

Гибкие решения для защиты каналов связи

Защищенные виртуальные сети с
использованием Шифр-VPN

ООО “Сайфер БИС”:

Влад Ковтун
Николай Байбуз

Agenda

- Зачем это нужно?
- Существующие решения
- На что обратить внимание
- Предложение от компании Сайфер
 - 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 передаче 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 | Сетевой (IP, IPSec) |
| ООО Автор | Аппаратная | CryptoIP | До 30 | Сетевой (IP, IPSec) |
| 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-поток 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) | Сетевой (IP, IPSec) |
| ООО ИТ инжиниринг | Программная | HP Encryptor UA (оборудование HPE) | До 900 (HW) До 60 (simple HW) До 95 (vSW) | Сетевой (IP, IPSec) |
| ООО ИТ инжиниринг | Программная | Quant | До 900 (HW) До 60 (simple HW) До 95 (vSW) | Сетевой (IP, IPSec) |

*- 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 LZ0, ZIP
- Гибкость настройки на стороне клиентов, посредством предустановленных конфигурационных файлов
- Поддержка различных криптографических алгоритмов

Ключи ЦСК/АЦСК

- Поддержка ключей изданных АЦСК
 - Проверка статуса сертификата по OCSP
 - Ведение списка доверенных ЦСК на сервере VPN
 - Ведение списка разрешенных пользователей на сервере VPN
- Поддержка ключей изданных внутренним ЦСК
 - Использование СКЗИ «Шифр-Х.509» (возможна квалификация)
 - Использование СКЗИ «Шифр-хСА» (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/PKCS#12 (ЦСК построенные на основе АО ИИТ)
 - PZ2 (АЦСК Украина)

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 сервера**
- **Мониторинг состояния сервера**

*-сторонних разработчиков, совместимость для международных криптографических алгоритмов

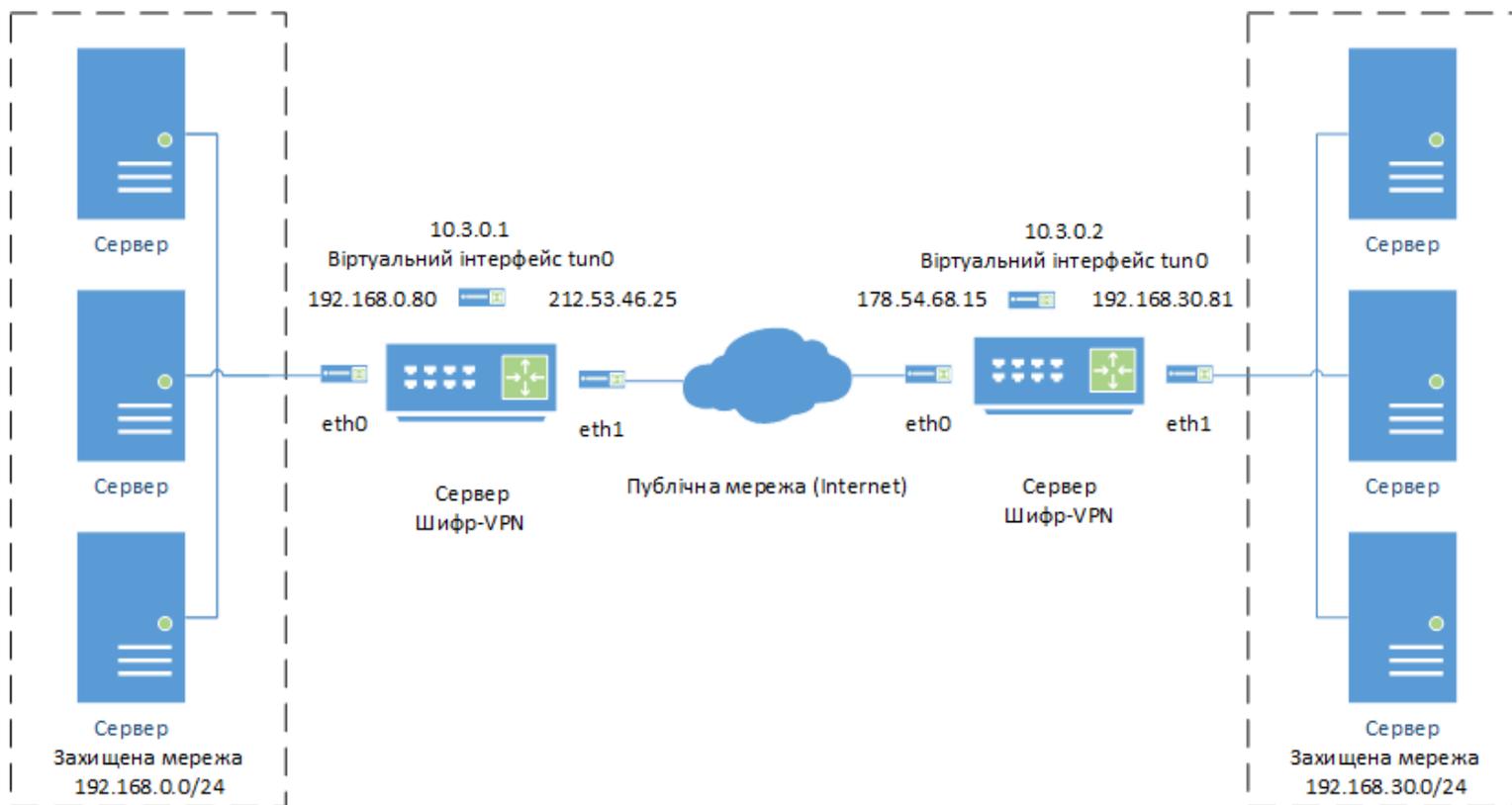
Интеграция и масштабирование

- 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, с маршрутизацией по разным сетям
- Возможность работы как на физическом так и виртуальном оборудовании

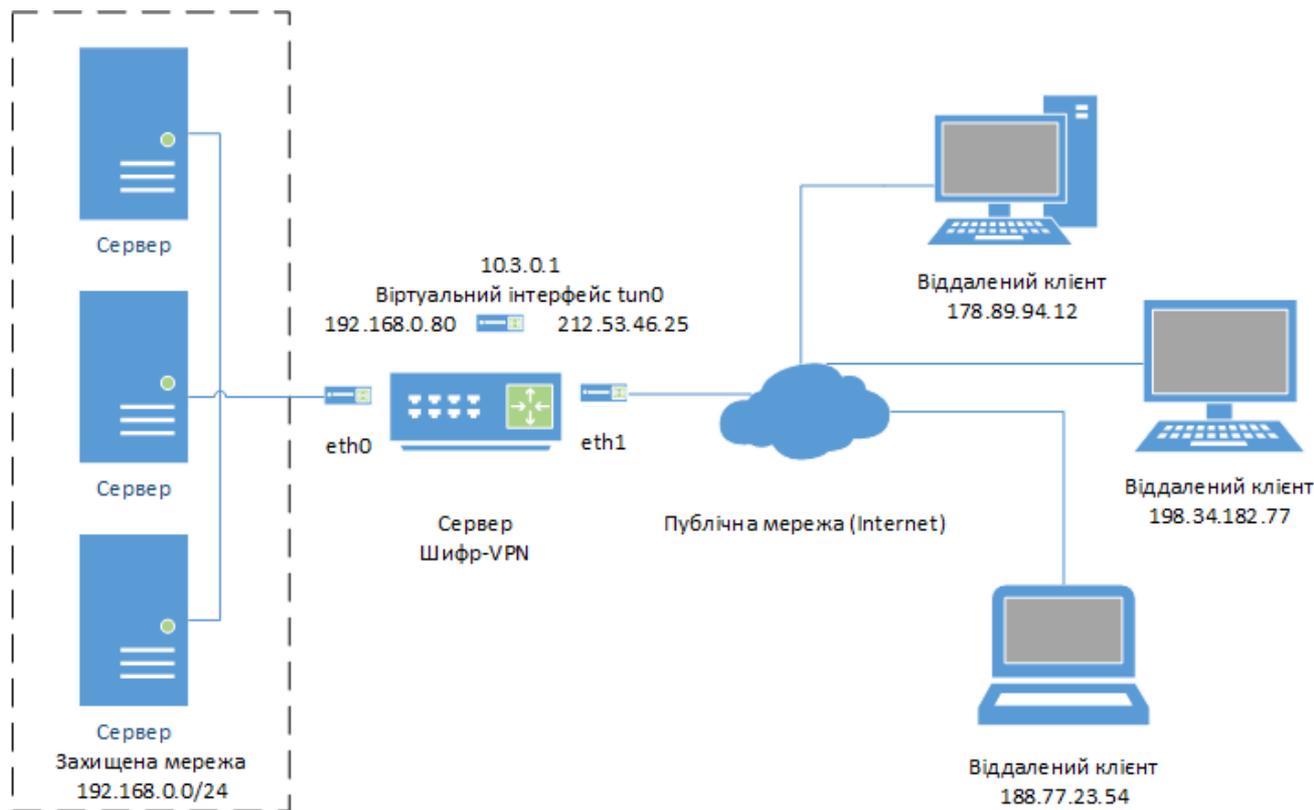
Описание

- Симметричное шифрование
 - ДСТУ 7654:2014, поддержка аппаратного ускорения
 - AES, поддержка аппаратного ускорения
 - ДСТУ ГОСТ 28147:2009
 - DEA/TDEA
- 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

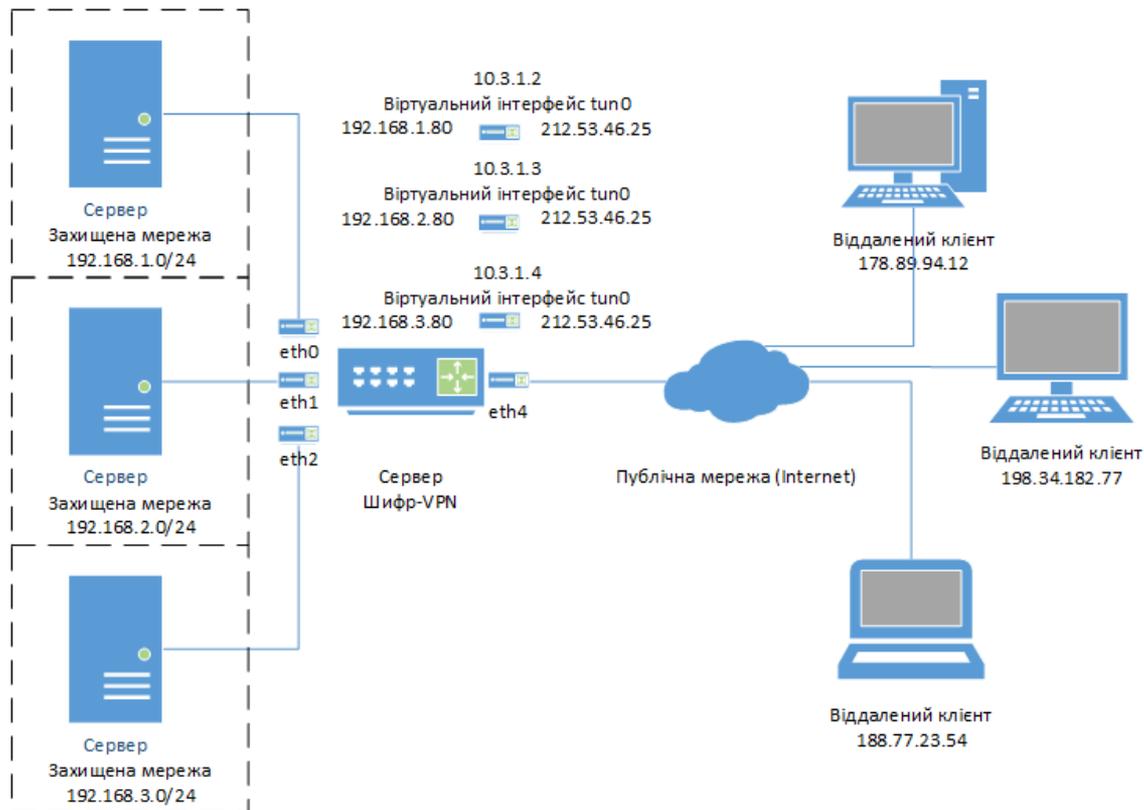
Сервер-Сервер (Сеть-Сеть)



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-хСА (для генерации и управления ключами клиентов и серверов)
 - ЦСК Шифр-Х.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

Внедрения*

Основные заказчики:

- Площадки системы Prozorro
- Государственные учреждения
- Банки

* - Более 20 масштабных внедрений

ООО «Сайфер БИС»

Николай Байбуз: nb@cipher.com.ua

Влад Ковтун: vk@cipher.com.ua

Вопросы?

www: <https://cipher.com.ua>