
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Меня хорошо видно && слышно?

Ставьте +, если все хорошо
Напишите в чат, если есть проблемы

IPSec

Кулиничев Алексей

Администратор Сетей

Santchous42@yandex.ru

Правила вебинара

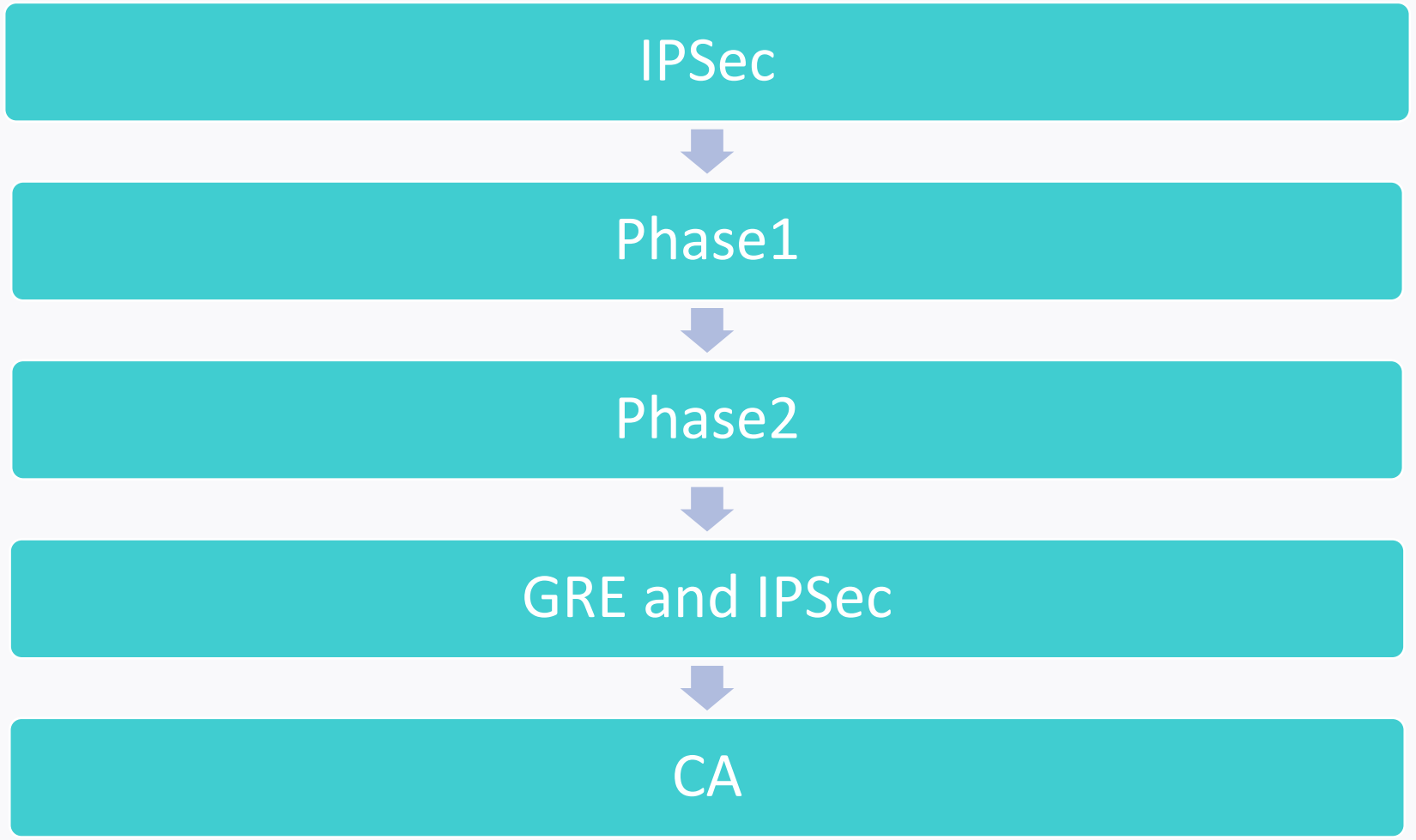
Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара



1 IPSec

IPSec

IPSec –набор протоколов, использующихся для обеспечения приватности и аутентификации на сетевом уровне модели OSI.

Эти протоколы можно разделить на два класса:

- протоколы защиты передаваемых данных (AH, ESP)
- протоколы обмена ключами (IKE)

IPSec

IPSec разработан для повышения безопасности протокола IP.

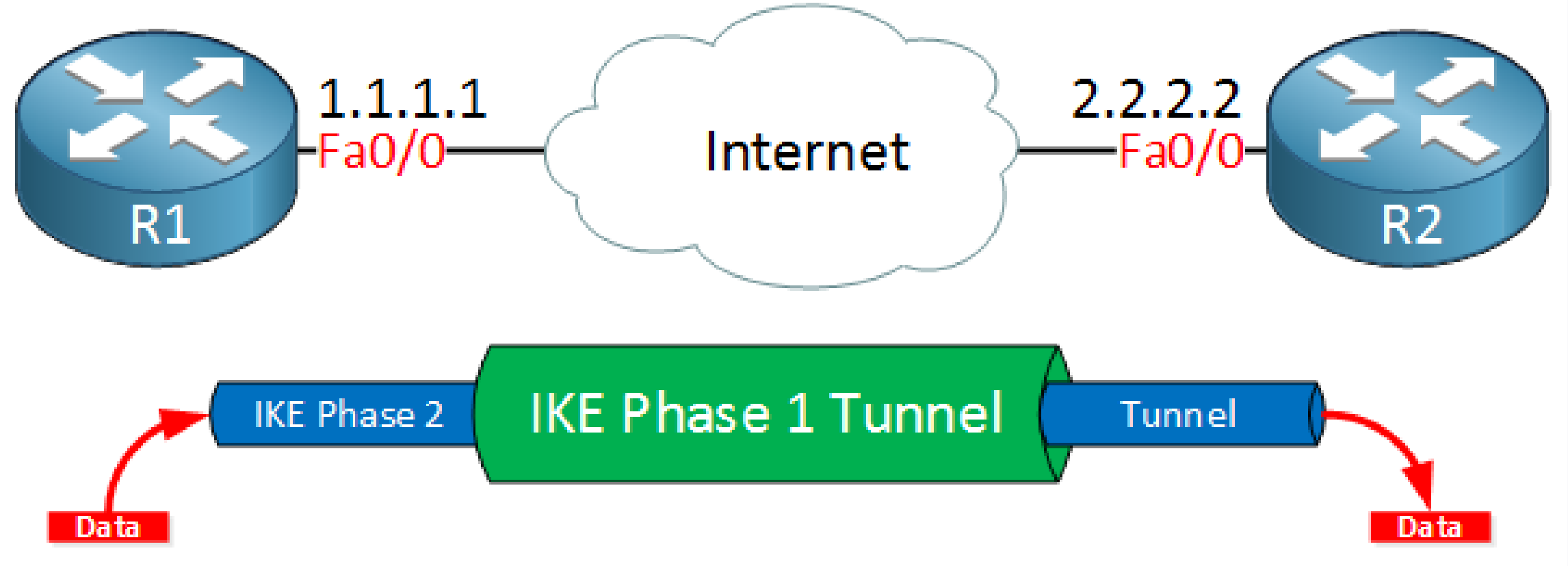
Безопасность достигается инкапсуляцией пакета IP в заголовки протоколов IPSec

IPSec не создает дополнительных интерфейсов на оборудовании

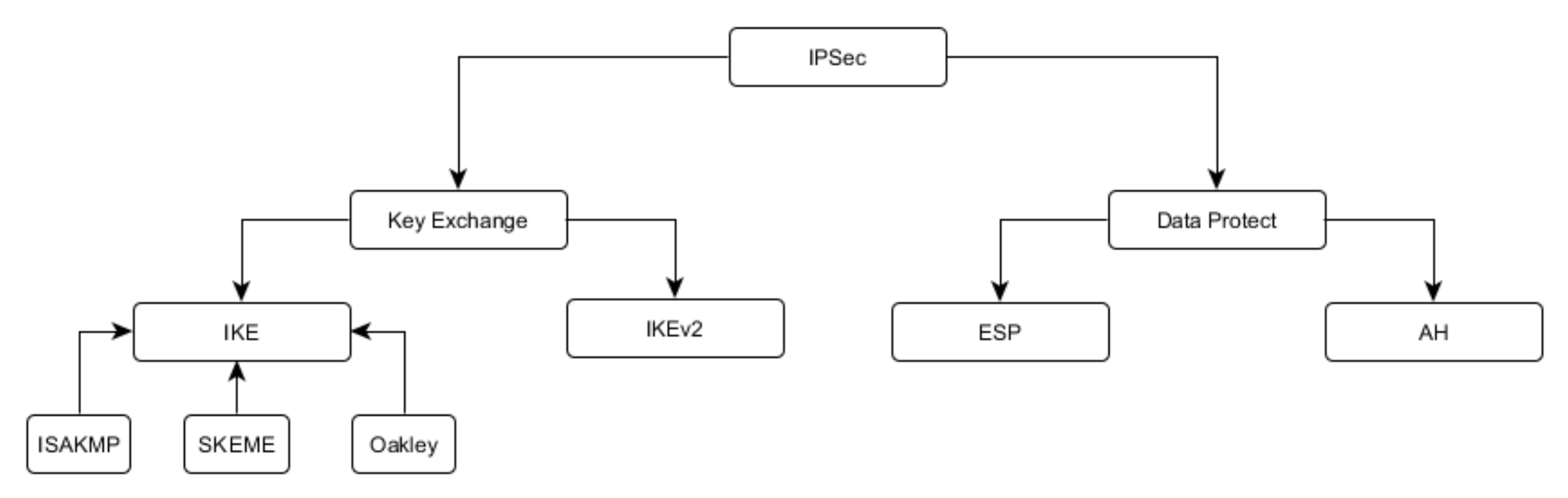
IPSec

Inside-to-Outside	Outside-to-Inside
• If IPSec then check input access list • decryption - for CET (Cisco Encryption Technology) or IPSec • check input access list • check input rate limits • input accounting • redirect to web cache • policy routing • routing • **NAT inside to outside (local to global translation)** • crypto (check map and mark for encryption) • check output access list • inspect (Context-based Access Control (CBAC)) • TCP intercept • encryption • Queueing	• If IPSec then check input access list • decryption - for CET or IPSec • check input access list • check input rate limits • input accounting • redirect to web cache • **NAT outside to inside (global to local translation)** • policy routing • routing • crypto (check map and mark for encryption) • check output access list • inspect CBAC • TCP intercept • encryption • Queueing

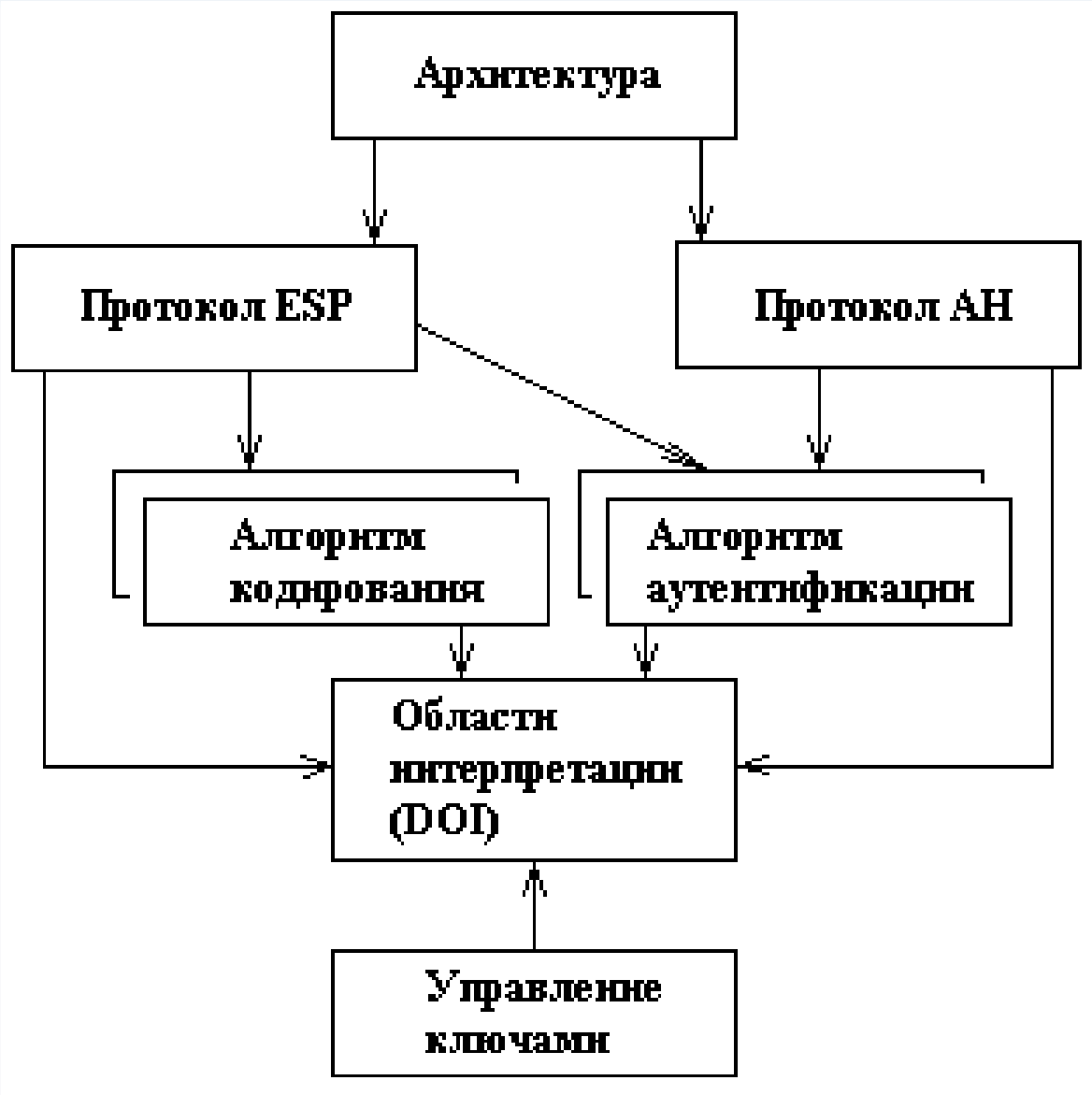
IPSec


1.1.1.1
Fa0/0
Internet
2.2.2.2
Fa0/0
R1
R2
IKE Phase 2
IKE Phase 1 Tunnel
Tunnel
Data
Data

IPSec


IPSec
Key Exchange
Data Protect
IKE
IKEv2
ESP
AH
ISAKMP
SKEME
Oakley

IPSec


Архитектура
Протокол ESP
Протокол AH
Алгоритм кодирования
Алгоритм аутентификации
Области интерпретации (DOI)
Управление ключами

IPSec

Туннель устанавливается в два этапа(фаза):

1. 1 фаза (Phase 1) – согласование метода идентификации, алгоритм шифрования, алгоритм хеширования и группа Diffie Hellman

2. 2 фаза (Phase 2) – генерируются ключи для шифрования данных. 2 фаза может начать работу только после установления первой фазы.

После согласования параметров и ключей во второй фазе туннель считается установленным и могут ходить данные.

IPSec

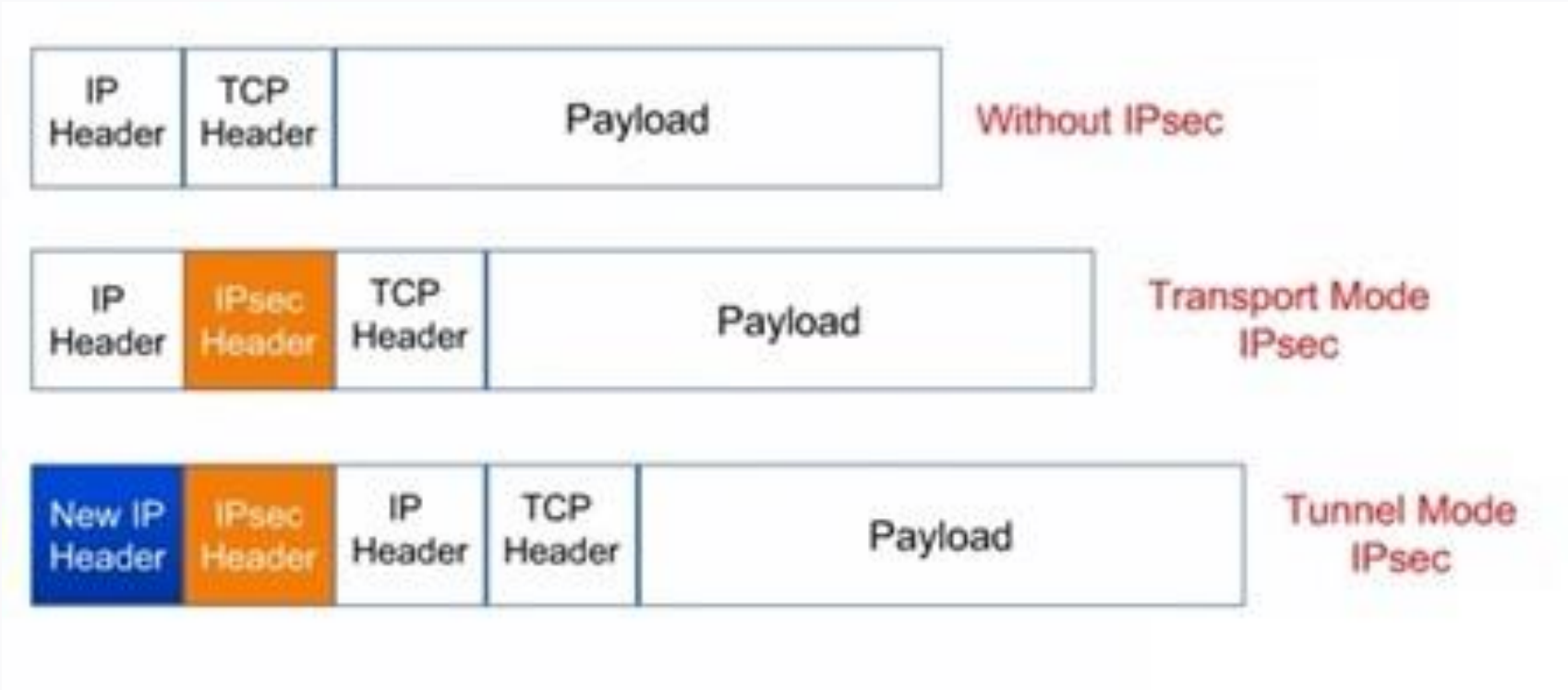
Два режима работы:

1. Транспортный
2. Туннельный

IPSec

Два режима работы:

1. Транспортный
2. Туннельный




2
Phase1

Phase1

Для согласования служебной информации работает протокол IKE(Internet Key Exchange) – формирует IPSec SA(Security Association – политики безопасности).

То есть IKE согласовывает работу пиров защищенного соединения:

- Алгоритм шифрования
- Проверка целостности
- Аутентификация

Phase1

Существует две версии протокола IKE

- IKEv1 – разработан в 1998г. На данный момент распространен и везде поддерживается
- IKEv2 – разработан в 2005. Интернет стандартом стал в 2014. На данный момент большинство оборудования поддерживает. Однако есть различия в реализациях у многих вендоров. Remote access(удаленные сотрудники) не у всех поддерживается до сих пор.

Phase1

Параметры первого туннеля – ISAKMP определяется политикой ISAKMP.

По шагам:

1. Согласование хеш-функций
2. Согласование алгоритмов шифрования
3. Обмен ключами Диффи-Хеллмана (DH)
4. Аутентификация

При прохождении всех шагов устанавливается ISAKMP-туннель.

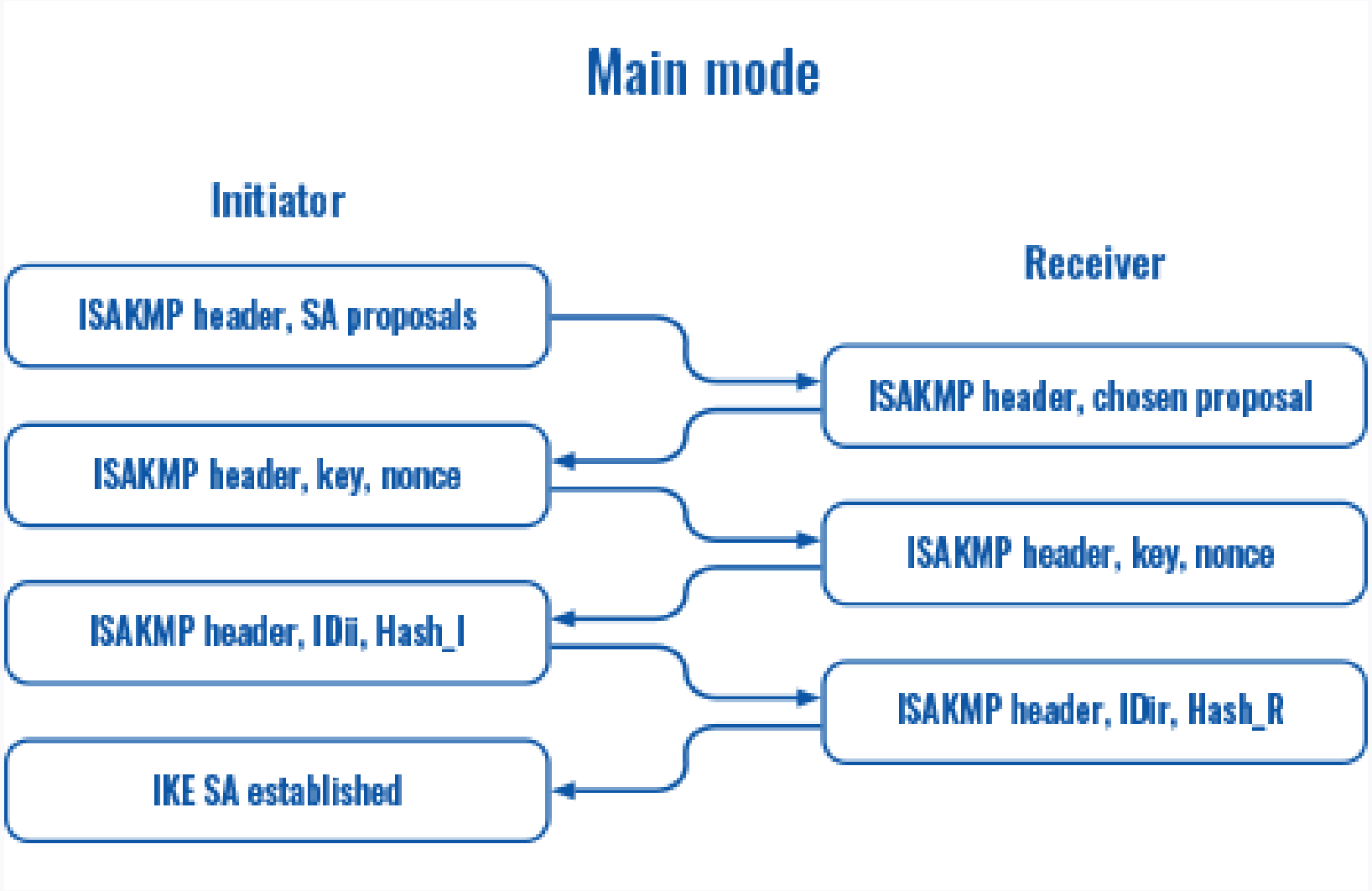
Phase1

Режимы работы 1 фазы:

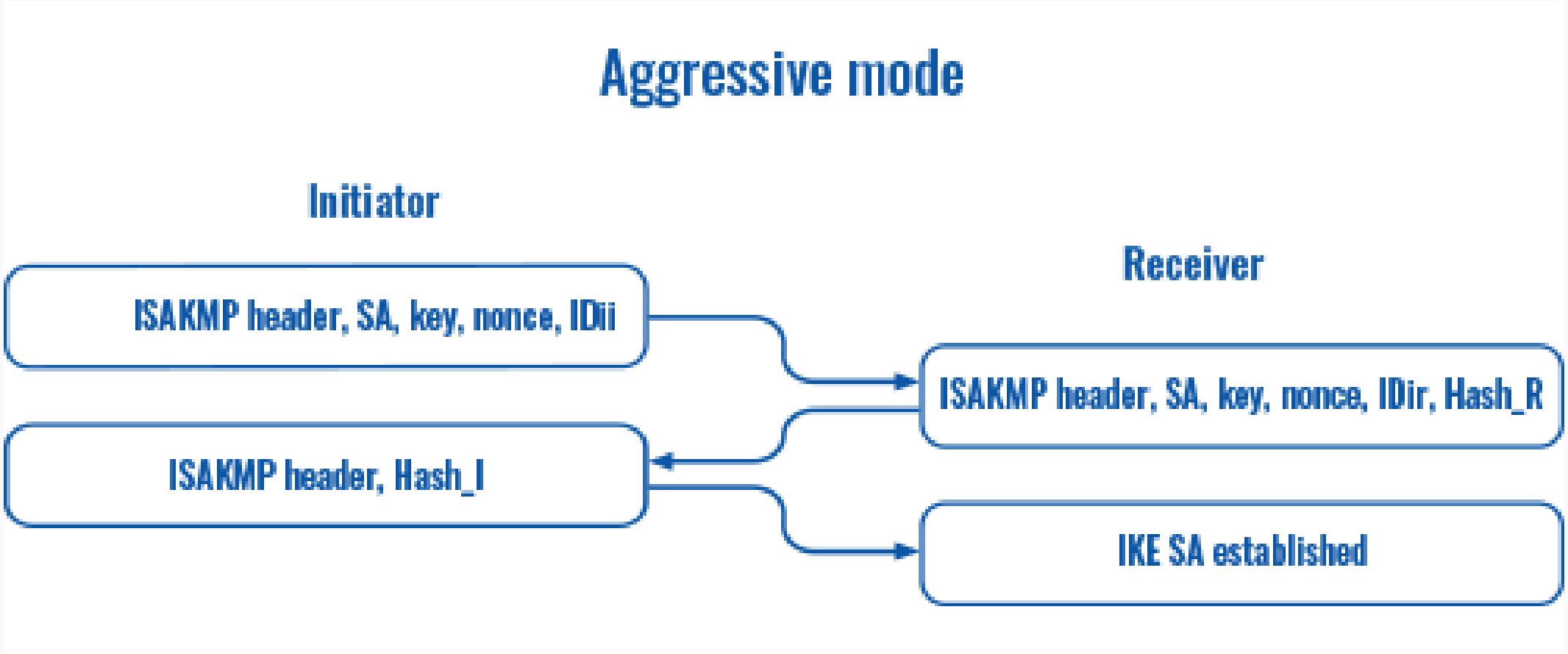
- main mode – основной режим при котором каждый параметр согласовывается отдельным сообщением. При этом часть сообщений передаются в открытом виде. Всего 6 сообщений

- aggressive mode – режим, при котором отправляется всего 3 сообщения для установки соединения. Все сообщения передаются в открытом виде

Phase1


Main mode
Initiator
Receiver
ISAKMP header, SA proposals
ISAKMP header, chosen proposal
ISAKMP header, key, nonce
ISAKMP header, key, nonce
ISAKMP header, IDii, Hash_I
ISAKMP header, IDir, Hash_R
IKE SA established

Phase1


Aggressive mode
Initiator
Receiver
ISAKMP header, SA, key, nonce, IDii
ISAKMP header, SA, key, nonce, IDir, Hash_R
ISAKMP header, Hash_I
IKE SA established

Phase1

Сравнение протоколов IKEv1 и IKEv2

Оба протокола работают по 500 порту UDP. Однако между собой не совместимы

Основные различия в IKEv2:

- Гибкое использование протоколов шифрования. Возможность использовать ГОСТовые протоколы
- Защита от DoS-атак. Используется что-то вроде cookie
- Поддержка аппаратным обеспечением
- Более сильное шифрование
- Защита от потери пакетов
- Возможно подключение дополнений для различных видов использования(Remote access, High Availability, etc)


3
Phase2

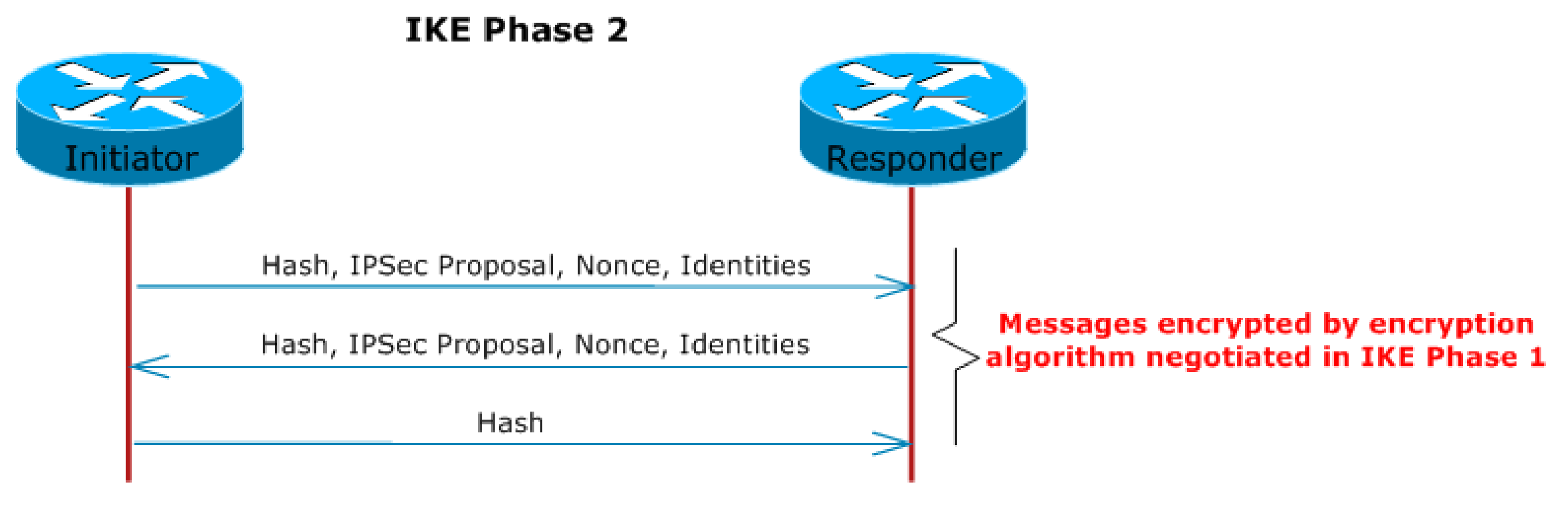
Phase2

2 фаза IPSec генерирует данные ключей и пиры договариваются об используемой политике

Эта фаза так же называется быстрым режимом - quick mode.

Начать согласование вторая фаза может только после полного завершения первой фазы.

Phase2


IKE Phase 2
Initiator
Responder
Hash, IPSec Proposal, Nonce, Identities
Hash, IPSec Proposal, Nonce, Identities
Hash
Messages encrypted by encryption algorithm negotiated in IKE Phase 1


3.1
Phase2. Protocols

Phase2. Protocols

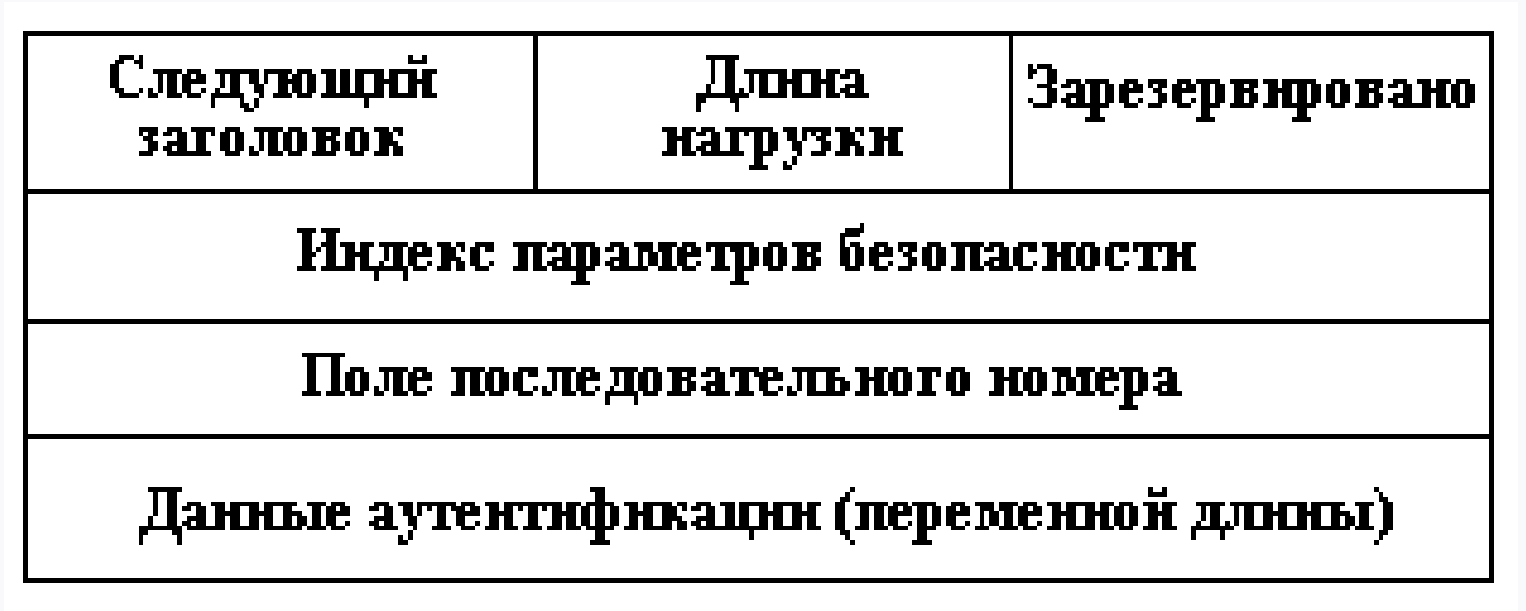
Authentication Header – AH обеспечивают идентификацию, проверку целостности и защиту от воспроизведения информации.

Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней.

Основным и единственным назначением AH является обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня.

Протоколы более высокого уровня должны быть модифицированы в целях осуществления проверки аутентичности полученных данных.

Phase2. Protocols



- Next Header указывает на следующий заголовок
- Payload Len представляет длину пакета
- SPI является указателем на контекст безопасности
- Sequence Number Field содержит последовательный номер пакета

Phase2. Protocols

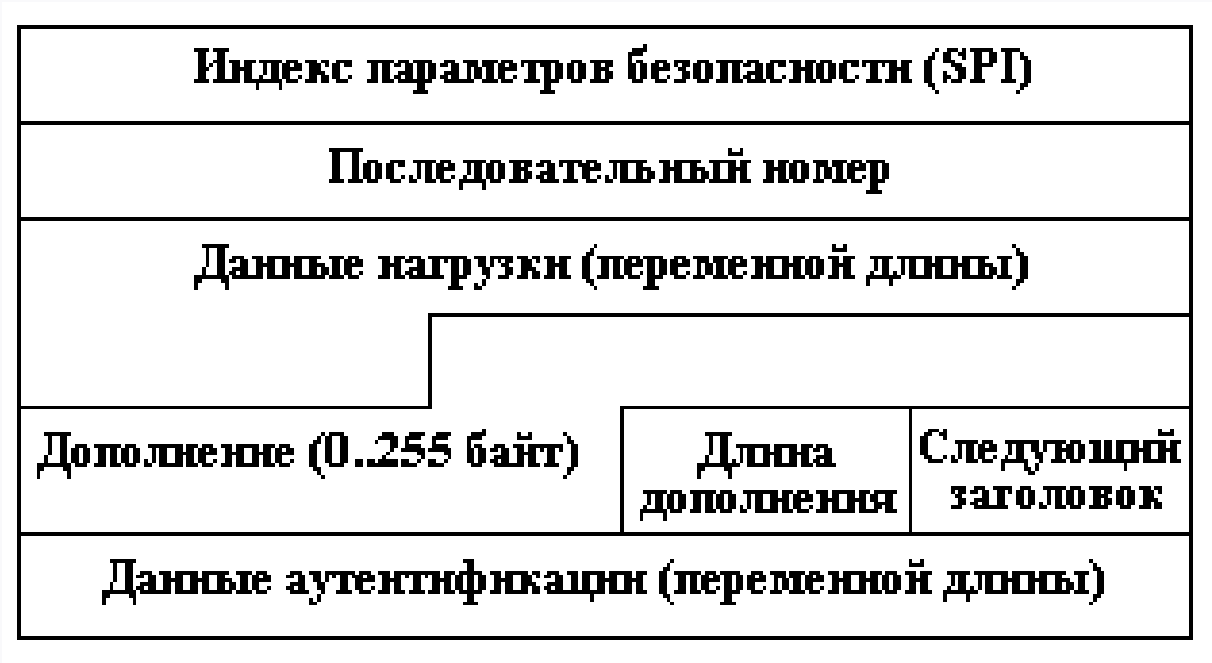
Encapsulating Security Payload (ESP) – обеспечивает конфиденциальность данных. Так же позволяет идентифицировать отправителя данных и обеспечить целостность данных, защиту от воспроизведения информации.

Отличие протокола ESP от протокола Authentication Header (AH) состоит в том, что ESP выполняет шифрование данных.

Возможна работа в двух режимах

- Туннель
- Транспорт

Phase2. Protocols



- SPI, указывающее на контекст безопасности
- Sequence Number Field, содержащее последовательный номер пакета
- "ESP Authentication Data" (контрольная сумма), не является обязательным в заголовке ESP.

Phase2. Protocols

Mode / Protocol	Transport	Tunnel
AH	IP | AH | Data	IP | AH | IP | Data
ESP	IP | ESP | Data | ESP-T	IP | ESP | IP | Data | ESP-T
AH-ESP	IP | AH | ESP | Data | ESP-T	IP | AH | ESP | IP | Data | ESP-T

Phase2. Protocols

Алгоритмы шифрования данных:

- DES (3DES)
- RC5
- RC4
- AES или AES-CBC

Алгоритмы идентификации

- HMAC-MD5
- HMAC-SHA
- HMAC-SHA-256
- AES-XCBC-MAC

4

GRE and IPSec

GRE and IPSec

Настройки 1 фазы

Задать политику isakmp:
crypto isakmp policy 10
(config)# authentication pre-share

Задать пароль для удаленного пира
(config)# crypto isakmp key <password> address 192.168.2.1

Создать access-list со списком адресов, которые будут работать через IPSec:
(config)# access-list 101 permit ip host 192.168.10.0 255.255.255.0 any

GRE and IPSec

Настройки 2 фазы

```
crypto map MAP 10 ipsec-isakmp
 set peer 192.168.2.1
 set transform-set SET
 match address 101
```

Установка алгоритма шифрования

```
crypto ipsec transform-set SET esp-des
```

Привязать к интерфейсу

```
 interface FastEthernet0/0
 crypto map MAP
```

GRE and IPSec

GRE внутри IPSec

IPSec внутри GRE

GRE and IPSec

Задать политику isakmp:

```
crypto isakmp policy 10
 authentication pre-share
 encr 3des
 hash md5
 group 2
 lifetime 86400
```

Задать пароль для удаленного пира

```
crypto isakmp key password address 192.168.3.3
```

Создать access-list со списком адресов, которые будут работать через IPSec:

```
access-list 101 permit gre host 192.168.3.3 host 192.168.2.1
```

GRE and IPSec

```
crypto map MAP 10 ipsec-isakmp
 set peer 192.168.2.1
 set transform-set SET
 match address 101
```

Установка алгоритма шифрования

```
crypto ipsec transform-set SET esp-des
 mode transport – переводим в режим транспорта(экономит 20 байт)
```

Привязать к интерфейсу

```
 interface FastEthernet0/0
 crypto map MAP
```

GRE and IPSec

Команды просмотра:

ISAKMP:

sh crypto isakmp sa

sh crypto isakmp sa detail

sh crypto isakmp peers

IPSec:

sh crypto ipsec sa

sh crypto ipsec sa detail

sh crypto ipsec profile


5
CA

CA

При работе с DMVPN IPsec с аутентификацией через сертификаты самое удобное и безопасное решение.

1. Настройка CA сервера
2. Выпуск сертификатов
3. Настройка 1 и 2 фазы
4. Привязка к интерфейсу

CA

Настройка центра сертификации.
Задать имя домена:
ip domain-name otus.ru

Включить http-сервер:
ip http server

Создать пару корневых ключей:
crypto key generate rsa general-keys label CA exportable modulus 2048

Включаем CA-сервер:
crypto pki server CA
 no shut

CA

Настройка клиентов CA-сервера
Создать пару ключей:
crypto key generate rsa label VPN modulus 2048

Настроить trustpoint:
crypto pki trustpoint VPN
 enrollment url http://10.0.0.1
 subject-name CN=R4,OU=VPN,O=Otus,C=RU
 rsakeypair VPN
 revocation-check none

CA

Запросить сертификат CA
(config)#crypto pki authenticate VPN

Запросить сертификат для маршрутизатора
(config)#crypto pki enroll VPN

Выдать сертификат на маршрутизаторе CA:
crypto pki server CA grant

CA

Выдать сертификат маршрутизатору, который работает как CA-сервер:

Сгенерировать еще один trustpoint
```
crypto pki trustpoint I_CA
 enrollment url http://10.0.1.1
 subject-name CN=R1,OU=VPN,O=OTUS,C=RU
 revocation-check none
 rsakeypair I_CA
```

И аналогично запросить оба сертификата:
```
crypto pki authenticate I_CA
crypto pki enroll I_CA
```

CA

Настройка IPSec через сертификаты:

```
crypto isakmp policy 10
 authentication rsa-sig
```

Настроить политику защиты данных

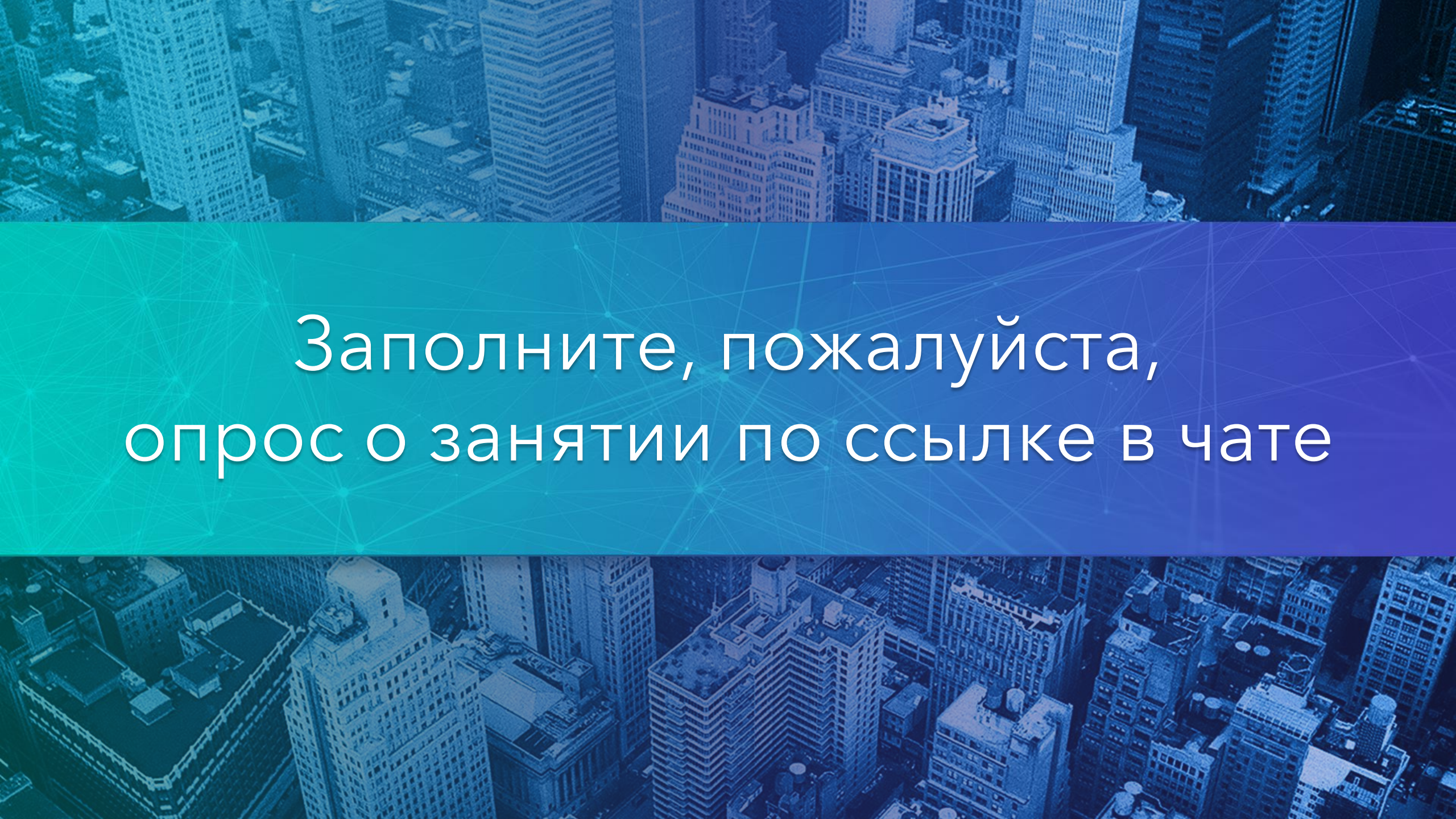
```
crypto ipsec transform-set SET esp-aes esp-sha-hmac

crypto ipsec profile VTI_prof
 set transform-set SET
```

Привязать к виртуальному интерфейсу

```
 interface Tunnel0
 tunnel protection ipsec profile VTI_prof
```

CA

ISAKMP: sh crypto isakmp sa sh crypto isakmp sa detail sh crypto isakmp peers IPSec: sh crypto ipsec sa sh crypto ipsec sa detail sh crypto ipsec profile sh crypto session { brief | detaill}	Проверить работу CA-сервера sh crypto pki server Посмотреть сертификаты на маршрутизаторе sh crypto pki certificates Посмотреть запросы на сертификат sh crypto pki server CA requests


Заполните, пожалуйста,
опрос о занятии по ссылке в чате

До новых встреч!
Приходите на следующие занятия

Кулиничев Алексей
Администратор Сетей
Santchous42@yandex.ru