Packet Tracer lab 17

Site to site IPSEC VPN with ASA 5505

Lab instructions

This lab will show you how to configure site-to-site IPSEC VPN using the Packet Tracer 7.2.1 ASA 5505 firewall.

By default, the Cisco ASA 5505 firewall denies the traffic entering the outside interface if no explicit ACL has been defined to allow the traffic.

This default behaviour helps protecting the enterprise network from the internet during the VPN configuration.

Packet Tracer 7.2.1 also features the newest Cisco ASA 5506-X firewall.

In this lab, a small branch office will be securely connected to the enterprise campus over the internet using a broadband DSL connection to demonstrate ASA 5505 site-to-site VPN capabilities. No dynamic routing protocol will be configured between the two sites.

Campus addressing scheme :

- Campus IP addresses : 172.16.0.0/17
- DC : 172.16.0.0/18
- Users : 172.16.64.0/20
- DMZ : 172.16.96.0/21
- Network devices : 172.16.252.0/23
- L3 P2p links : 172.16.254.0/24

Branch office 1 IP subnet :172.16.129.0/24

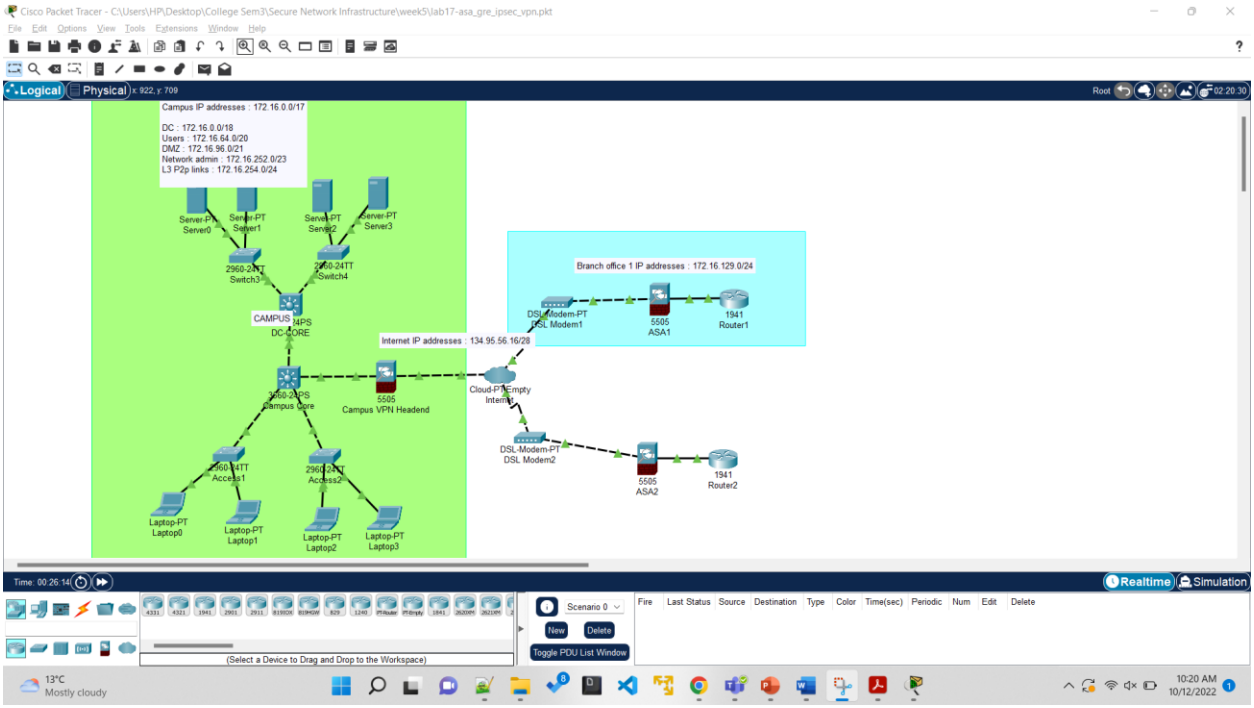
Enterprise internet IP addresses: 134.95.56.16/28

IPSEC VPN configuration to apply:

- ESP Encryption : AES-256
- AH hash algorithm : SHA
- Pre shared key : SHAREDSECRET

Network diagram

- In this Lab, I have done setup of the VPN tunnel in Campus ASA and then in the Branch ASA1. Setup commands I have mentioned below with screenshots.
- After the setup I did ping from Campus laptop to Branch router and showed the IPsec protocol in the Simulation mode.
- Then I showed the results for the crypto **isakmp** and crypto **ipsec** with screenshots.



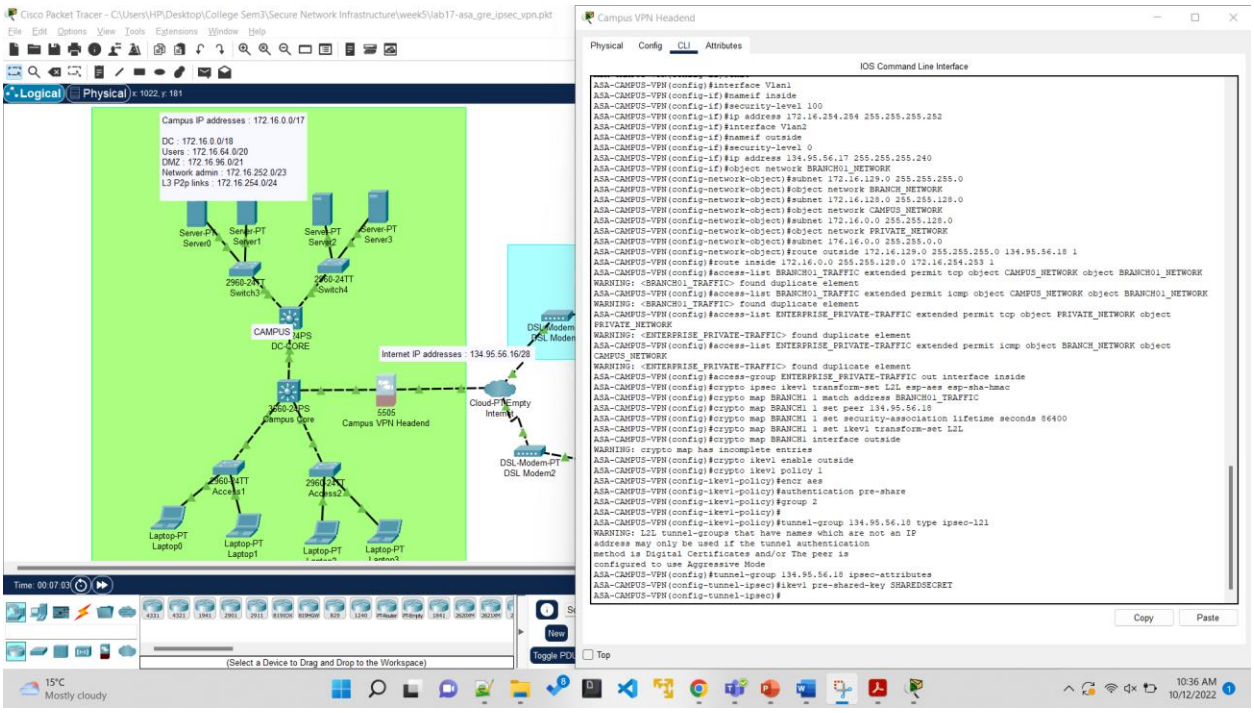
Step 1

Campus network - ASA 5505 IPSEC VPN headend device configuration

Below commands executed for the setup in Campus ASA.

```
ASA-CAMPUS-VPN(config)#interface Vlan1
ASA-CAMPUS-VPN(config-if)#nameif inside
ASA-CAMPUS-VPN(config-if)#security-level 100
ASA-CAMPUS-VPN(config-if)#ip address 172.16.254.254 255.255.255.252
ASA-CAMPUS-VPN(config-if)#interface Vlan2
ASA-CAMPUS-VPN(config-if)#nameif outside
ASA-CAMPUS-VPN(config-if)#security-level 0
ASA-CAMPUS-VPN(config-if)#ip address 134.95.56.17 255.255.255.240
ASA-CAMPUS-VPN(config-if)#object network BRANCH01_NETWORK
ASA-CAMPUS-VPN(config-network-object)#subnet 172.16.129.0 255.255.255.0
ASA-CAMPUS-VPN(config-network-object)#object network BRANCH_NETWORK
ASA-CAMPUS-VPN(config-network-object)#subnet 172.16.128.0 255.255.128.0
ASA-CAMPUS-VPN(config-network-object)#object network CAMPUS_NETWORK
ASA-CAMPUS-VPN(config-network-object)#subnet 172.16.0.0 255.255.128.0
ASA-CAMPUS-VPN(config-network-object)#object network PRIVATE_NETWORK
ASA-CAMPUS-VPN(config-network-object)#subnet 176.16.0.0 255.255.0.0
ASA-CAMPUS-VPN(config-network-object)#route outside 172.16.129.0 255.255.255.0
134.95.56.18 1
ASA-CAMPUS-VPN(config)#route inside 172.16.0.0 255.255.128.0 172.16.254.253 1
ASA-CAMPUS-VPN(config)#access-list BRANCH01_TRAFFIC extended permit tcp object
CAMPUS_NETWORK object BRANCH01_NETWORK
WARNING: <BRANCH01_TRAFFIC> found duplicate element
ASA-CAMPUS-VPN(config)#access-list BRANCH01_TRAFFIC extended permit icmp object
CAMPUS_NETWORK object BRANCH01_NETWORK
WARNING: <BRANCH01_TRAFFIC> found duplicate element
ASA-CAMPUS-VPN(config)#access-list ENTERPRISE_PRIVATE-TRAFFIC extended permit tcp
object PRIVATE_NETWORK object PRIVATE_NETWORK
WARNING: <ENTERPRISE_PRIVATE-TRAFFIC> found duplicate element
ASA-CAMPUS-VPN(config)#access-list ENTERPRISE_PRIVATE-TRAFFIC extended permit icmp
object BRANCH_NETWORK object CAMPUS_NETWORK
WARNING: <ENTERPRISE_PRIVATE-TRAFFIC> found duplicate element
ASA-CAMPUS-VPN(config)#access-group ENTERPRISE_PRIVATE-TRAFFIC out interface inside
ASA-CAMPUS-VPN(config)#crypto ipsec ikev1 transform-set L2L esp-aes esp-sha-hmac
ASA-CAMPUS-VPN(config)#crypto map BRANCH1 1 match address BRANCH01_TRAFFIC
ASA-CAMPUS-VPN(config)#crypto map BRANCH1 1 set peer 134.95.56.18
```

ASA-CAMPUS-VPN(config)#crypto map BRANCH1 1 set security-association lifetime seconds 86400
ASA-CAMPUS-VPN(config)#crypto map BRANCH1 1 set ikev1 transform-set L2L
ASA-CAMPUS-VPN(config)#crypto map BRANCH1 interface outside
WARNING: crypto map has incomplete entries
ASA-CAMPUS-VPN(config)#crypto ikev1 enable outside
ASA-CAMPUS-VPN(config)#crypto ikev1 policy 1
ASA-CAMPUS-VPN(config-ikev1-policy)#encr aes
ASA-CAMPUS-VPN(config-ikev1-policy)#authentication pre-share
ASA-CAMPUS-VPN(config-ikev1-policy)#group 2
ASA-CAMPUS-VPN(config-ikev1-policy)#
ASA-CAMPUS-VPN(config-ikev1-policy)#tunnel-group 134.95.56.18 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ASA-CAMPUS-VPN(config)#tunnel-group 134.95.56.18 ipsec-attributes
ASA-CAMPUS-VPN(config-tunnel-ipsec)#ikev1 pre-shared-key SHAREDSECRET
ASA-CAMPUS-VPN(config-tunnel-ipsec)#

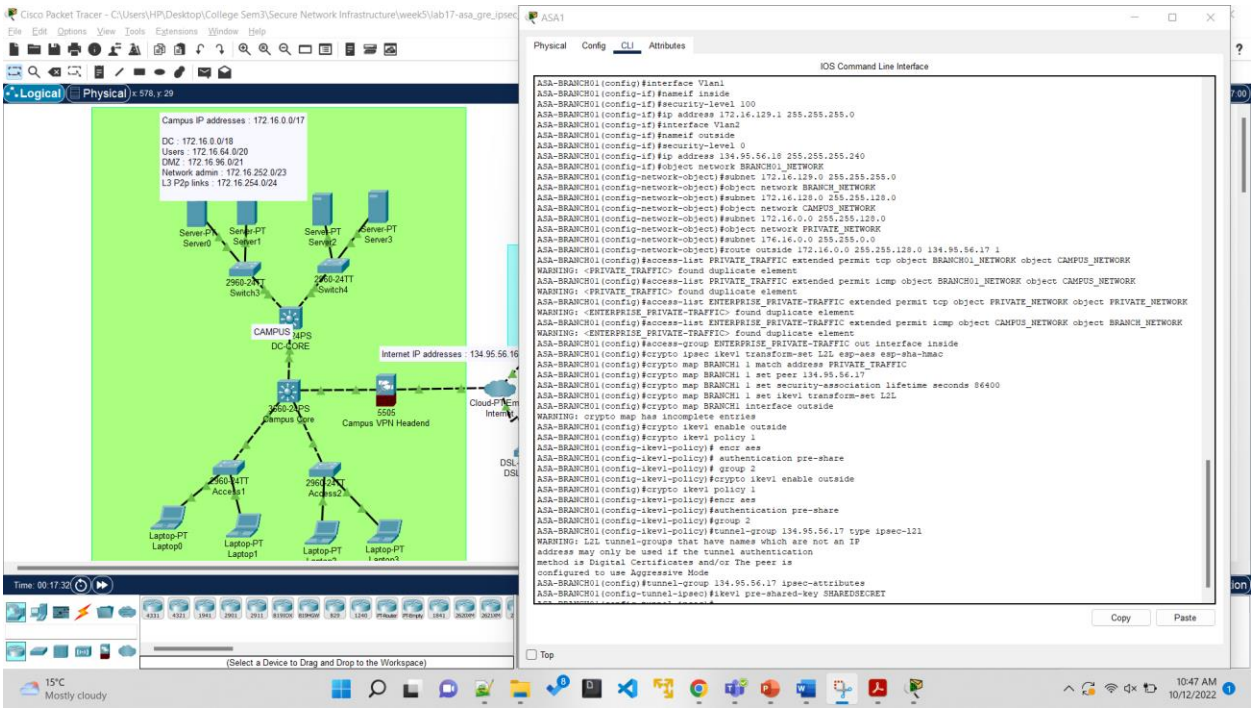


Branch office 1 - ASA 5505 remote device configuration.

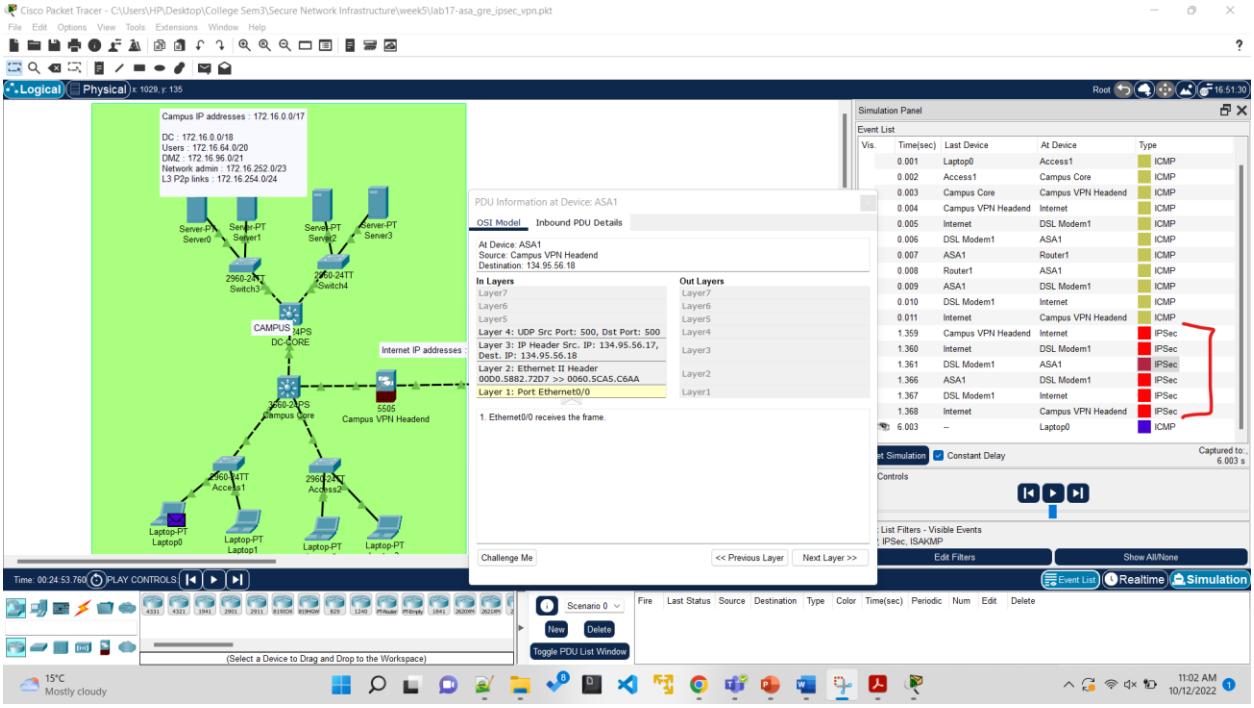
Below commands executed for the setup in Branch ASA.

```
ASA-BRANCH01(config)#interface Vlan1
ASA-BRANCH01(config-if)#nameif inside
ASA-BRANCH01(config-if)#security-level 100
ASA-BRANCH01(config-if)#ip address 172.16.129.1 255.255.255.0
ASA-BRANCH01(config-if)#interface Vlan2
ASA-BRANCH01(config-if)#nameif outside
ASA-BRANCH01(config-if)#security-level 0
ASA-BRANCH01(config-if)#ip address 134.95.56.18 255.255.255.240
ASA-BRANCH01(config-if)#object network BRANCH01_NETWORK
ASA-BRANCH01(config-network-object)#subnet 172.16.129.0 255.255.255.0
ASA-BRANCH01(config-network-object)#object network BRANCH_NETWORK
ASA-BRANCH01(config-network-object)#subnet 172.16.128.0 255.255.128.0
ASA-BRANCH01(config-network-object)#object network CAMPUS_NETWORK
ASA-BRANCH01(config-network-object)#subnet 172.16.0.0 255.255.128.0
ASA-BRANCH01(config-network-object)#object network PRIVATE_NETWORK
ASA-BRANCH01(config-network-object)#subnet 176.16.0.0 255.255.0.0
ASA-BRANCH01(config-network-object)#route outside 172.16.0.0 255.255.128.0 134.95.56.17 1
ASA-BRANCH01(config)#access-list PRIVATE_TRAFFIC extended permit tcp object
BRANCH01_NETWORK object CAMPUS_NETWORK
WARNING: <PRIVATE_TRAFFIC> found duplicate element
ASA-BRANCH01(config)#access-list PRIVATE_TRAFFIC extended permit icmp object
BRANCH01_NETWORK object CAMPUS_NETWORK
WARNING: <PRIVATE_TRAFFIC> found duplicate element
ASA-BRANCH01(config)#access-list ENTERPRISE_PRIVATE-TRAFFIC extended permit tcp object
PRIVATE_NETWORK object PRIVATE_NETWORK
WARNING: <ENTERPRISE_PRIVATE-TRAFFIC> found duplicate element
ASA-BRANCH01(config)#access-list ENTERPRISE_PRIVATE-TRAFFIC extended permit icmp object
CAMPUS_NETWORK object BRANCH_NETWORK
WARNING: <ENTERPRISE_PRIVATE-TRAFFIC> found duplicate element
ASA-BRANCH01(config)#access-group ENTERPRISE_PRIVATE-TRAFFIC out interface inside
ASA-BRANCH01(config)#crypto ipsec ikev1 transform-set L2L esp-aes esp-sha-hmac
ASA-BRANCH01(config)#crypto map BRANCH1 1 match address PRIVATE_TRAFFIC
ASA-BRANCH01(config)#crypto map BRANCH1 1 set peer 134.95.56.17
ASA-BRANCH01(config)#crypto map BRANCH1 1 set security-association lifetime seconds 86400
ASA-BRANCH01(config)#crypto map BRANCH1 1 set ikev1 transform-set L2L
ASA-BRANCH01(config)#crypto map BRANCH1 interface outside
WARNING: crypto map has incomplete entries
ASA-BRANCH01(config)#crypto ikev1 enable outside
```

```
ASA-BRANCH01(config)#crypto ikev1 policy 1
ASA-BRANCH01(config-ikev1-policy)# encr aes
ASA-BRANCH01(config-ikev1-policy)# authentication pre-share
ASA-BRANCH01(config-ikev1-policy)# group 2
ASA-BRANCH01(config-ikev1-policy)#crypto ikev1 enable outside
ASA-BRANCH01(config)#crypto ikev1 policy 1
ASA-BRANCH01(config-ikev1-policy)#encr aes
ASA-BRANCH01(config-ikev1-policy)#authentication pre-share
ASA-BRANCH01(config-ikev1-policy)#group 2
ASA-BRANCH01(config-ikev1-policy)#tunnel-group 134.95.56.17 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ASA-BRANCH01(config)#tunnel-group 134.95.56.17 ipsec-attributes
ASA-BRANCH01(config-tunnel-ipsec)#ikev1 pre-shared-key SHAREDSECRET
ASA-BRANCH01(config-tunnel-ipsec)#
```



Showing IPsec Protocol in the Simulation mode while doing ping from Campus laptop to Branch laptop.



Check the IPSEC tunnel establishment using show commands

For this step I have used Two Commands –

 # show crypto isakmp sa

 # show crypto ipsec sa

1. **Checking first command**

ASA-CAMPUS-VPN#show crypto isakmp sa

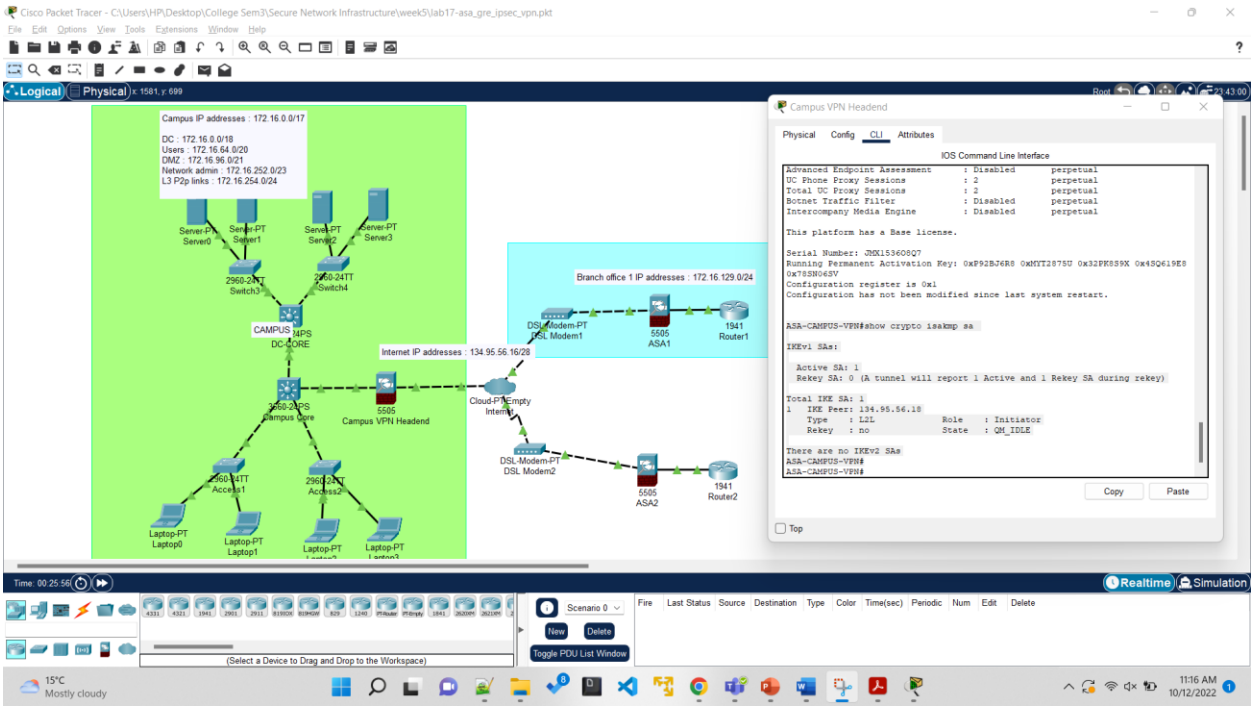
IKEv1 SAs:

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1

1 IKE Peer: 134.95.56.18
Type : L2L Role : Initiator
Rekey : no State : QM_IDLE

There are no IKEv2 SAs
ASA-CAMPUS-VPN#



2. Checking Second command

ASA-CAMPUS-VPN#show crypto ipsec sa

interface: outside
Crypto map tag: BRANCH1, seq num: 1, local addr 134.95.56.17

permit tcp object CAMPUS_NETWORK object BRANCH01_NETWORK
local ident (addr/mask/prot/port): (172.16.0.0/255.255.128.0/6/0)
remote ident (addr/mask/prot/port): (172.16.129.0/255.255.255.0/6/0)
current_peer 134.95.56.18
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors 0, #recv errors 0

local crypto endpt.: 134.95.56.17/0, remote crypto endpt.:134.95.56.18/0
path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
current outbound spi: 0x109FE31C(278913820)
current inbound spi: 0x1B6B7132(278913820)

inbound esp sas:
spi: 0x1B6B7132(460026162)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn id: 2000, crypto map: BRANCH1
sa timing: remaining key lifetime (k/sec): (4525504/86055)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:
0x00000000 0x0000001F
outbound esp sas:
spi: 0x109FE31C(278913820)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn id: 2001, crypto map: BRANCH1
sa timing: remaining key lifetime (k/sec): (4525504/86055)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:

0x00000000 0x00000001

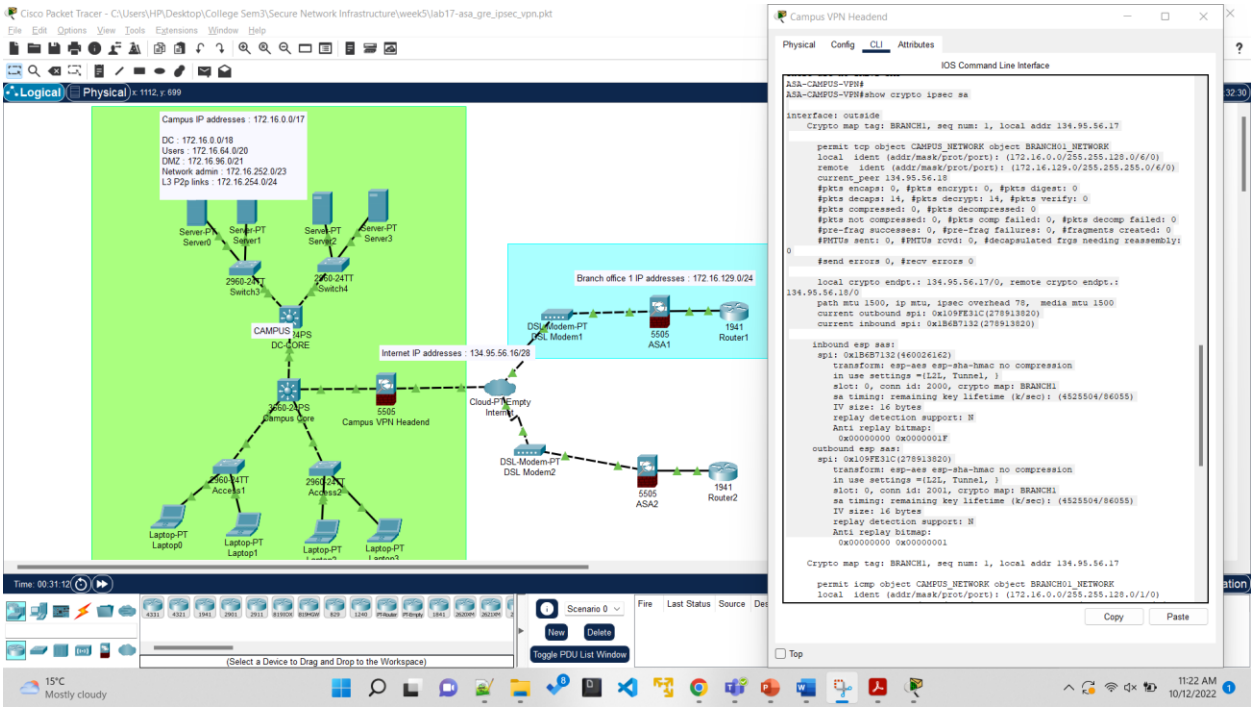
Crypto map tag: BRANCH1, seq num: 1, local addr 134.95.56.17

permit icmp object CAMPUS_NETWORK object BRANCH01_NETWORK
local ident (addr/mask/prot/port): (172.16.0.0/255.255.128.0/1/0)
remote ident (addr/mask/prot/port): (172.16.129.0/255.255.255.0/1/0)
current_peer 134.95.56.18
#pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors 1, #recv errors 0

local crypto endpt.: 134.95.56.17/0, remote crypto endpt.:134.95.56.18/0
path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
current outbound spi: 0x109FE31C(278913820)
current inbound spi: 0x1B6B7132(278913820)

inbound esp sas:
spi: 0x1B6B7132(460026162)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn id: 2000, crypto map: BRANCH1
sa timing: remaining key lifetime (k/sec): (4525504/86055)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:
0x00000000 0x0000001F
outbound esp sas:
spi: 0x109FE31C(278913820)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn id: 2001, crypto map: BRANCH1
sa timing: remaining key lifetime (k/sec): (4525504/86055)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:
0x00000000 0x00000001

ASA-CAMPUS-VPN#
ASA-CAMPUS-VPN#


Cisco Packet Tracer - C:\Users\HP\Desktop\College Sem3\Secure Network Infrastructure\week5\lab17-asa_gre_ipsec_vpn.pkt
Campus VPN Headend
Physical
Config
CLI
Attributes
IOS Command Line Interface
Campus IP addresses : 172.16.0.0/17
DC : 172.16.0.0/18
Users : 172.16.64.0/20
DMZ : 172.16.96.0/21
Network admin : 172.16.252.0/23
L3 P2p links : 172.16.254.0/24
Branch office 1 IP addresses : 172.16.129.0/24
Internet IP addresses : 134.95.56.16/28
CAMPUS DC-CORE
5505 Campus VPN Headend
5505 ASA1
5505 ASA2
1941 Router1
1941 Router2
Laptop-PT Laptop0
Laptop-PT Laptop1
Cloud-PT Empty Internet
DSL-Modem-PT DSL Modem1
DSL-Modem-PT DSL Modem2
(Select a Device to Drag and Drop to the Workspace)
Toggle PDU List Window
Copy
Paste
Top
15°C
Mostly cloudy
11:22 AM
10/12/2022