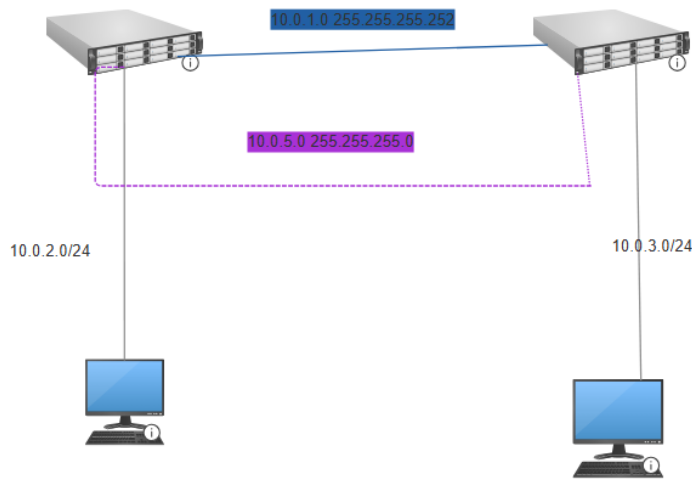


# Route based vpn Router-Router



Here we assume that OSPF is already configured. Router on the left is R1 and on the right is R2

## Step 1: ISAKMP policy

R1:

```
crypto isakmp policy 10
```

```
    encr aes
```

```
    authentication pre-share
```

```
    group 2
```

```
    lifetime 3600
```

```
    hash sha
```

R2:

```
crypto isakmp policy 10
```

```
    encr aes
```

```
    authentication pre-share
```

```
    group 2
```

```
    lifetime 3600
```

```
    hash sha
```

## Step 2 Key

R1:

```
crypto isakmp key cisco address [address of R2 physical interface connected to R1]  
10.0.1.2
```

R2:

```
crypto isakmp key cisco address [address of R2 physical interface connected to R2]  
10.0.1.1
```

## Step 3. Transform set + ipsec profile

R1 and R2:

```
crypto ipsec transform-set R1R2 esp-aes esp-sha-hmac  
mode tunnel  
crypto ipsec profile VTI  
set transform-set R1R2
```

## Step 4. Creating VTI interface

R1:

```
interface Tunnel0  
ip address 10.0.5.1 255.255.255.0  
tunnel source [ip address of physical interface of R2 connected to R1] 10.0.1.2  
tunnel mode ipsec ipv4  
tunnel destination [ip address of physical interface of R1->R2] 10.0.1.1  
tunnel protection ipsec profile VTI
```

R2:

```
interface Tunnel0  
ip address 10.0.5.2 255.255.255.0  
tunnel source [ip address of physical interface of R1->R2] 10.0.1.1
```

tunnel mode ipsec ipv4

tunnel destination [ip address of physical interface of R2->R1] 10.0.1.2

tunnel protection ipsec profile VTI

## Final step: adding route to go through tunnel

This is needed to make sure that traffic from PC-A to PC-B goes through tunnel

Command: ip route [ip address of remote network + netmask + interface of local tunnel

R1:

ip route 10.0.3.0 255.255.255.0 Tunnel0

R2:

ip route 10.0.2.0 255.255.255.0 Tunnel0

## Verification

Ping from PC to PC and enter “show crypto ipsec sa” command to see if the number of packets encrypted/decrypted is increasing with each ping