NST41092 Practical for Secure Network Infrastructure

Continuous Assessment 2:

Submission date 30/11/2022

Submission guideline: Mark your registration numbers clearly in your assessment files and forward it to razmik@gmail.com with the subject “NST41092 assessment2 - ” on or before the deadline.

PC1: 192.168.5.10

Gateway 192.168.5.1

PC2: 192.168.5.20

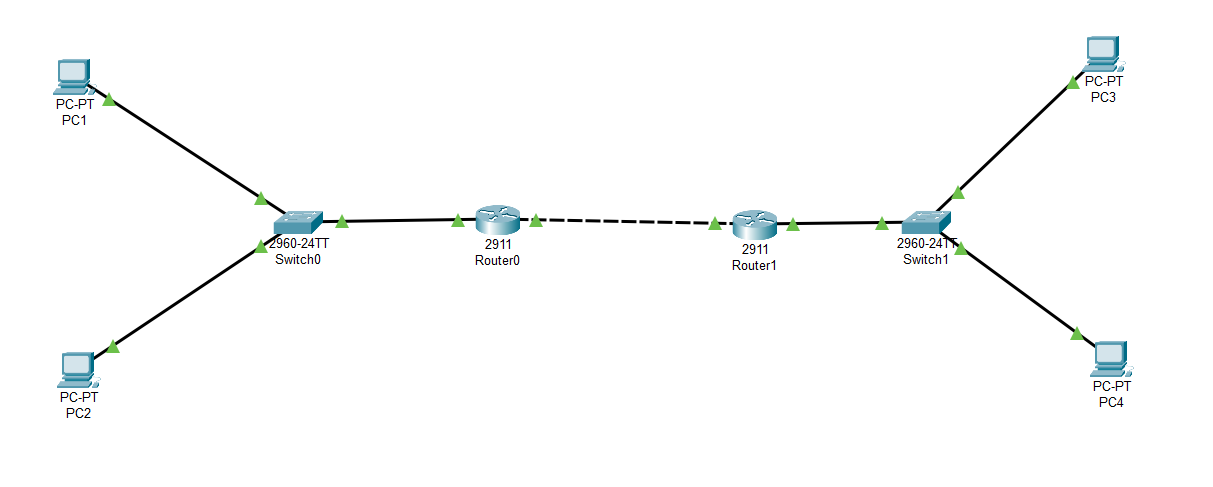
Gateway 192.168.5.1

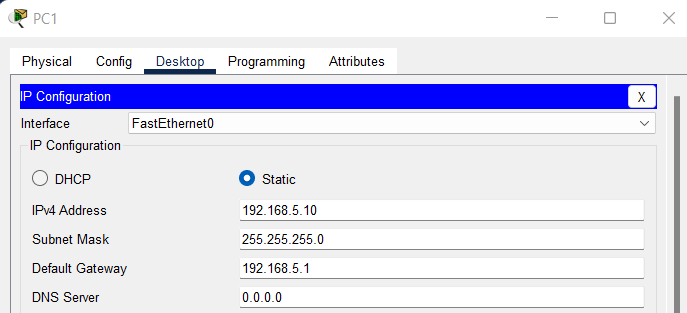
PC3: 192.168.6.10

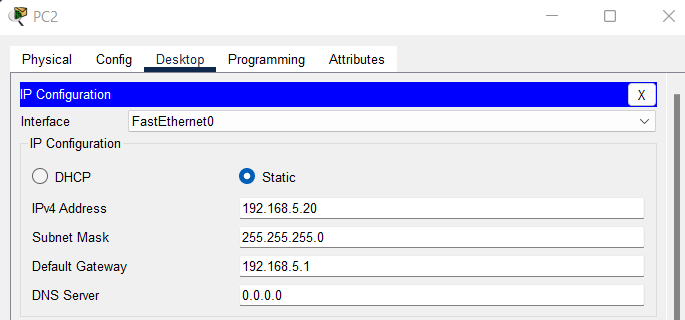
Gateway 192.168.6.1

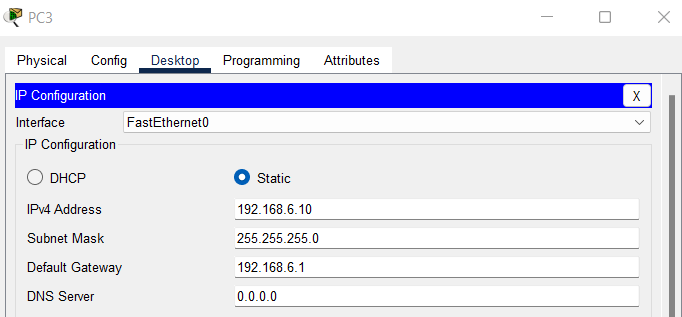
PC4: 192.168.6.20

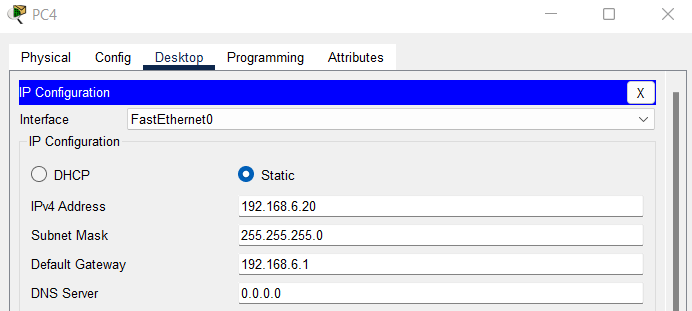
Gateway 192.168.6.1











In ROUTER 0

Steps to Configure the Default Routing

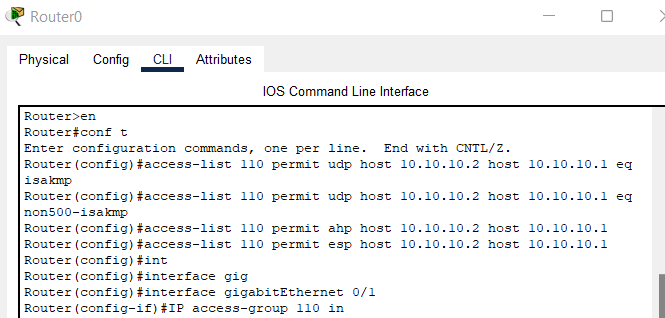
ip route 0.0.0.0 0.0.0.0 10.0.0.2

Check for security module

license boot module c2900 technology-package securityk9

Save the configuration and reload the router

1. Permit protocols required for IPSec VPN



2. Define the interesting traffic to pass through the tunnel. You may assume all IP traffic between

both site as interesting traffic.



3. Create ISAKMP (IKE) policy to establish the phase 1 tunnel with the below parameter

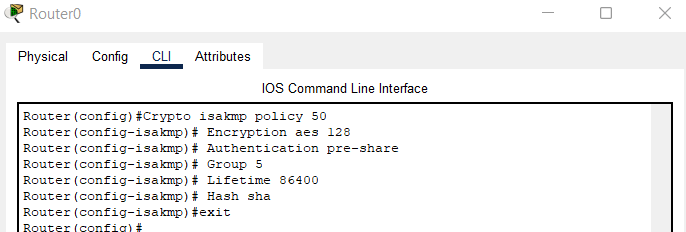
Encryption: AES 128

Authentication pre-shared

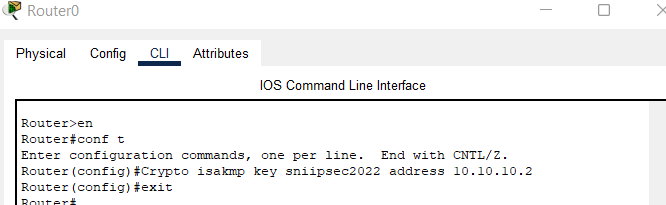
Diffie Hellman group 5

Hash SHA

Lifetime 24 hours



Configure the pre-shared key



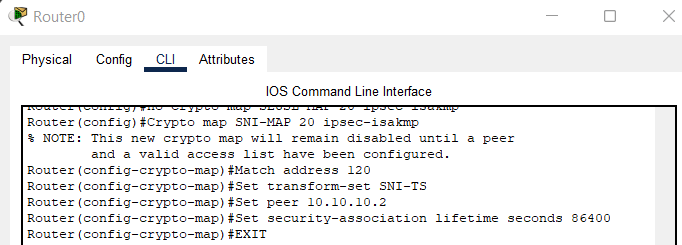
4. Configure IPSec transform set (parameters IPSec users to protect data)

AH – none

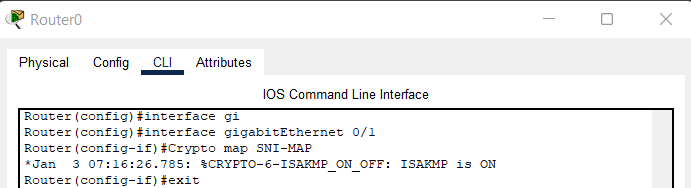
ESP – esp-aes, esp-sha-hmac



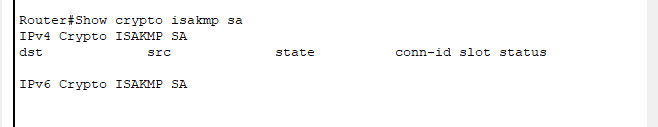
5. Create cypto map



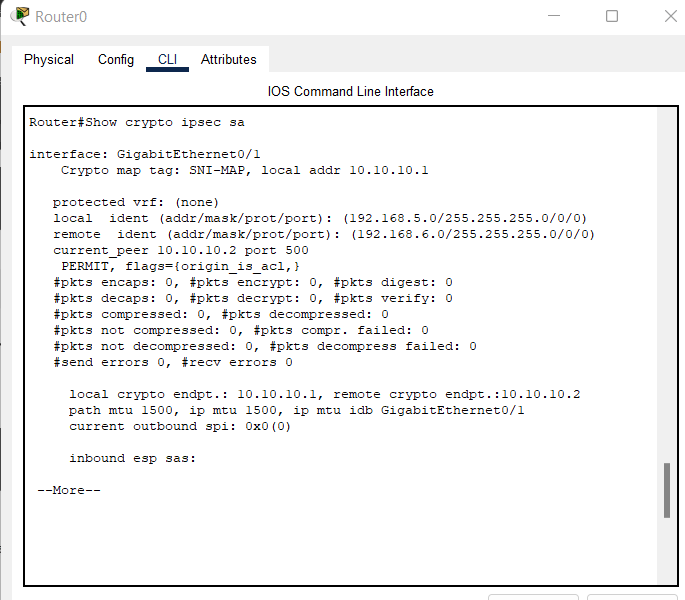
6. Apply crypto map to interface



Attach the output of Show crypto isakmp sa and



Show crypto ipsec sa commands



Attach the show run command and the packet tracer file

Router#show run

Building configuration...

Current configuration : 1516 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Router

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

!

license udi pid CISCO2911/K9 sn FTX152471K4-

license boot module c2900 technology-package securityk9

!

!

!

crypto isakmp policy 50

encr aes 128

authentication pre-share

group 5

!

crypto isakmp key sniipsec2022 address 10.10.10.2

!

!

!

crypto ipsec transform-set SNI-TS esp-aes esp-sha-hmac

!

crypto map SNI-MAP 20 ipsec-isakmp

set peer 10.10.10.2

set security-association lifetime seconds 86400

set transform-set SNI-TS

match address 120

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface GigabitEthernet0/0

ip address 192.168.5.1 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 10.10.10.1 255.0.0.0

ip access-group 110 in

duplex auto

speed auto

crypto map SNI-MAP

!

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

ip route 0.0.0.0 0.0.0.0 10.10.10.2

!

ip flow-export version 9

!

!

access-list 110 permit udp host 10.10.10.2 host 10.10.10.1 eq isakmp

access-list 110 permit udp host 10.10.10.2 host 10.10.10.1 eq non500-isakmp

access-list 110 permit ahp host 10.10.10.2 host 10.10.10.1

access-list 110 permit esp host 10.10.10.2 host 10.10.10.1

access-list 120 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

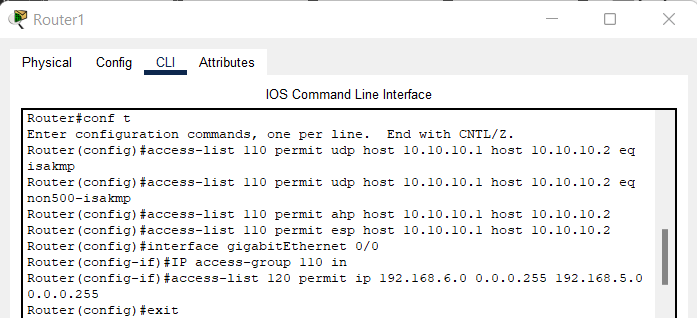
!

!

end

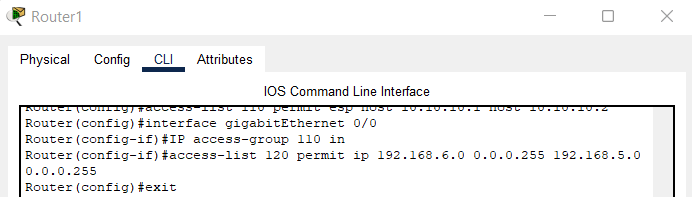
for Router 1

1. Permit protocols required for IPSec VPN



2. Define the interesting traffic to pass through the tunnel. You may assume all IP traffic between

both site as interesting traffic.



3. Create ISAKMP (IKE) policy to establish the phase 1 tunnel with the below parameter

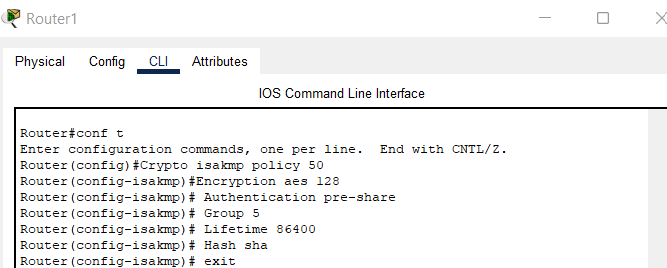
Encryption: AES 128

Authentication pre-shared

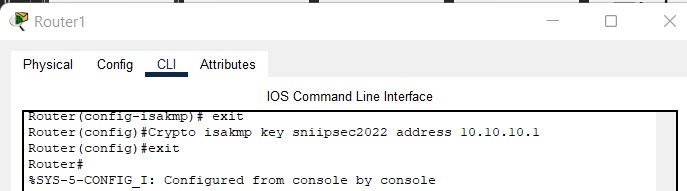
Diffie Hellman group 5

Hash SHA

Lifetime 24 hours



Configure the pre-shared key



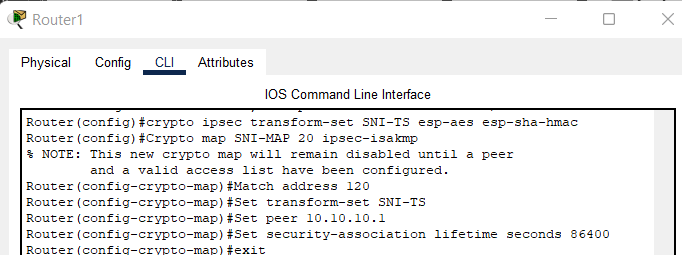
4. Configure IPSec transform set (parameters IPSec users to protect data)

AH – none

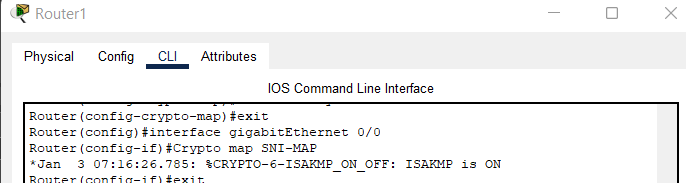
ESP – esp-aes, esp-sha-hmac



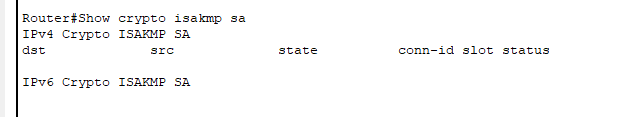
5. Create cypto map



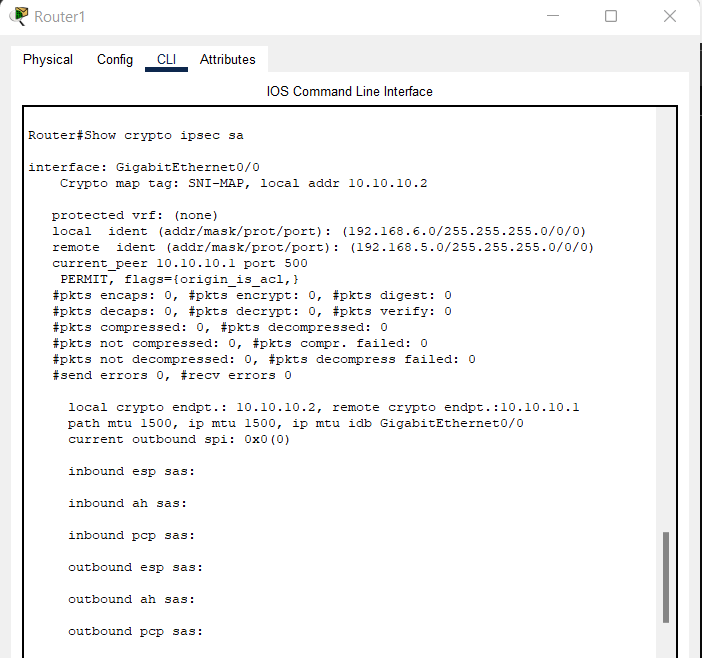
6. Apply crypto map to interface



Attach the output of Show crypto isakmp sa and



Show crypto ipsec sa commands



Attach the show run command and the packet tracer file

Router#show run

Building configuration...

Current configuration : 1551 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Router

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

!

license udi pid CISCO2911/K9 sn FTX152485WX-

license boot module c2900 technology-package securityk9

!

!

!

crypto isakmp policy 50

encr aes 128

authentication pre-share

group 5

!

crypto isakmp key sniipsec2022 address 10.10.10.1

!

!

!

crypto ipsec transform-set SNI-TS esp-aes esp-sha-hmac

!

crypto map SNI-MAP 20 ipsec-isakmp

set peer 10.10.10.1

set security-association lifetime seconds 86400

set transform-set SNI-TS

match address 120

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface GigabitEthernet0/0

ip address 10.10.10.2 255.0.0.0

ip access-group 110 in

duplex auto

speed auto

crypto map SNI-MAP

!

interface GigabitEthernet0/1

ip address 192.168.6.1 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

ip route 0.0.0.0 0.0.0.0 10.10.10.1

ip route 0.0.0.0 0.0.0.0 10.0.0.1

!

ip flow-export version 9

!

!

access-list 110 permit udp host 10.10.10.1 host 10.10.10.2 eq isakmp

access-list 110 permit udp host 10.10.10.1 host 10.10.10.2 eq non500-isakmp

access-list 110 permit ahp host 10.10.10.1 host 10.10.10.2

access-list 110 permit esp host 10.10.10.1 host 10.10.10.2

access-list 120 permit ip 192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end

