NST41092 Practical for Secure Network Infrastructure

Continuous Assessment 2:

Submission date 30/11/2022

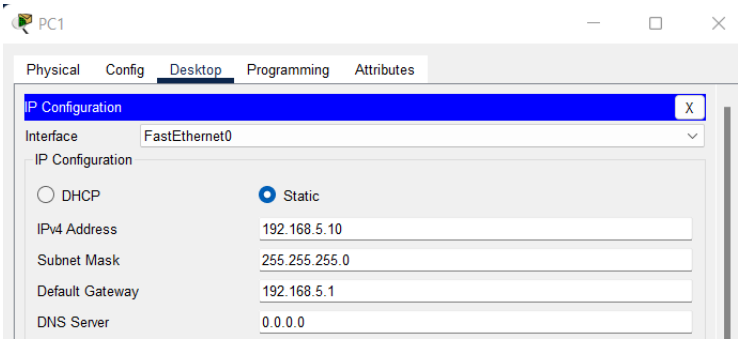
Submission guideline: Mark your registration numbers clearly in your assessment files and forward it to razmik@gmail.com with the subject “NST41092 assessment2 - ” on or before the deadline.

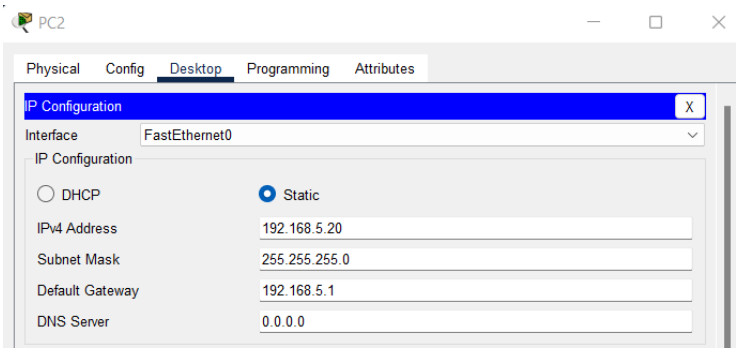
PC1: 192.168.5.10
Gateway 192.168.5.1

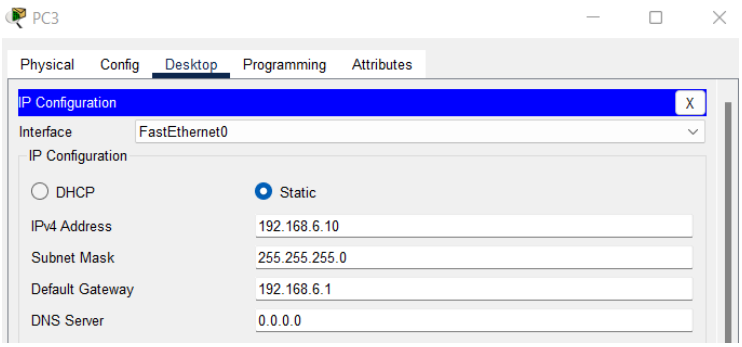
PC2: 192.168.5.20
Gateway 192.168.5.1

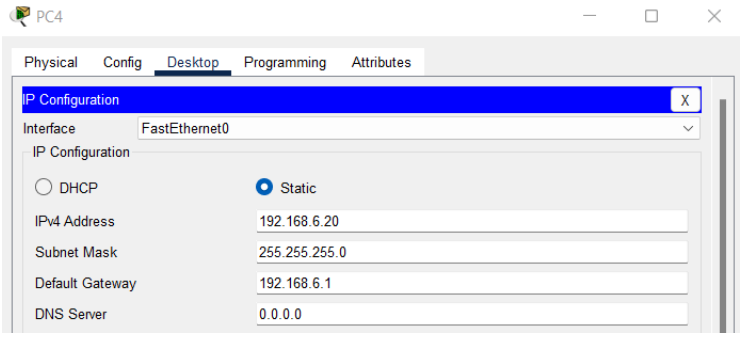
PC3: 192.168.6.10
Gateway 192.168.6.1

PC4: 192.168.6.20
Gateway 192.168.6.1









<u>In ROUTER 0</u>

Steps to Configure the Default Routing

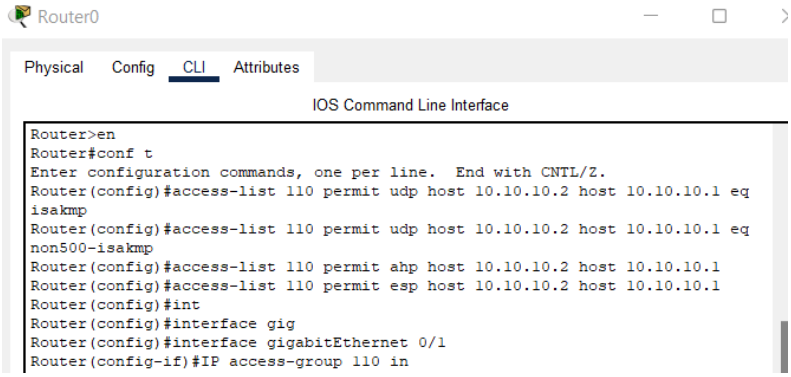
ip route 0.0.0.0 0.0.0.0 10.0.0.2

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.

```
Router(config-if)#access-list 120 permit ip 192.168.5.0 0.0.0.255 192.168.6.0
0.0.0.255
```

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

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#Crypto isakmp policy 50
Router(config-isakmp)# Encryption aes 128
Router(config-isakmp)# Authentication pre-share
Router(config-isakmp)# Group 5
Router(config-isakmp)# Lifetime 86400
Router(config-isakmp)# Hash sha
Router(config-isakmp)#exit
Router(config)#
```

Configure the pre-shared key

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#Crypto isakmp key sniipsec2022 address 10.10.10.2
Router(config)#exit
Router#
```

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

AH – none

ESP – esp-aes, esp-sha-hmac

```
Router(config)#crypto ipsec transform-set SNI-TS esp-aes esp-sha-hmac
```

5. Create cypto map

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#Crypto map SNI-MAP 20 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#Match address 120
Router(config-crypto-map)#Set transform-set SNI-TS
Router(config-crypto-map)#Set peer 10.10.10.2
Router(config-crypto-map)#Set security-association lifetime seconds 86400
Router(config-crypto-map)#EXIT
```

6. Apply crypto map to interface

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#interface gi
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#Crypto map SNI-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
```

Attach the output of Show crypto isakmp sa and

```
Router#Show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

Show crypto ipsec sa commands

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#Show crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: SNI-MAP, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.5.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.6.0/255.255.255.0/0/0)
   current_peer 10.10.10.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.10.10.1, remote crypto endpt.:10.10.10.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:

 --More--
```

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 GigabitEtherneto/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 GigabitEtherneto/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
```

<u>for Router 1</u>

1. Permit protocols required for IPSec VPN

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 permit udp host 10.10.10.1 host 10.10.10.2 eq
isakmp
Router(config)#access-list 110 permit udp host 10.10.10.1 host 10.10.10.2 eq
non500-isakmp
Router(config)#access-list 110 permit ahp host 10.10.10.1 host 10.10.10.2
Router(config)#access-list 110 permit esp host 10.10.10.1 host 10.10.10.2
```

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

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#IP access-group 110 in
Router(config-if)#access-list 120 permit ip 192.168.6.0 0.0.0.255 192.168.5.0
0.0.0.255
Router(config)#exit
```

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

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#Crypto isakmp policy 50
Router(config-isakmp)#Encryption aes 128
Router(config-isakmp)# Authentication pre-share
Router(config-isakmp)# Group 5
Router(config-isakmp)# Lifetime 86400
Router(config-isakmp)# Hash sha
Router(config-isakmp)# exit
```

Configure the pre-shared key

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config-isakmp)# exit
Router(config)#Crypto isakmp key sniipsec2022 address 10.10.10.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

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

AH – none

ESP – esp-aes, esp-sha-hmac

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto ipsec transform-set SNI-TS esp-aes esp-sha-hmac
```

5. Create cypto map

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#crypto ipsec transform-set SNI-TS esp-aes esp-sha-hmac
Router(config)#Crypto map SNI-MAP 20 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#Match address 120
Router(config-crypto-map)#Set transform-set SNI-TS
Router(config-crypto-map)#Set peer 10.10.10.1
Router(config-crypto-map)#Set security-association lifetime seconds 86400
Router(config-crypto-map)#exit
```

6. Apply crypto map to interface

Router1

Physical Config CLI Attributes

IOS Command Line Interface

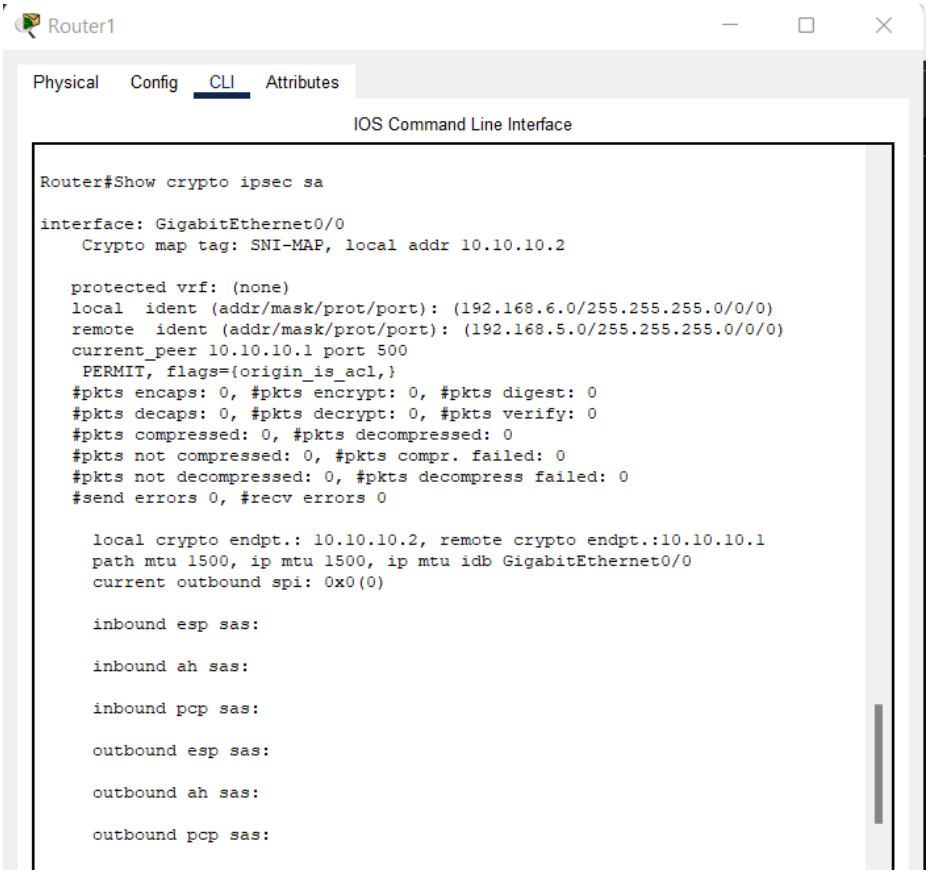
```
Router(config-crypto-map)#exit
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#Crypto map SNI-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
```

Attach the output of Show crypto isakmp sa and

```
Router#Show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

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
```