КРИПТОНИТ

Создание стенда тестирования совместимости отечественных СКЗИ

Спиридонов Александр,
руководитель лаборатории
информационной и сетевой
безопасности
АО «НПК «Криптонит»

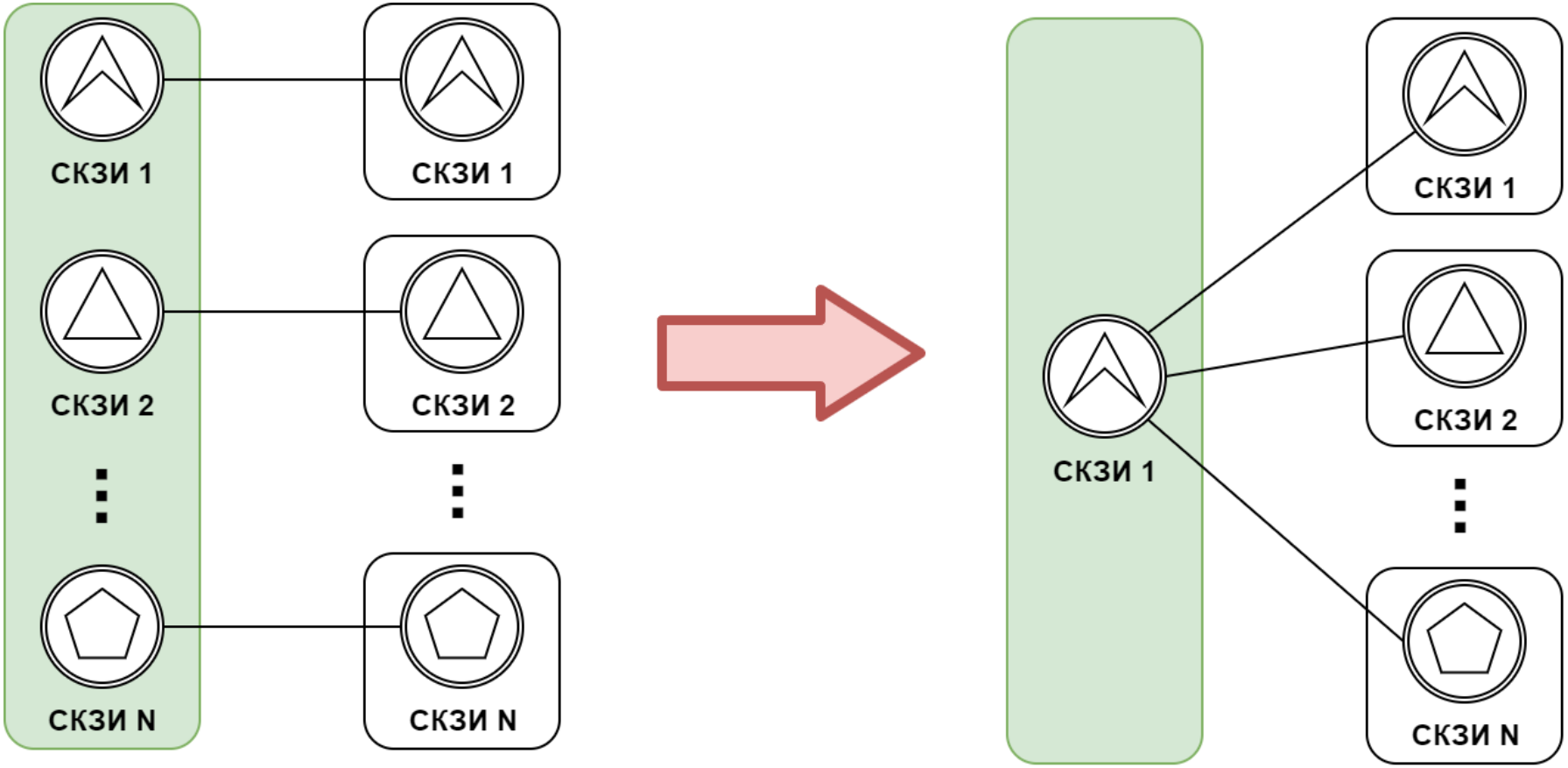
О нас

НПК «Криптонит» — центр компетенций в области научных исследований и опытных разработок

Приоритетные направления исследований:

- Криптография и квантовые вычисления
- Машинное обучение, нейросети
- Обработка больших данных
- Сетевая и информационная безопасность
- Новые телекоммуникационные стандарты и их безопасность

Проблема совместимости СКЗИ



Методика проведения тестовых испытаний совместимости СКЗИ, реализующих российские криптографические алгоритмы для протоколов TLS 1.2, TLS 1.3 и IPsec IKEv2

- Приложение 1: сценарии тестовых испытаний для протоколов TLS 1.2 , TLS 1.3
  - TLS 1.2 - 6 сценариев
  - TLS 1.3 - 4 сценария
- Приложение 2: сценарии тестовых испытаний для протокола IPsec IKEv2
  - 20 сценариев

Сценарии тестирования для протокола TLS 1.2

Проверка	Варианты
Схема обмена сообщениями в протоколе Handshake	Полная/Session ID/Session Ticket
Тип аутентификации	Односторонняя/двусторонняя
Сертификат сервера ГОСТ Р 34.10-2012	W256/W512/Ed256/Ed512
Сертификат клиента ГОСТ Р 34.10-2012	W256/Ed512
Криптонабор	KUZNYECHIK/MAGMA/28147
Расширение renegotiation_info	Пустое/verify_data
Расширение extended_master_secret	Да/нет
Смены ключей защиты TLS записей	

Сценарии тестирования для протокола TLS 1.3

Проверка	Варианты
Схема выработки ключа	ecdhe_ke/psk_ke/psk_ecdhe_ke
Тип аутентификации	cert/iPSK/ePSK
Кривые для ECDHE (ГОСТ Р. 34.10-2012)	W256/Ed512/Ed256
Кривые для подписи (ГОСТ Р. 34.10-2012)	W256/W512
Криптонабор	Kuznyechik-S/Kuznyechik-L Magma-S/Magma-L
Сообщение HelloRetryRequest	
Post-handshake аутентификация	
Сообщение NewSessionTicket	
Сообщение KeyUpdate	
Защита TLS записей	TLSTREE/zero padding

Сценарии тестирования для протокола IPsec IKEv2

Проверка	Варианты
IKEv2 соединение	ENCR_MAGMA_MGM_KTREE/ ENCR_KUZNYECHIK_MGM_KTREE PRF_HMAC_STRIBOG_512 GOST3410_2012_256/GOST3410_2012_512
ESP соединение	ENCR_KUZNYECHIK_MGM_KTREE ENCR_MAGMA_MGM_KTREE ENCR_KUZNYECHIK_MGM_MAC_KTREE ENCR_MAGMA_MGM_MAC_KTREE
«Узкое» ESP SA ICMP соединение	
«Узкое» ESP SA TCP соединение	
ESP соединение без NAT Traversal	
IKE over TCP	
IPsec Re-keying	Со стороны инициатора/ответчика
DELETE_PAYLOAD IPSEC SA	Со стороны инициатора/ответчика

Этапы тестирования

1. Подача заявки (gost@kryptonite.ru)
2. Подготовка индивидуального стенда («белые» IP адреса, все сертификаты выданы тестовым УЦ)
3. Проведение тестирования (самостоятельное)
4. Составление акта по результатам тестирования

Поддерживаемые стандарты

- Стенд тестирования протокола TLS
  - TLS 1.2 (криптонаборы 0xFF85, 0xC102 - ГОСТ 28147-89)
  - TLS 1.2 (криптонаборы 0xC100 – «Кузнечик», 0xC101 – «Магма») – октябрь - ноябрь 2020
  - TLS 1.3 - 2021 год

- Стенд IPsec IKEv2
  - RFC 7296 (IKEv2), RFC 4555 (IKEv2 MOBIKE) …
  - Using GOST ciphers in ESP and IKEv2 (draft-smyslov-esp-gost)
  - Using GOST algorithms in IKEv2 (draft-smyslov-ike2-gost)

Стенд тестирования протокола TLS

Программные компоненты:

- ОС Ubuntu 18.04
- Библиотека OpenSSL 1.1.1
- Модуль gost-engine

Состав:

- TLS-сервер с сертификатом подписи ГОСТ Р 34.10-2012 256 бит
- TLS-сервер с сертификатом подписи ГОСТ Р 34.10-2012 512 бит
- TLS-клиент

Схема сети стенда тестирования сервера TLS

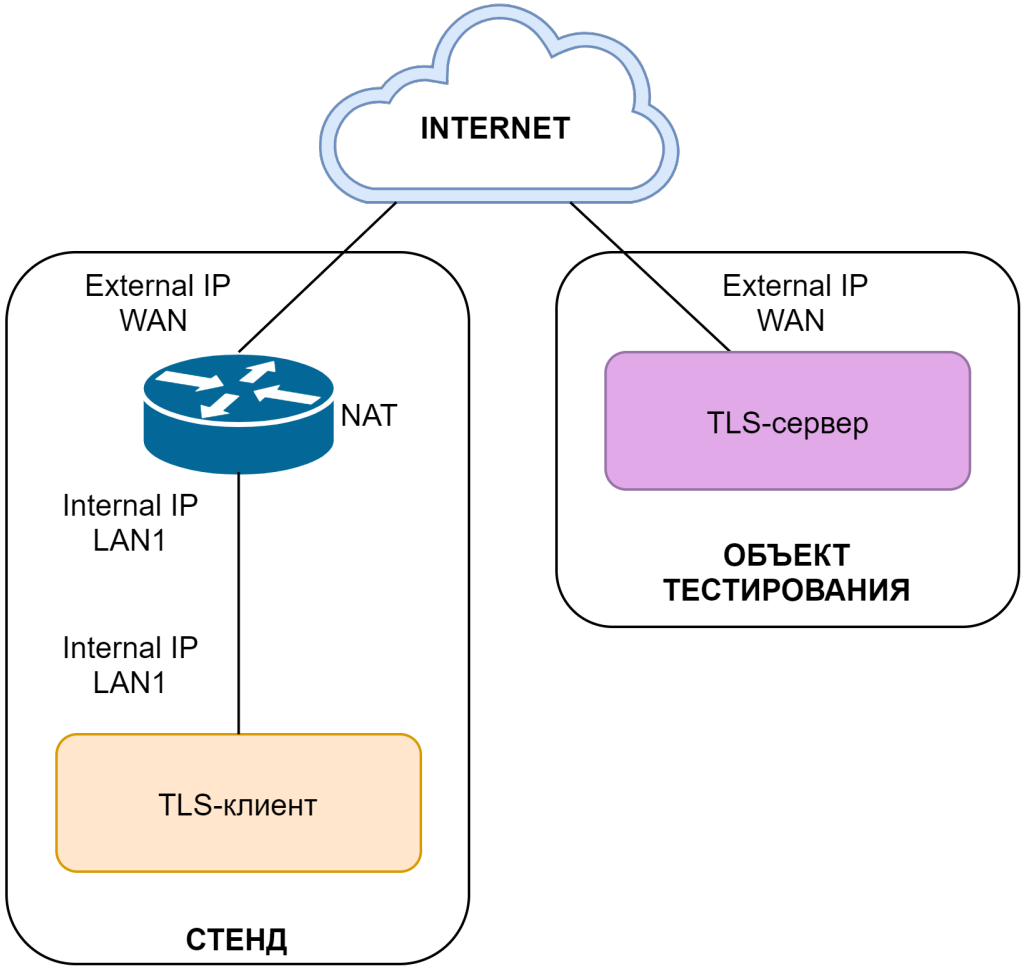
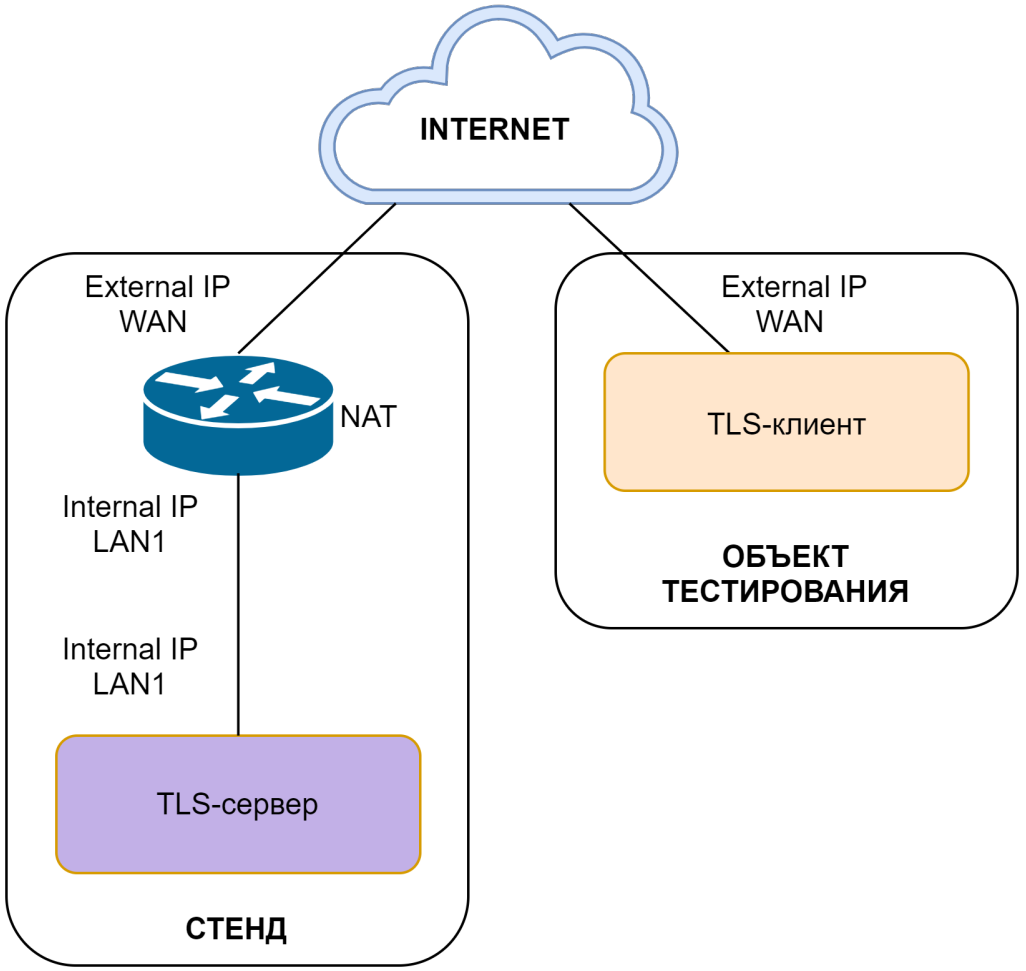


Схема сети стенда тестирования клиента TLS



Стенд тестирования протокола IPsec IKEv2

Программные компоненты:

- ОС Windows Server 2016
- Программный комплекс (IPsec шлюз) «ЗАСТАВА-Офис»
- Криптопровайдер КриптоПро CSP 5.0

Состав:

- IPsec IKEv2 шлюз с прямым подключением к сети Интернет
- IPsec IKEv2 шлюз с подключением к сети Интернет через NAT
- 2 IP Host

Схема сети стенда тестирования протокола IPsec IKEv2 с прямым подключением

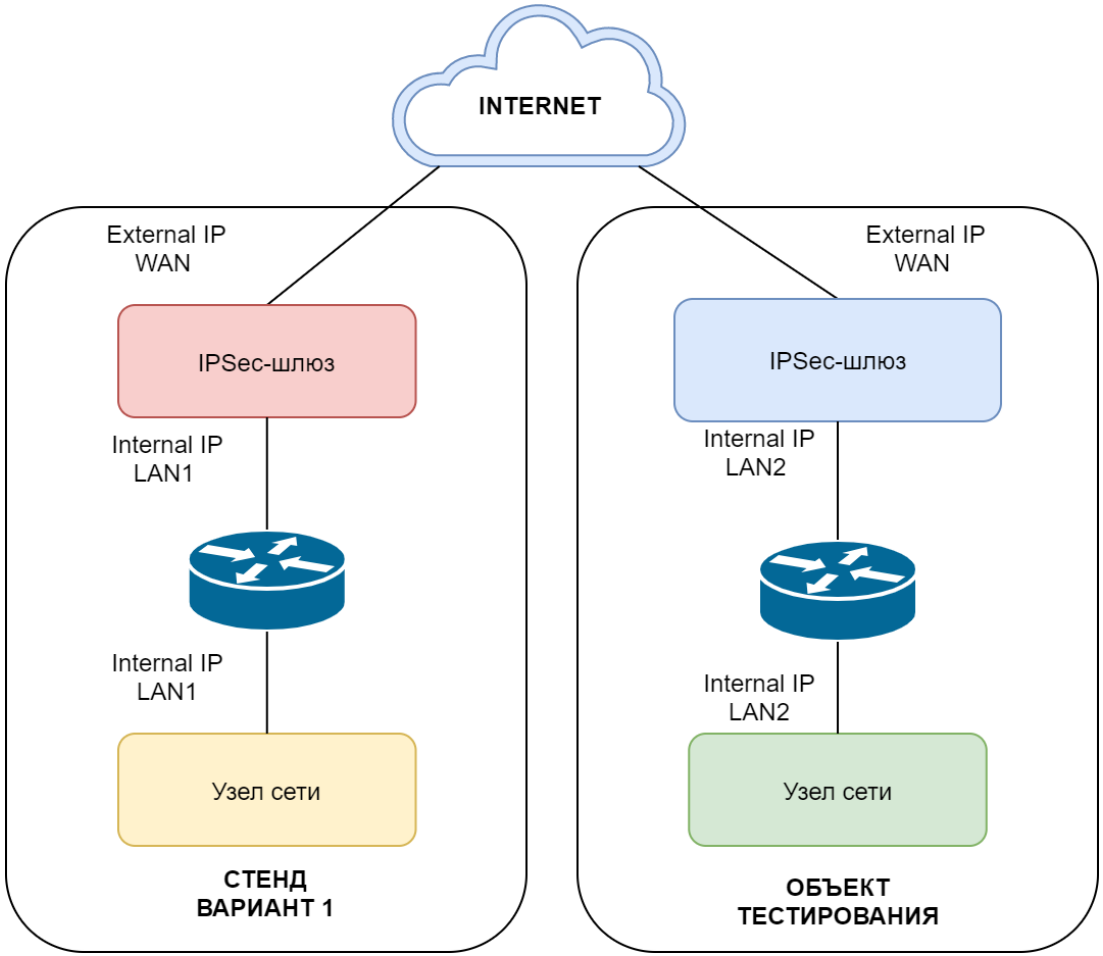
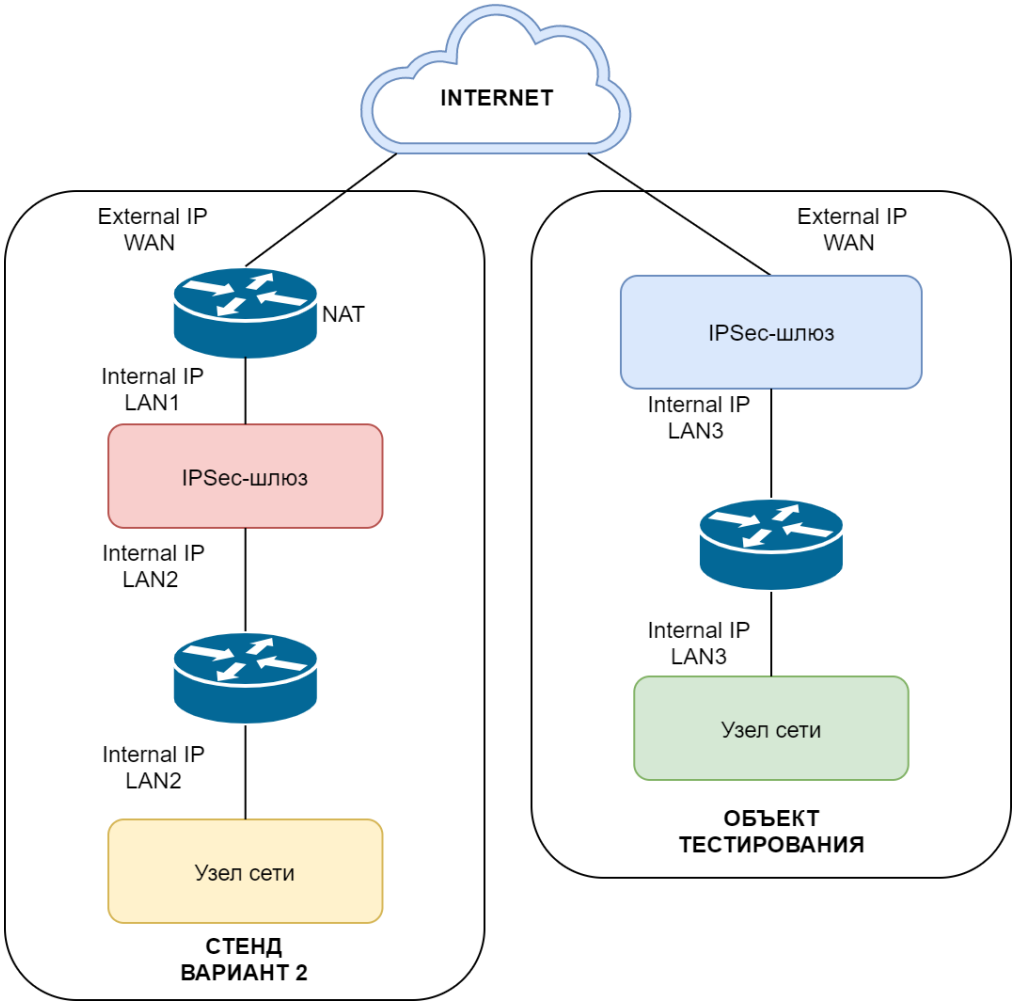


Схема сети стенда тестирования протокола IPsec IKEv2 с подключением через NAT



Спасибо за внимание!

https://gost.kryptonite.ru
gost@kryptonite.ru

Вопросы?