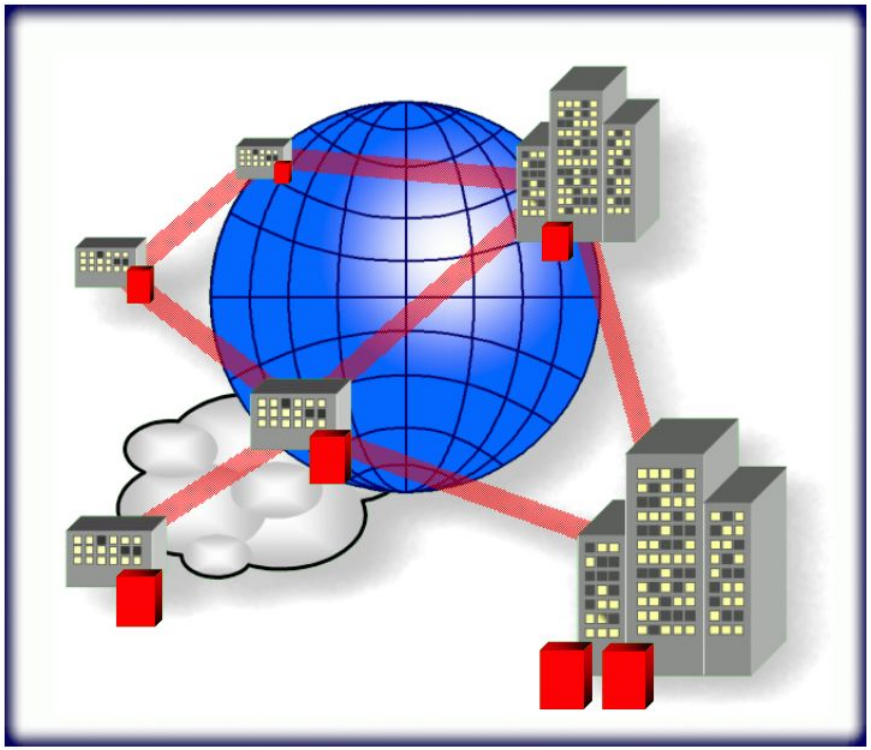
межсетевых взаимодействий

на основе продуктов CSP VPN™ и NME-RVPN™

Область применения

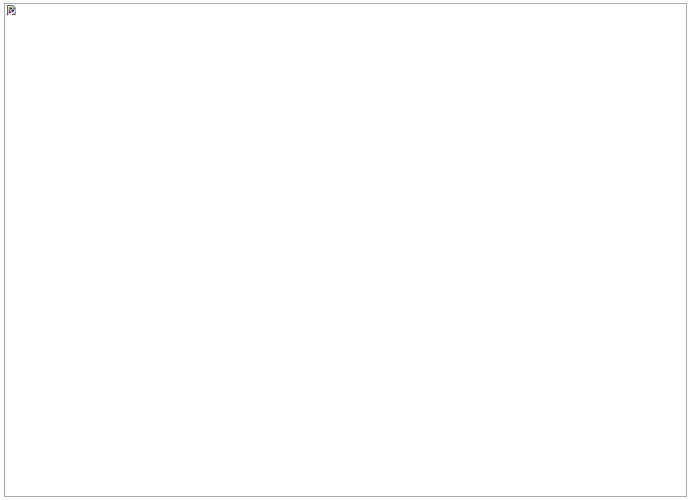
s·terra
c s p
Cisco Solution Technology Integrator

Сценарии межсетевого взаимодействия



- Сценарии *межсетевого взаимодействия* (LAN-to-LAN или Site-to-Site VPN) применяются для защиты коммуникаций территориально распределенных корпоративных сетей через публичные (открытые, не заслуживающие доверия) сети/каналы связи

Двухэшелонный дизайн

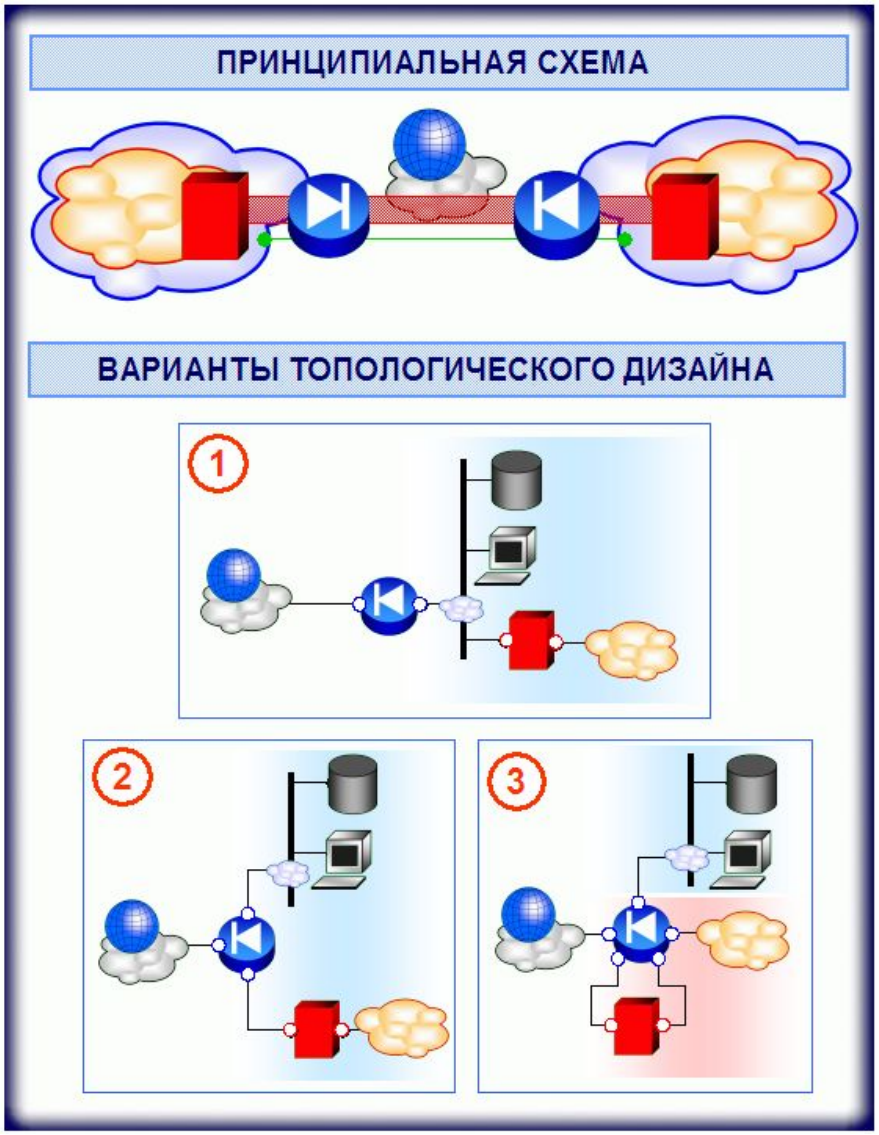


- Сценарии в настоящем руководстве рассмотрены применительно к двухэшелонному дизайну на основе продуктов Cisco (внешний периметр, голубой цвет) и CSP VPN (красная, защищенная зона)
- На внешнем периметре сети могут быть реализованы следующие меры защиты (или их комбинации):
  - сетевой контроль доступа (пакетная фильтрация)
    - испытан более чем десятилетней практикой защиты сетей и достаточно надежен
    - практически не имеет альтернатив при необходимости доступа из корпоративной сети в Интернет
    - не обеспечивает полную изоляцию корпоративной сети и аутентификацию доступа пользователей внутрь корпоративного периметра
  - коммутация на основе меток (MPLS VPN)
    - обеспечивает сильный контроль доступа на внешнем периметре
    - не использует криптографической защиты; как следствие – корпоративный трафик может быть защищен от хакерских атак из Интернет, но не может быть защищен от атаки со стороны недобросовестного коммуникационного провайдера
  - защита при помощи IPsec
    - обеспечивает наивысшую степень защиты
    - использует более сложные сценарии защиты и может ограничивать производительность сети

Межсетевой экран на внешнем периметре

s·terra
c s p
Cisco Solution Technology Integrator

Пакетный фильтр на внешнем периметре

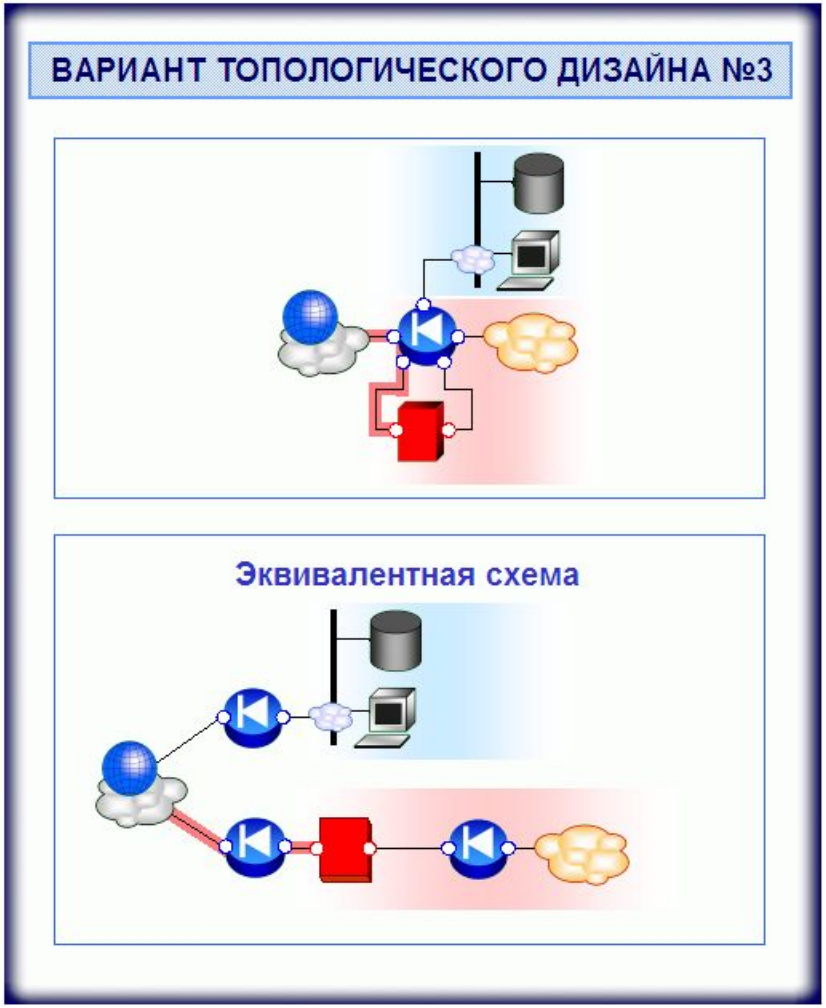


- В простейшем случае шифрованный туннель (IPsec/ESP) устанавливается между устройствами защиты внутренних периметров, а на внешнем периметре применяется сетевой контроль доступа (пакетная фильтрация)
- Эти сценарии достаточно надежны, поскольку IPsec-туннель полностью изолирует сети внутреннего периметра, а извне доступны только туннельные адреса IPsec-шлюзов, не принимающих открытого трафика

Варианты 1 и 2

- **Топологические варианты 1 и 2 по функциональности и по степени защищенности практически эквивалентны**
  - **отличие варианта 2 в том, что на туннельный адрес VPN шлюза не попадает открытый IP трафик**
- **Рекомендуется применение средств обнаружения проникновения, реализующих следующую политику безопасности:**
  1. **доступ к ресурсам внешнего периметра строго соответствует политике пакетной фильтрации**
  2. **на VPN-шлюз проходит только IKE/IPsec и технологический трафик**
  3. **VPN-шлюз не выдает открытого IP-трафика**

Вариант 3

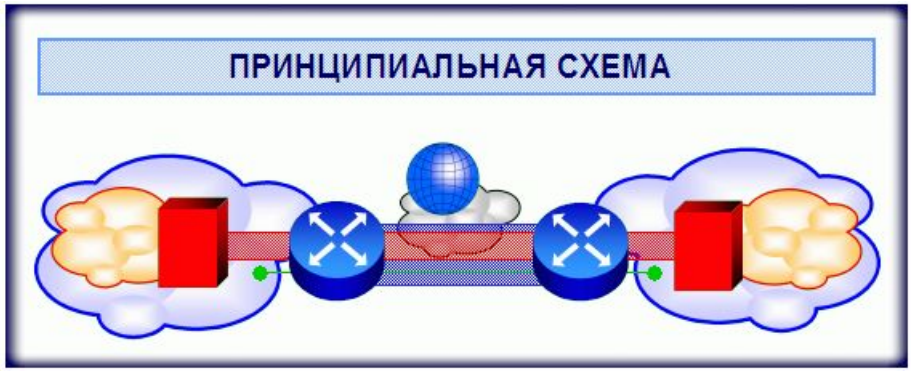


- **Вариант 3 является популярной схемой, поскольку обеспечивает повторное использование входного межсетевого экрана для контроля доступа применительно к расшифрованному трафику внутреннего периметра**
  - **основанием для применения этой схемы является то, что межсетевые экраны и маршрутизаторы Cisco реализуют независимые политики пакетной фильтрации трафика на различных интерфейсах устройства (см. эквивалентную схему)**
  - **при этом, однако, делается неявное предположение о доверии к устройству, обрабатывающему одновременно транзитный трафик внешнего и внутреннего периметров**

Туннель на внешнем периметре

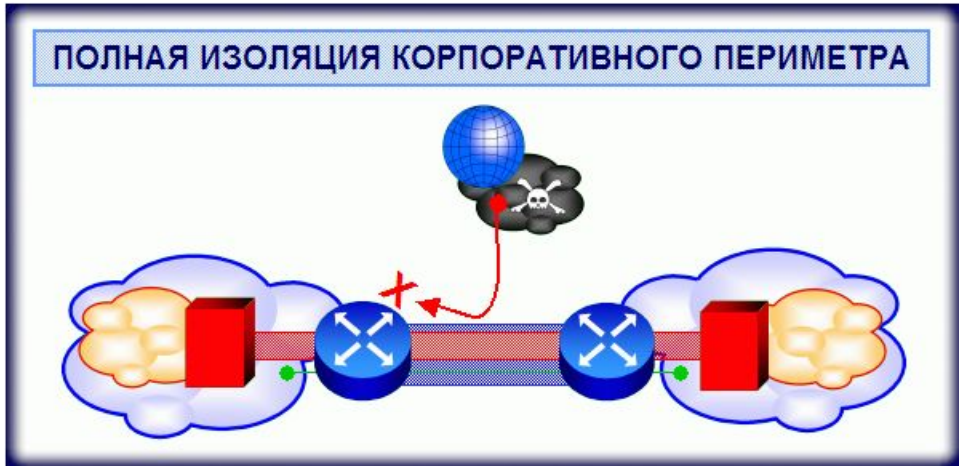
s·terra
c s p
Cisco Solution Technology Integrator

Туннелирование на внешнем периметре



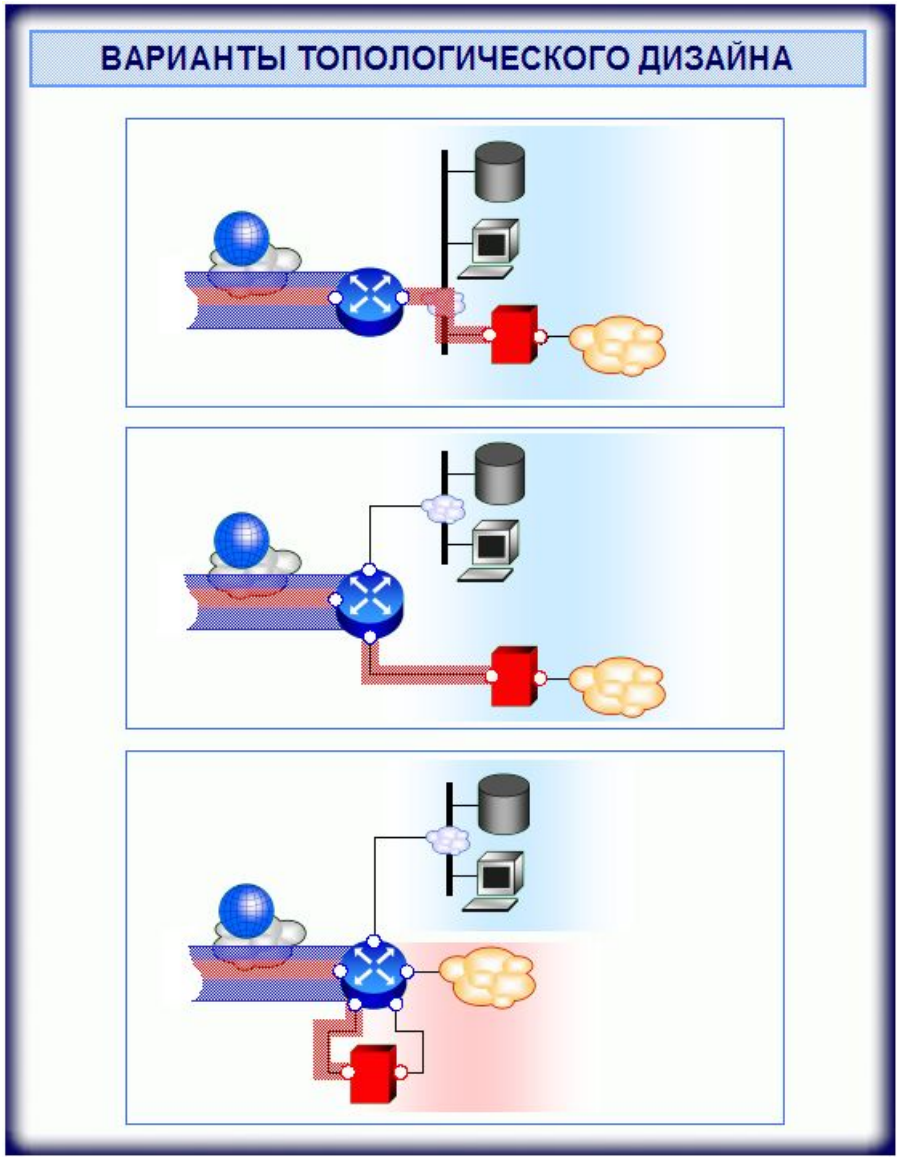
- **Наиболее надежным представляется сценарий защиты внешнего периметра , когда весь межсетевой трафик «упаковывается» в туннель между устройствами защиты внешних периметров (*изоляция корпоративной сети*)**
  - **это может быть MPLS-туннель**
  - **или IPsec-туннель**
    - **нешифрованный туннель IPsec/AH**
    - **шифрованный туннель (IPsec/ESP/[AH])**

Дополнительные факторы защиты



- В сценариях с туннелированием на внешнем периметре все внутренние взаимодействия скрыты от внешних наблюдателей (Интернет); несанкционированный доступ в сеть практически исключен
  - внутрь внешнего периметра может попасть только тот, кто знает секретный ключ, либо имеет сертификат корпоративного PKI
    - т.е., при правильной политике работы с ключами/ сертификатами проникновение постороннего практически исключено
- Это – классический пример *архитектуры интранет*

Топологический дизайн



- Топологический дизайн и политика безопасности межсетевых взаимодействий при использовании туннелирования на внешнем периметре практически совпадают с аналогичными дизайном и топологией для случая пакетной фильтрации
- Различие состоит в том, что на внешнем периметре исключается доступ в Интернет и устанавливается политика туннелирования

Взаимодействие периметров

s-terra
c s p
Cisco Solution Technology Integrator

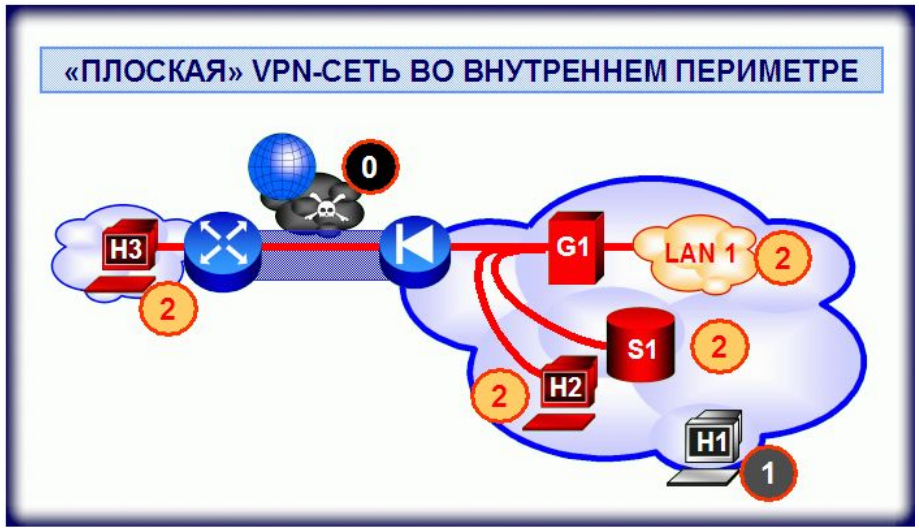
Защита при взаимодействии периметров

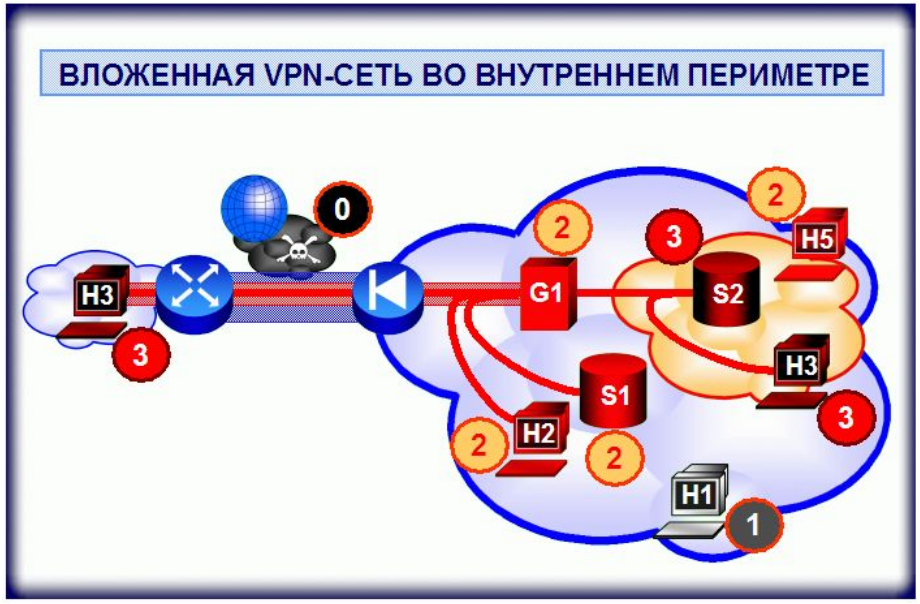
1. Пакетная фильтрация с сохранением контекста (stateful inspection)
2. Особый топологический дизайн (буферная зона, DMZ, проксирование)
3. Строгая (в т.ч. многофакторная) аутентификация
4. Применение средств анти-вирусной профилактики, контроля мобильного кода
5. Применение средств обнаружения проникновения, тревожной сигнализации, мониторинга, событийного протоколирования
6. Применение мер защиты информации прикладного уровня

Вложенные VPN

s·terra
c s p
Cisco Solution Technology Integrator

Конфиденциальность во внутр. периметре





- **VPN сеть может иметь достаточно сложную топологическую структуру при одноуровневой модели конфиденциальности/ доверия (верхний рисунок)**
  - **уровень доверия 0: ресурсы Интернет**
  - **уровень доверия 1: ресурсы внешнего периметра (например, хост H1)**
  - **уровень доверия 2: ресурсы VPN (сервер S1, хосты H2 и H3, шлюз G1 и защищаемая им подсеть LAN 1)**
- **На нижнем рисунке показана вложенная VPN-сеть, образованная сервером S2 и двумя клиентскими хостами H3 и H4 с уровнем доверия 3**
  - **при этом ресурсы с уровнем доверия 2 «видят» трафик этой сети только в шифрованном виде, а ресурсы с уровнем доверия 1 даже не знают о существовании сети с уровнем доверия 3 (не видят ее пакетов вообще)**

Критерии выбора продуктов

s-terra
c s p
Cisco Solution Technology Integrator

Производительность канала связи

- **Основным критерием выбора шлюзов безопасности для защиты межсетевых взаимодействий является производительность, которая должна соответствовать реальной скорости канала передачи данных**
  - **рекомендации по применению шлюзов безопасности сделаны на базе *номинальных производительностей устройств,* рассчитанных для реальной статистики трафика**
    - **номинальная производительность в 3-5 раз ниже пиковой, измеренной на пакетах размером 1500 килобайт**
    - **в случае, если шлюз будет использоваться исключительно для защиты голосового трафика, целесообразно использовать шлюзы повышенных производительностей**
- **Продукты CSP VPN и NME-RVPN покрывают практически весь спектр скоростей современных каналов связи**

Скорость канала передачи данных

	CSP VPN Gate 100	CSP VPN Gate 1000	ISR 28xx + NME-RVPN	CSP VPN Gate 3000	ISR 3825 + 2 x (NME-RVPN)	ISR 3845 + 4 x (NME-RVPN)	CSP VPN Gate 7000	CSP VPN Gate 10000
Выделенные и коммутируемые каналы связи (до 2 Мбит/с)	■	■						
«Широкополосный Интернет», xDSL (до 10 Мбит/с)	■	■	■					
OC-1, Ethernet 100BaseT (до 100 Мбит/с)		■	■	■	■	■		
OC-3 (155 Мбит/с)				■	■	■	■	■
OC-12 (622 Мбит/с)						■	■	■
Модуль узла защиты гигабитного канала связи							■	■

Выбор типа лицензии

- Лицензия на шлюз безопасности определяет число одновременно поддерживаемых VPN-соединений (IPsec SA)
- Помимо номинальных лицензий шлюзов безопасности, существует три типа специальных лицензий:
  - «B» (Gate 100B и Server B) – применяется для защиты автономных систем (банкоматов в платежных сетях)
  - «V» – применяются в голосовых сетях и в сетях с высокой удельной долей IP-телефонов; поскольку IP-телефоны работают напрямую друг с другом, лицензии «V» расширяют количество одновременно устанавливаемых соединений
  - «Security Bundle» – лицензия для модулей NME-RVPN с неограниченным количеством соединений

Сегментирование сети и периферия

- Шлюзы безопасности при помощи различных сетевых интерфейсов позволяют подключать к VPN независимое изолированные сегменты ЛВС и реализовать для них различные (независимые) политики безопасности
- Число сетевых интерфейсов шлюзов зависит от аппаратной платформы
  - при необходимости на каждом физическом сетевом интерфейсе может быть сконфигурировано несколько виртуальных интерфейсов
  - помимо Ethernet-портов могут использоваться последовательные порты, на которых, при использовании проводных или GPRS-модемов, могут быть организованы резервные каналы связи
- На шлюзах серий 3000, 7000 и 10000 при помощи специализированных адаптеров могут поддерживаться WAN-протоколы (V.35, RS 530, X.21, G.703, G.704, G.823)

Cisco ISR с модулем NME-RVPN

- Маршрутизаторы Cisco ISR с модулями NME-RVPN обеспечивают возможность применения в VPN чрезвычайно широкого спектра периферии:
  - для организации множества защищенных сегментов могут применяться дополнительные сетевые интерфейсы и встроенные в маршрутизатор коммутаторы, встроенные беспроводные точки доступа
  - для организации WAN-каналов могут применяться синхронные и асинхронные многопортовые адаптеры последовательных портов, встроенные серверы доступа и карты WAN-интерфейсов, ATM, FR, адаптеры спутниковых систем связи IP VSAT Satellite WAN module, модули интеграции с сетями цифровой телефонии
- Маршрутизаторы с модулями NME-RVPN могут применяться как платформы для ряда защищенных сетевых приложений и сервисов информационной безопасности:
  - сервисы компрессии данных
  - Call Manager Express («АТС» IP-телефонии), голосовая почта
  - сервисы мониторинга и управления
  - контентные фильтры, анализаторы трафика, IDS/IPS, антивирус и проч.

Характеристики платформ

	CSP VPN Gate 100	CSP VPN Gate 1000	ISR 28xx + NME-RVPN	CSP VPN Gate 3000	ISR 3825 + 2 x (NME-RVPN)	ISR 3845 + 4 x (NME-RVPN)	CSP VPN Gate 7000	CSP VPN Gate 10000
Число процессоров/RAM (MB)	1/512M	1/512M	1/512M [1]	1/1G+	1-2 [2]	1-4 [2]	2/1G+	4/2G+
Compact Flash/HDD/Disk on Module	512M CF/DoM	1G DoM/HDD	512M CF	36G+ HDD	512M CF	512M CF	36G+ HDD	36G+ HDD
Ethernet 10/100 Mbps	3	2(3)	2 [3]	-	-	-	-	-
Ethernet 1000 Mbps	-	-	1 [4]	2-4	1-2 [4]	1-4 [4]	2-6	2-6
Serial/USB ports	2/2	1/2	*/1(2) [5]	1/2	*/1-2(2) [5]	*/1-4(2) [5]	1/2	1/2
Число VPN-туннелей (тип лицензии) [6]	5(B)/10/ 200(V)	50/ 500(V)	500/∞ (S.Bndl)	1000	500/ ∞ (S.Bndl)	500/ ∞ (S.Bndl)	∞	∞
Производитель аппаратных платформ	Kraftway	Kraftway	Cisco	Kraftway, HP, IBM, Sun	Cisco	Cisco	Kraftway, HP, IBM, Sun	Kraftway, HP, IBM, Sun

[1] - процессор/память на модуле NME-RVPN
[2] - по числу модулей NME-RVPN
[3] - встроенные интерфейсы шасси 28xx; доступен набор опций
[4] - интерфейсы модулей NME-RVPN; дополнительно: 2 встроенных интерфейса шасси + набор опций
[5] - последовательные порты устанавливаются в качестве опций; 1 USB порт на модуле, 2 – в шасси
[6] - типы лицензий: «B» - автономные устройства, банкоматы; «V» - расширенная лицензия для голосовых сетей; «S.Bndl» - расширенная лицензия NME-RVPN Security Bundle

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