САЙФЕР

Система криптографической защиты информации Шифр-VPN

Защищенные виртуальные сети

ООО “Сайфер БИС”: Влад Ковтун
Николай Байбуз

Agenda

- Зачем это нужно?
- Существующие решения
- На что обратить внимание
- Предложение от компании Сайфер - Сайфер Шифр-VPN
  - Описание
  - Состав
  - Варианты применения
  - Алгоритмы
  - Производительность
- Внедрения
- Вопросы ...

Зачем это нужно

- Организация защищенной связи внутри компании - между офисами, филиалами, удаленными подразделениями.
- Организация защищенной связи с партнерами или клиентами.
- Защита данных при передачи по открытым каналам связи с использованием национальных криптографических стандартов

Остро возникает необходимость при построения КСЗИ для распределенных ИТС.

Существующие решения

Производитель	Реализация сервера/клиента	Решение	Пропускная способность*, Мб/с	Уровень
ООО Автор	Программная	CryptoIP VPN	До 30	Транспортный (TCP, UDP)
ООО Автор	Аппаратная	CryptoIP	До 30	Сетевой (IP, IP Sec)
АО ИИТ	Аппаратная/Программная	Захист з'єднань-2 Барьер-301 mini Барьер-301	До 125 До 250	Транспортный (TCP)
АО ИИТ	Аппаратная/Аппаратная	Захист IP-потоку Канал-201 Канал-301 Канал-401	До 125 До 1000 До 1000-5000	Сетевой (IP)

*- для среднестатистического потока

Существующие решения

Производитель	Реализация сервера/клиента	Решение	Пропускная способность*, Мб/с	Уровень
ООО ИТ инжиниринг	Программная	Cisco UVPN (оборудование Cisco)	До 80 (SW) До 100 (HW) До 550 (HW) До 970 (HW)	Транспортный (TCP, UDP)
ООО ИТ инжиниринг	Программная	HP Encryptor UA (оборудование HPE)	До 900 (HW) До 60 (simple HW) До 95 (vSW)	Транспортный (TCP, UDP)

*- для среднестатистического потока

На что обратить внимание

- Гибкость и удобство управления ключами
- Удобство эксплуатации и интеграции
- Гибкость и удобство настройки сети
- Скорость передачи данных
- Перспективность (поддерживаемые алгоритмы)
- Ориентация на облачные технологии
- Широкий спектр поддерживаемых платформ

Что предлагает Сайфер?

Система криптографической защиты информации “Шифр-VPN”

СКЗИ Шифр-VPN

Система криптографической защиты информации Шифр-VPN представляет программный или программно-аппаратный комплекс, основанный на распространенном и проверенном временем протоколе OpenVPN с поддержкой SSL/TLS.

Может выполняться в защищенном аппаратном исполнении.

Основан на базе:

- Библиотек криптографических примитивов Шифр+ v2.1*
- Богатом опыте компании Сайфер

*-имеется действующее позитивное экспертное заключение Госспецсвязи

Преимущества протокола OpenVPN

Использование протокола OpenVPN на основе SSL/TLS обеспечивает:

- Прозрачность прохождения Firewall, Proxy, NAT по сравнению с LT2P/IPsec
- Более высокую производительность при меньшем объеме потребляемых вычислительных ресурсов по сравнению с LT2P/IPsec
- Поддержку протоколов транспортного уровня TCP, UDP
- Сжатие трафика с помощью алгоритмов LZO, ZIP
- Гибкость настройки на стороне клиентов, посредством предустановленных конфигурационных файлов

Ключи ЦСК/АЦСК

- Поддержка ключей изданных АЦСК
  - Проверка статуса сертификата по OCSP
  - Ведение список доверенных ЦСК на сервере VPN
  - Ведение список разрешенных пользователей на сервере VPN
- Поддержка ключей изданных внутренним ЦСК
  - Использование СКЗИ “Шифр-X.509” (возможна аккредитация)
  - Использование СКЗИ “Шифр-xCA” (для внутреннего использования):
    - RSA, ECDSA, ДСТУ 4145-2002
    - SHA-2, ГОСТ 34.311-95, ДСТУ 7564:2014
    - AES, ГОСТ 28147-89, ДСТУ 7624:2014

Ключевые носители

- Аппаратный ключевой носитель (пассивный режим)
  - Aladdin/SafeNet/Gemalto eToken
  - Автор SecureToken-337
  - Авест AvestKey
  - Эфит EfitKey
  - И другие
- Файловый ключевой носитель
  - PFX/PKCS#12 (АЦСК НДУ, АЦСК Ощадбанк и другие)
  - JKS (АЦСК Приватбанк)
  - Key-6.dat (ЦСК построенные на основе АО ИИТ)
  - PZ2 (АЦСК Украина, после конвертации в Key-6.dat)

Платформы и архитектура

- Аппаратные платформы
  - x86, x86-64 (AES NI, CLMUL, SSE, AVX)
  - ARMv6, ARMv7, ARMv8
- Операционные системы
  - Сервер: Windows, Linux, FreeBSD
  - Клиент: Windows, Linux, MacOS, Android*, iOS*
- Варианты использования
  - Клиент-Сервер
  - Сеть-Сеть (Сервер-Сервер)
- Ведение журнала аудита сервере
- Мониторинг состояния сервера

*-сторонних разработчиков, совместимость для международных криптографических алгоритмов

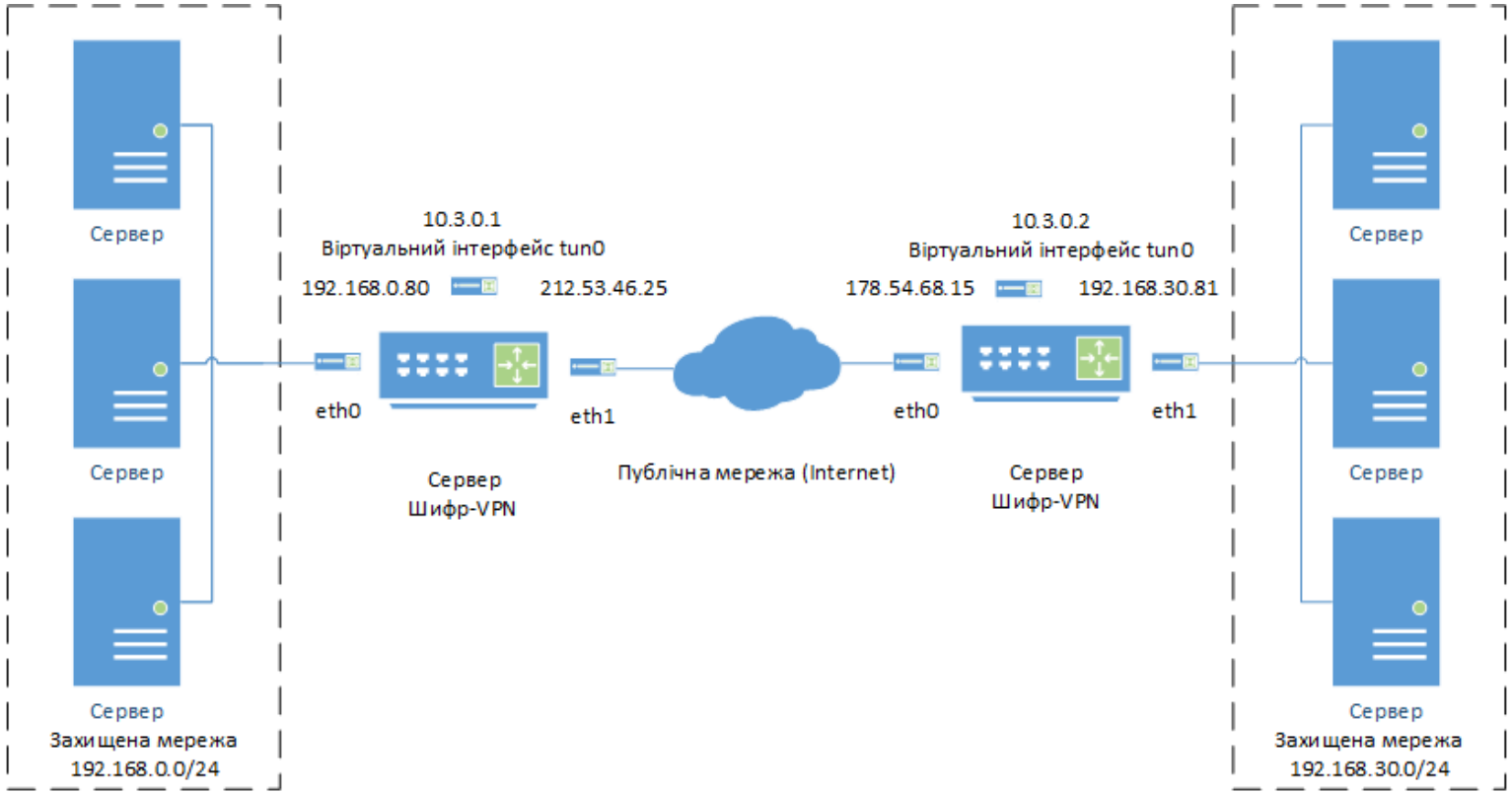
Интеграция и масштабирование

- Балансировка трафика
  - Несколько серверов VPN работают как один
- Агрегация трафика
  - Несколько виртуальных сетевых интерфейсов
- Параллельная работа нескольких серверов VPN
  - Несколько серверов VPN на одном физическом или виртуальном сервере, с разносом по портам
- Возможность работы как на физическом так и виртуальном оборудовании

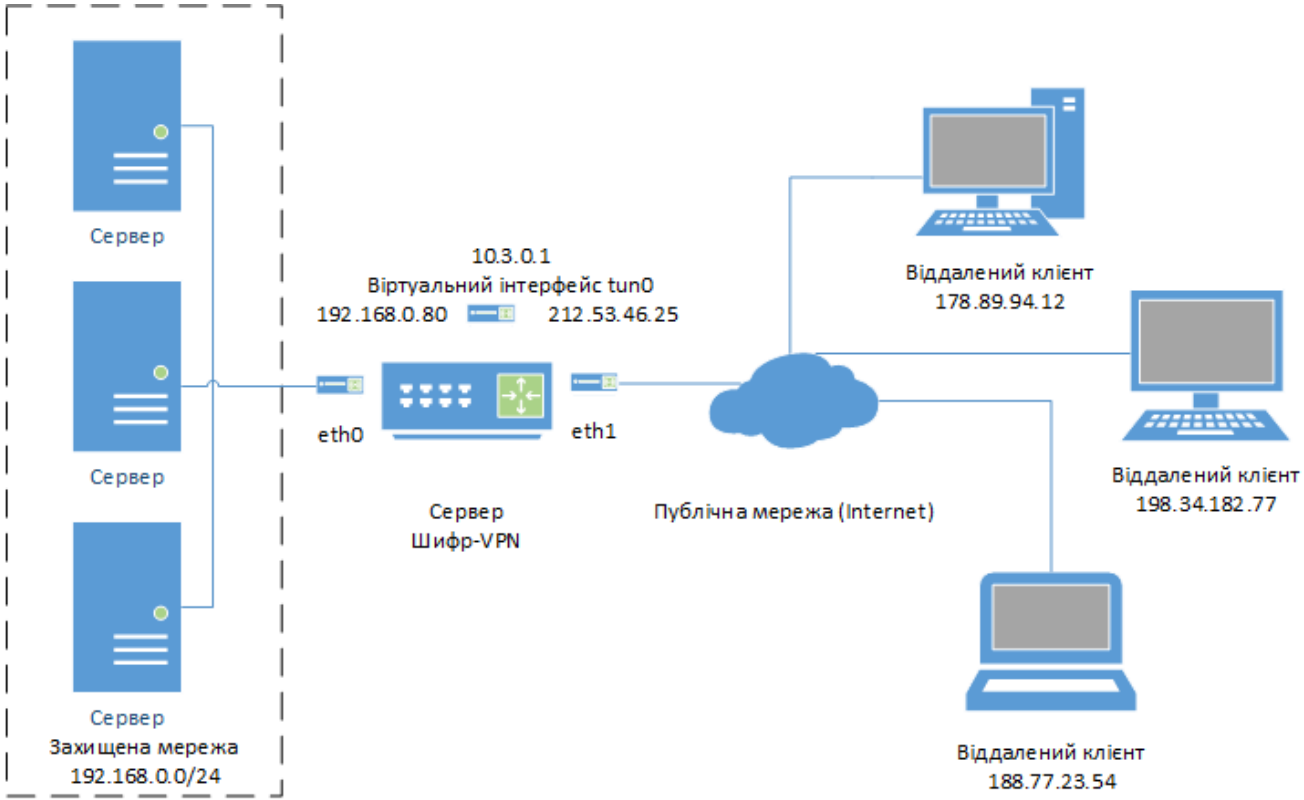
Описание

- Симметричное шифрование
  - ДСТУ 7654:2014
  - AES (128, 192, 256), поддержка аппаратного ускорения
  - ДСТУ ГОСТ 28147:2009
  - DEA/TDEA (64/192)
- ЭЦП
  - ECDSA (простое, двоичное поле), поддержка аппаратного ускорения
  - ДСТУ 4145:2002, поддержка аппаратного ускорения
  - RSA (PKCS#1 v1.5, v2.2)
- Хеш-функция
  - ДСТУ 7564:2014
  - ГОСТ 34.311-95
  - SHA-1, SHA-2

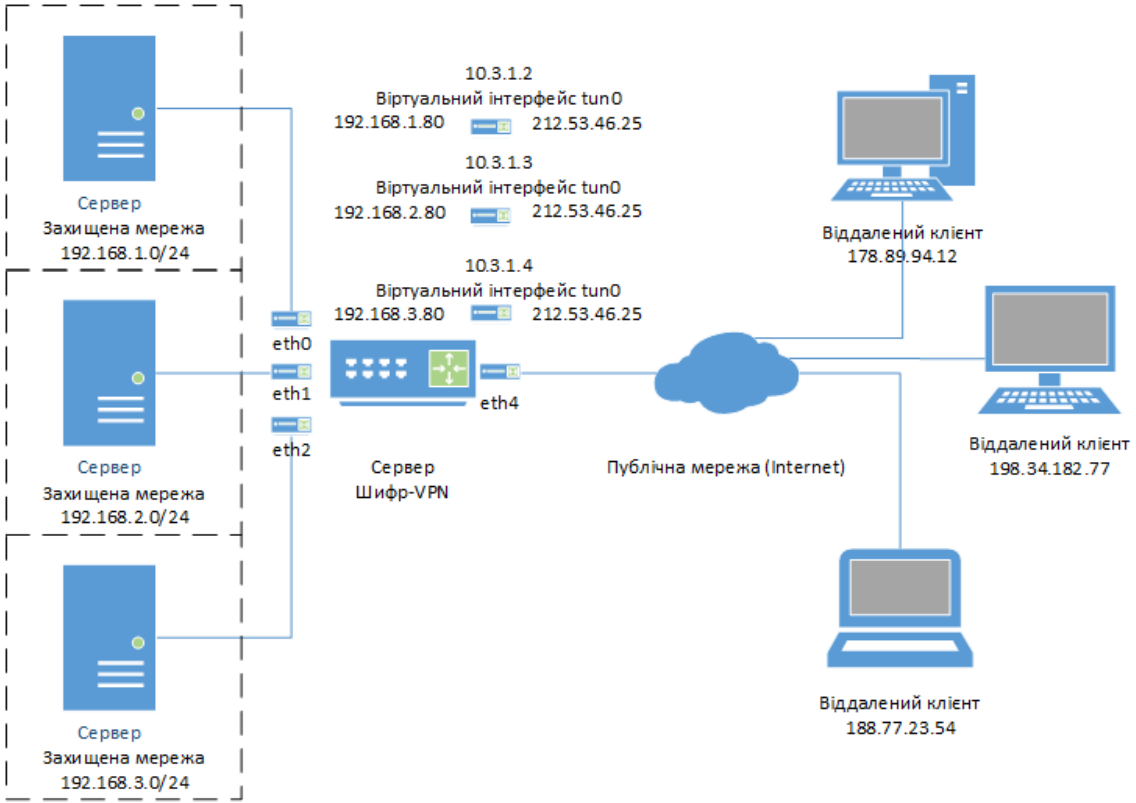
Сервер-Сервер (Сеть-Сеть)



Клиент-Сервер



Клиент-Сервер (разные сети)



Состав

- Построение защищенного туннеля Сервер-Сервер (Сеть-Сеть):
  - Сервер Шифр-VPN
  - Сервер Шифр-VPN
- Построение защищенного туннеля Клиент-Сервер (ключи АЦСК):
  - Сервер Шифр-VPN
  - Клиент Шифр-VPN
- Построение защищенного туннеля Клиент-Сервер (ключи своего ЦСК):
  - Сервер Шифр-VPN
  - Клиент Шифр-VPN
  - ЦСК Шифр-xCA (для генерации и управления ключами клиентов и серверов)
  - ЦСК Шифр-X.509 (для генерации и управления ключами клиентов и серверов)

Производительность (агрегация)*

Алгоритм	TCP, Mb/s	UDP, Mb/s
AES-256 (NI)	720	920
ГОСТ 28147-89	100	200
ДСТУ 7624:2014	500	900

*-пропускная способность показана при агрегации 4-х логических каналов VPN с использованием 4-х ядер процессора.

Сервер (физический):

- CPU: Intel Xeon E5450 3.0 GHz
- RAM: 8 GB
- HDD: 60 GB
- OS: CentOS Linux v7 x86-64

Клиент (физический):

- CPU: Intel Core i5-6400 2.7 GHz
- RAM: 16 GB
- HDD: 1 TB
- OS: Windows 10 x86-64

Производительность*

Алгоритм	TCP, Mb/s	UDP, Mb/s
AES-256 (NI)	190	290
ГОСТ 28147-89	30	55
ДСТУ 7624:2014	140	260

*-пропускная способность показана на одно ядро процессора. При необходимости, пропускная способность может быть увеличена за счет агрегации виртуальных каналов

Сервер (физический):

- CPU: Intel Xeon E5450 3.0 GHz
- RAM: 8 GB
- HDD: 60 GB
- OS: CentOS Linux v7 x86-64

Клиент (физический):

- CPU: Intel Core i5-6400 2.7 GHz
- RAM: 16 GB
- HDD: 1 TB
- OS: Windows 10 x86-64

ООО “Сайфер БИС”

Николай Байбуз: nb@cipher.kiev.ua

Влад Ковтун: vk@cipher.kiev.ua

Вопросы?

www: https://cipher.kiev.ua