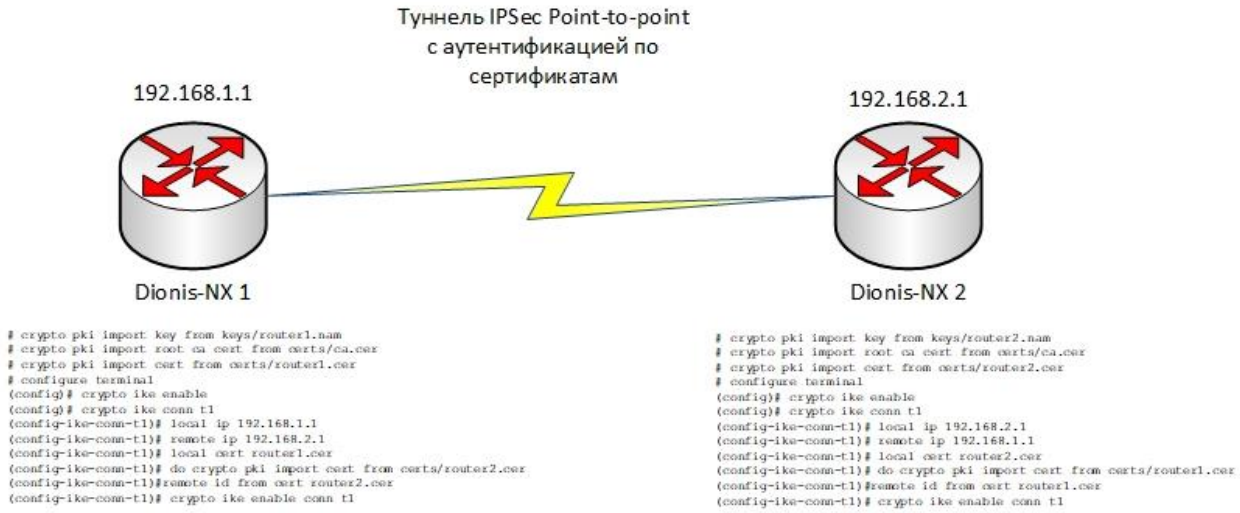
Настройка IPSec Point-to-point (аутентификация по сертификатам X.509)

Рассмотрим самый простой пример настройки соединения типа «точка-точка» со взаимной аутентификацией по сертификатам X.509. Допустим у нас есть два узла Dionis-NX с IP-адресами 192.168.1.1 и 192.168.2.1.



Настройка узла 1:
Импортируем сертификат узла, сертификат удостоверяющего центра и закрытый ключ узла с внешнего носителя:

```
# crypto pki import key from keys/router1.nam
# crypto pki import root ca cert from certs/ca.cer
# crypto pki import cert from certs/router1.cer
```

Входим в режим конфигурации и запускаем службу IKE:

```
# configure terminal
(config)# crypto ike enable
```

Создаём настройку соединения. Назовём его «t1»:

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

Вид строки приглашения говорит о том, система находится в режиме редактирования настроек соединения «t1».

По умолчанию действует режим аутентификации по сертификатам X.509, что эквивалентно опции:

```
(config-ike-conn-t1)# auth pubkey
```

Задаём IP-адреса концов туннеля - локального и удалённого:

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

Задаём имя используемого сертификата:

```
(config-ike-conn-t1)# local cert router1.cer
```

Задаём X500-имя сертификата нашего оппонента:

```
(config-ike-conn-t1)# remote id "CN=Узел 2, O=Хорошая организация, C=RU"
```

Можно импортировать X500-имя непосредственно из сертификата оппонента. Для этого необходимо предварительно загрузить сертификат оппонента в систему:

```
(config-ike-conn-t1)# do crypto pki import cert from certs/router2.cer
(config-ike-conn-t1)# remote id from cert router2.cer
```

Новые созданные соединения изначально находятся в выключенном состоянии. Чтобы наше соединение смогло стать активным, его необходимо включить:

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

Теперь соединение включено и находится в «слушающем» состоянии, то есть оно готово начать установление туннеля IPsec. Установление туннеля может быть инициировано данным узлом, либо может быть инициировано нашим оппонентом.

Теперь выполним настройку узла 2, которая, по сути, будет симметричной настройке узла 1:

```
# crypto pki import key from keys/router2.nam
# crypto pki import root ca cert from certs/ca.cer
# crypto pki import cert from certs/router2.cer
# configure terminal
(config)# crypto ike enable
(config)# crypto ike conn t1
(config-ike-conn-t1)# local ip 192.168.2.1
(config-ike-conn-t1)# remote ip 192.168.1.1
(config-ike-conn-t1)# local cert router2.cer
(config-ike-conn-t1)# remote id "CN=Узел 1, O=Хорошая организация, C=RU"
(config-ike-conn-t1)# crypto ike enable conn t1
```

Теперь весь трафик (типа «точка-точка») между узлами 1 и 2 будет инкапсулироваться в протокол ESP. Важно помнить, что если к узлу 1, например, подключены другие сети, то проходящий трафик через узел 1 к узлу 2 из этих сетей НЕ будет попадать в туннель и (если не настроены фильтры) будет идти в открытом виде. Ибо данный трафик будет являться трафиком типа «подсеть-точка» и не будет попадать в туннель типа «точка-точка».