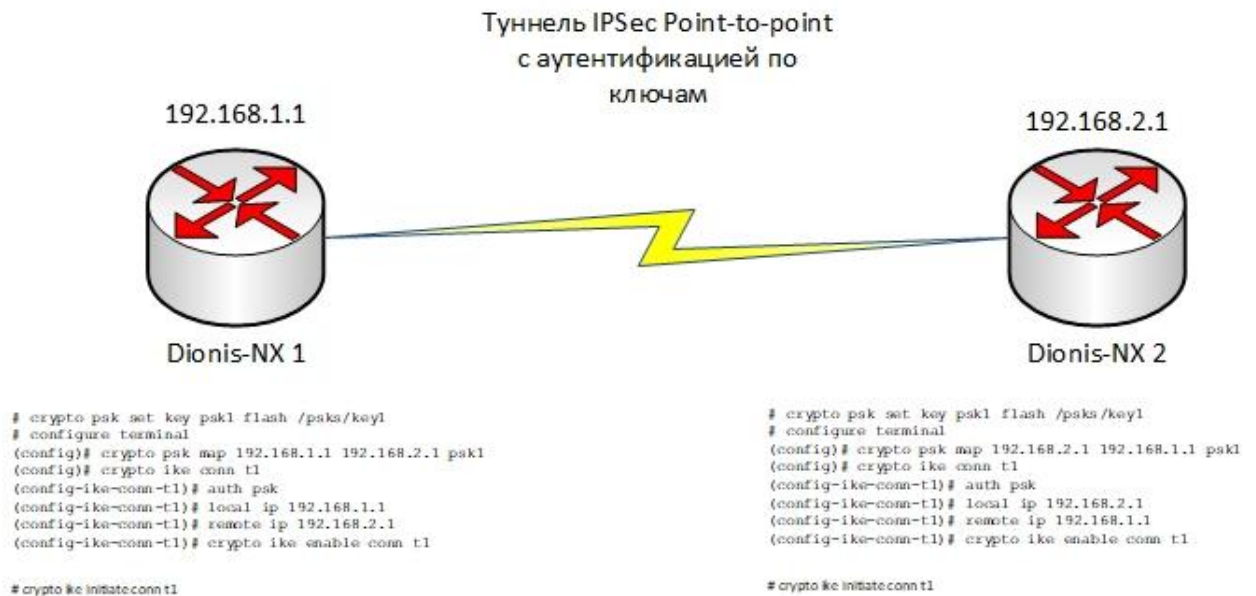


Настройка криптографического туннеля по протоколу IPSec Point-to-point (аутентификация по pre-shared ключам)

Рассмотрим самый простой пример настройки соединения типа «точка-точка» со взаимной аутентификацией по ключам.

Допустим у нас есть два узла Dionis-NX с IP-адресами 192.168.1.1 и 192.168.2.1.



Настройка узла 1:

Загружаем pre-shared ключ с внешнего носителя (допустим, из файла /psks/key1):

```
# crypto psk set key psk1 flash /psks/key1
```

Ассоциируем загруженный ключ с концами туннеля:

```
# configure terminal
(config)# crypto psk map 192.168.1.1 192.168.2.1 psk1
```

Создаём соединение, указываем метод аутентификации по PSK и IP-адреса концов туннеля:

```
(config)# crypto ike conn t1
(config-ike-conn-t1)# auth psk
(config-ike-conn-t1)# local ip 192.168.1.1
(config-ike-conn-t1)# remote ip 192.168.2.1
```

Включаем туннель и службу IKE:

```
(config-ike-conn-t1)# crypto ike enable
```

```
(config)# crypto ike enable conn t1
```

Выполняем симметричные настройки узла 2:

```
# crypto psk set key psk1 flash /psks/key1
# configure terminal
(config)# crypto psk map 192.168.2.1 192.168.1.1 psk1
(config)# crypto ike conn t1
(config-ike-conn-t1)# auth psk
(config-ike-conn-t1)# local ip 192.168.2.1
(config-ike-conn-t1)# remote ip 192.168.1.1
(config-ike-conn-t1)# crypto ike enable
(config)# crypto ike enable conn t1
```

Иницилируем соединение с любого из узлов:

```
(config)# do crypto ike initiate conn t1
```