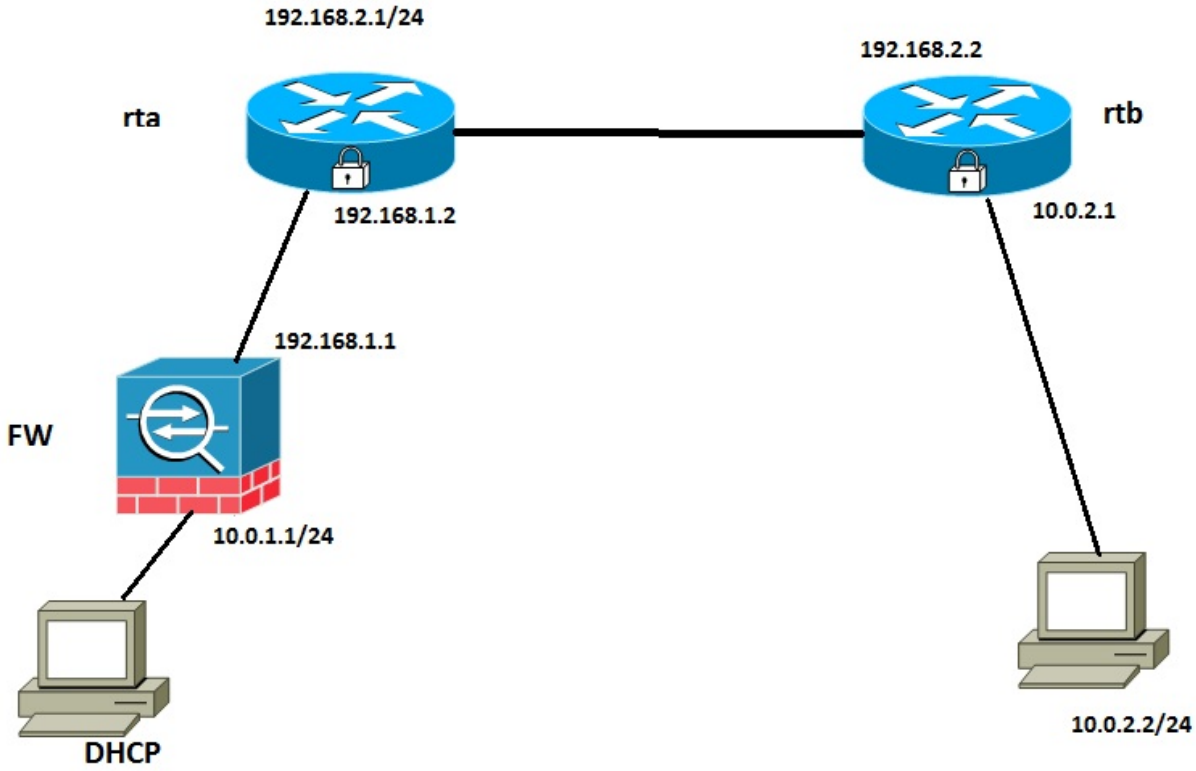
Case study: Configuring a Site-to-Site IPsec VPN Using CLI

Use as a reference these labs: Configuring a Site-to-Site VPN Using Cisco IOS, Configuring ASA Basic Settings and Firewall Using CLI

Objectives: Configure Site-to-Site IPsec between VPN Endpoint ASA(FW) and Router (rtb)



PC1 **PC2**

1. **Configure Routers Settings: IP addresses, static routing and static IP on PC2**
2. **Configure ASA Basic Settings and Firewall:**

   Configure ip adresses, the inside and outside VLAN interfaces.

   Configure port address translation (PAT) for the inside network.

   Configure a DHCP server for the inside network.

   Configure a static default route for the ASA.

3. **Configure a Site-to-Site IPSec VPN between ASA and rtb**

   Configure basic IPSec VPN connection settings on router and ASA (transform-set, encryption, hash, isakmp policy, crypto map, crypto ACL) , specify the pre-shared VPN key **cisco**
   Encrypt traffic between the **rtb** LAN and the LAN behind ASA
   Configure static address translation for VPN support on ASA
   Test the Site-to-Site IPsec VPN

FW VPN configuration:

crypto isakmp enable outside

crypto isakmp policy 10

authentication pre-share

encryption 3des

hash sha

group 2

lifetime 86400

!

tunnel-group 192.168.2.2 type ipsec-l2l

tunnel-group 192.168.2.2 ipsec-attributes

pre-shared-key cisco

!

access-list L2LACL extended permit ip 10.0.1.0 255.255.255.0 10.0.2.0 255.255.255.0

!

crypto ipsec transform-set 3DES_SHA esp-3des esp-sha-hmac

!

crypto map TEST_MAP 10 match address L2LACL

crypto map TEST_MAP 10 set peer 192.168.2.2

crypto map TEST_MAP 10 set transform-set 3DES_SHA

crypto map TEST_MAP 10 set reverse-route

!

crypto map TEST_MAP interface outside

object network NETWORK_OBJ_10.0.2.0_24

subnet 10.0.2.0 255.255.255.0

object network NETWORK_OBJ_10.0.1.0_24

subnet 10.0.1.0 255.255.255.0

nat (inside,outside) source static NETWORK_OBJ_10.0.1.0_24 NETWORK_OBJ_10.0.1.0_24 destination static NETWORK_OBJ_10.0.2.0_24 NETWORK_OBJ_10.0.2.0_24