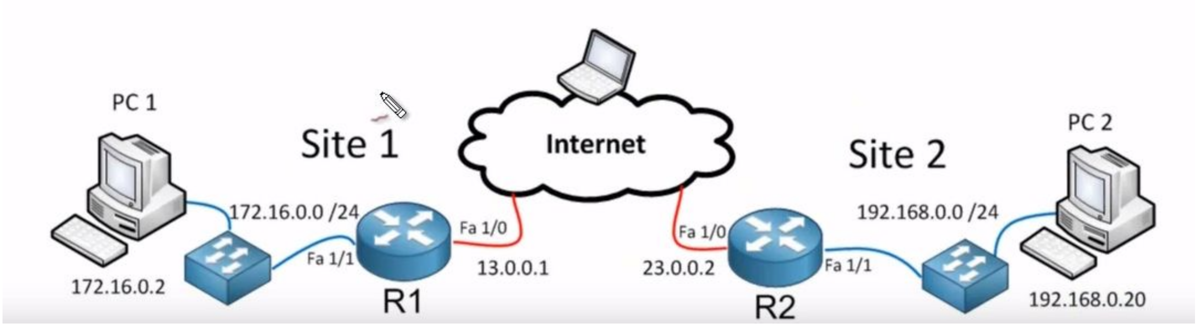
IPSEC Site to Site VPN using GNS3

Introduction to IPSEC

Before sending any packet in the Internet it is recommended to protect it. IPSEC is like a shield that protects packets travelling in the big bad Internet. Internet Protocol Security(IPSec) is a protocol implemented in the Internet layer of the TCP/IP suite. IPSec was invented to provide authentication and confidentiality over network. In the Network Security Project, where I created a OpenVpn which uses TLS (Transport layer) and SSH (Application layer) is implemented at higher layer. In contrast, IPSEC provides same functionality at lower layer(IP layer).

IPSEC can be divided in the following groups:

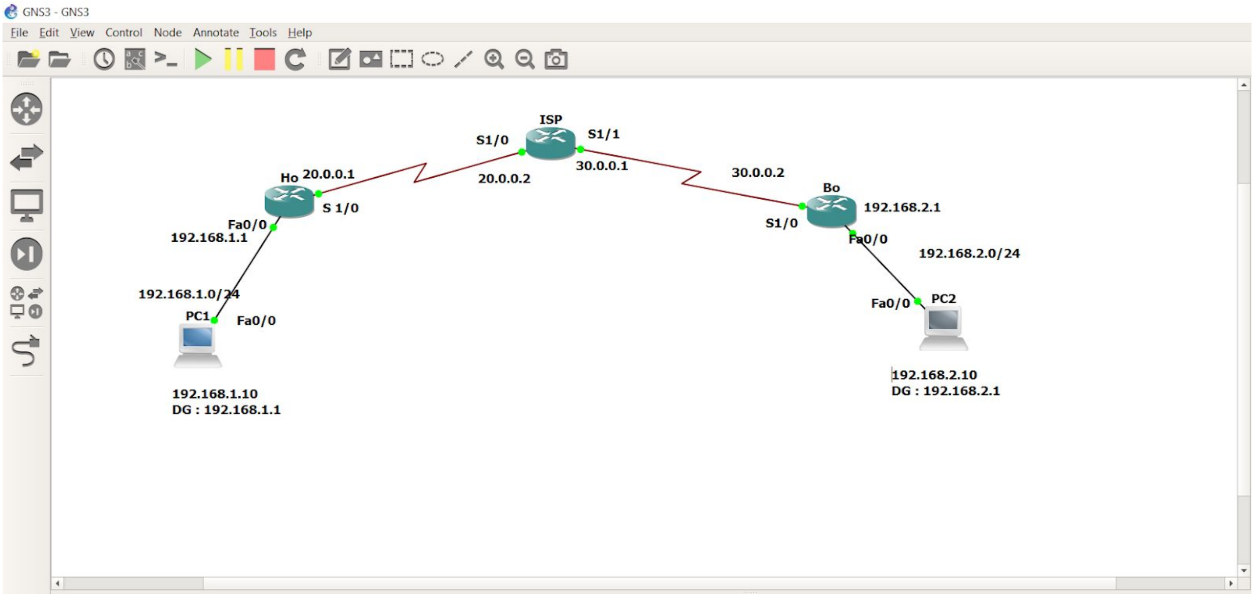
- **Authentication Header(AH)** : Integrity, Authentication
- **Encapsulation Security Payload (ESP)** : Authenticity, Integrity, Confidentiality
- **Security Associations** : Bunch of algorithms and parameters.



The above diagram shows a company located at two different sites (Site1 and Site2). As we can see that both the sites can rightnow connect with each other via Internet. What if this two sites want to share some classified information that can ruin their business if it is lost somewhere in the Internet. Or an eavesdropper is tracking all the data in between. For this reasons IPSEC is implemented in similar situation. Where packets are encrypted and send over a secure tunnel. Imagine creating a bridge connecting two nodes directly. In simple terms, let's suppose that PC1 Wants to send data to PC2. R1 sees that the packet is destined to Site 2 so, it encrypts the packet, encapsulates it and sends it to R2. We can only see that the 13.0.0.1 is sending some gibberish data to 23.0.0.2. Finally, Router 2 decrypts the packets ,encapsulates it and sends it to PC2.

Introduction to GNS3

Graphical Network Simulator - 3 (GNS3) is a network software emulator. It displays a fine GUI to plan, test and troubleshoot network environments across different vendor platform. It does not require direct interaction with the network hardware. After following some online instructions to download and install GNS3 I created a topology as shown below.



In order to create a site to site VPN I followed this manual. Main configuration included enabling isakmp on Ho and Bo routers, part of IKE which specifies the mechanism of key exchange.

```
Ho(config-crypto-map)#set peer 30.0.0.2
```

This command makes 30.0.0.2 that is B0 peer of 20.0.0.1 that is H0. So, any traffic flowing from 20.0.0.1 will be directly forwarded to 30.0.0.2. Similarly at the other side **Bo(config-crypto-map)#set peer 20.0.0.1.**

HO(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 Permits to tunnel all traffic coming from 192.168.1.0/24 network to 192.168.2.0/24. Any other address not in this range will not be permitted.

HO(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
BO(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.1
This two commands are set to specify a gateway address. It simply tells the router to forward all packets that do not have specific routes to the destination network pass through these default gateway.

These commands enables debug for IPSEC and isakmp on both routers and shows VPN process in the routers.

HO#debug crypto ipsec

Crypto IPSEC debugging is on

HO#debug crypto isakmp

Crypto ISAKMP debugging is on

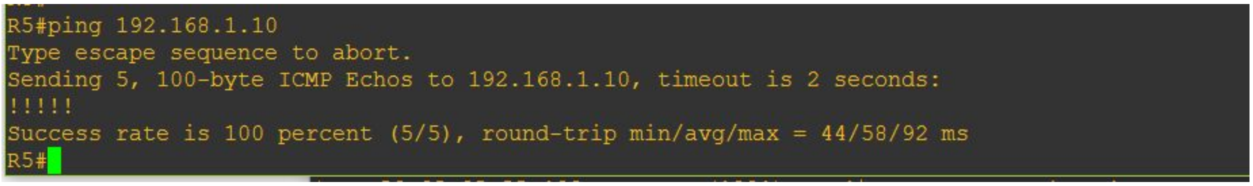
BO#debug crypto ipsec

Crypto IPSEC debugging is on

BO#debug crypto isakmp

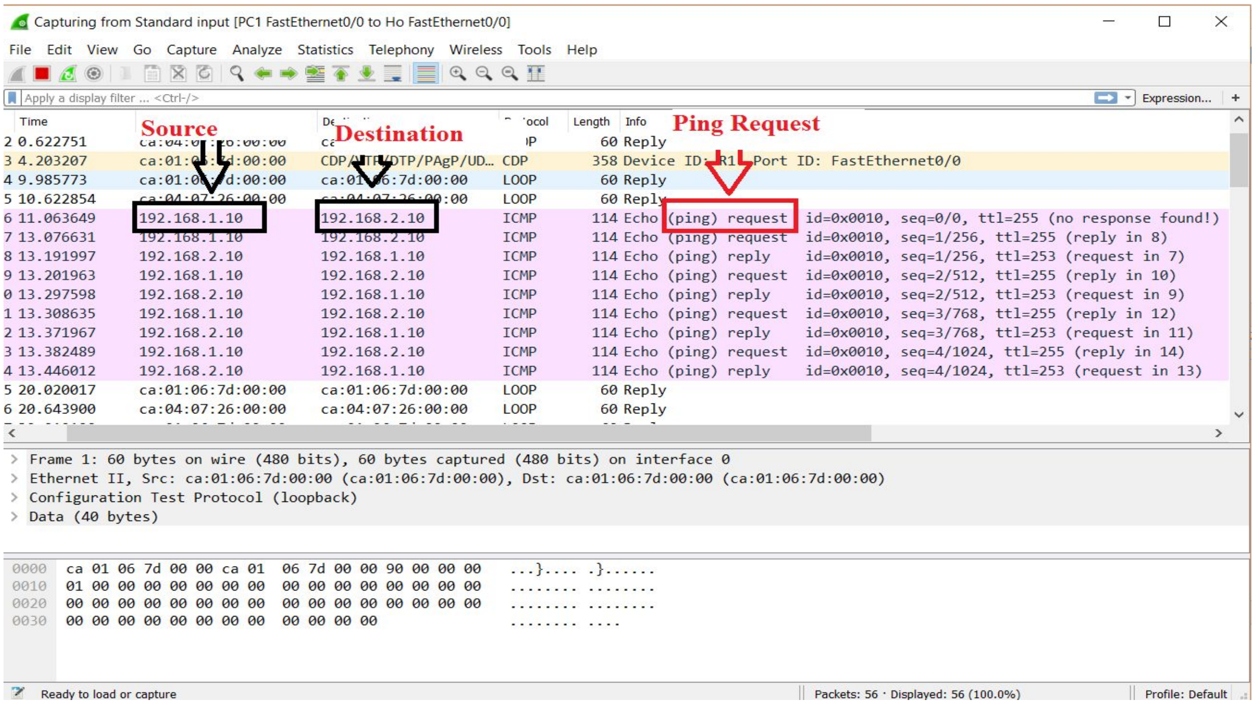
Crypto ISAKMP debugging is on

Once all the configuration were done correctly, when I try to ping 192.168.2.10 from 192.168.1.10 I got 100% success rate.



```
R5#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/58/92 ms
R5#
```

Packet capture in Wireshark

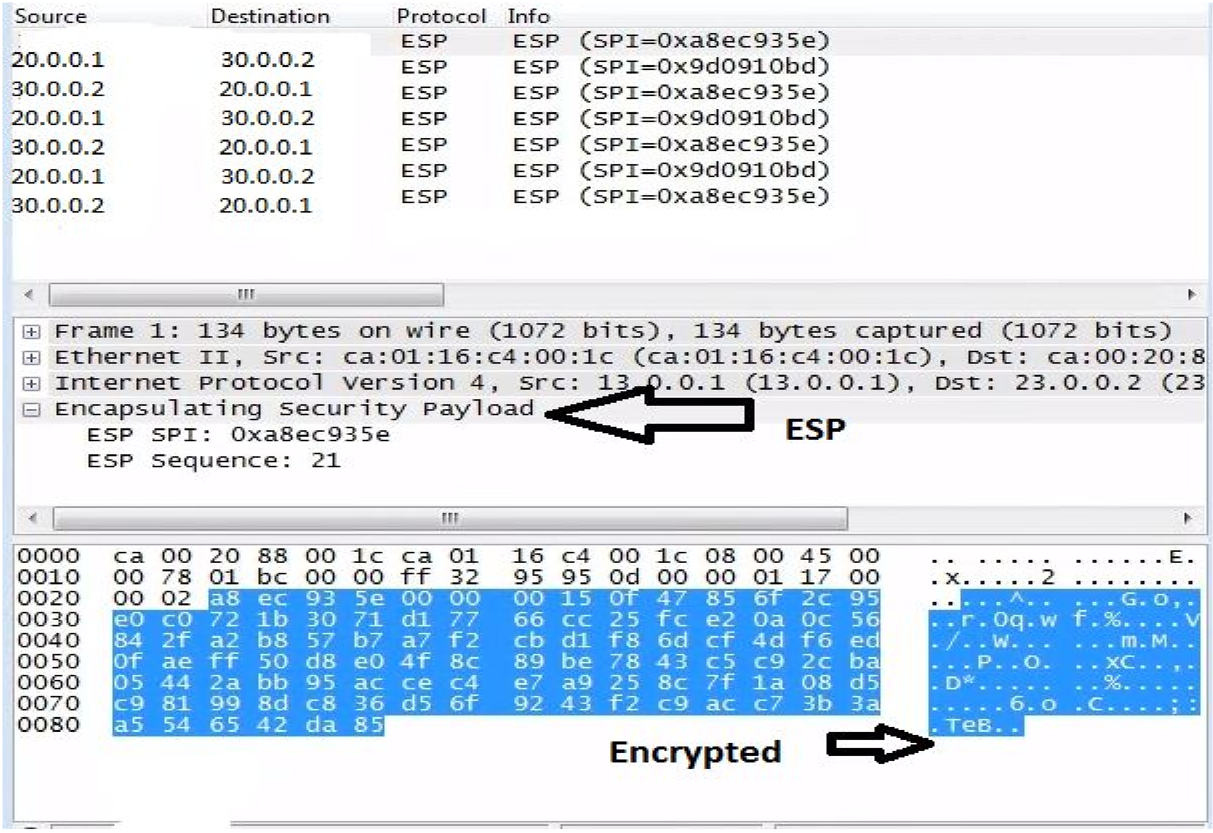

Capturing from Standard input [PC1 FastEthernet0/0 to Ho FastEthernet0/0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Source
Destination
Ping Request

```
  Time          Source              Destination               Protocol  Length  Info
2 0.622751      ca:04:07:26:00:00   ca                        P            60 Reply
3 4.203207      ca:01:06:7d:00:00   CDP/VTP/DTP/PAgP/UD...    CDP         358 Device ID: R1  Port ID: FastEthernet0/0
4 9.985773      ca:01:06:7d:00:00   ca:01:06:7d:00:00         LOOP         60 Reply
5 10.622854     ca:04:07:26:00:00   ca:04:07:26:00:00         LOOP         60 Reply
6 11.063649     192.168.1.10        192.168.2.10              ICMP        114 Echo (ping) request  id=0x0010, seq=0/0, ttl=255 (no response found!)
7 13.076631     192.168.1.10        192.168.2.10              ICMP        114 Echo (ping) request  id=0x0010, seq=1/256, ttl=255 (reply in 8)
8 13.191997     192.168.2.10        192.168.1.10              ICMP        114 Echo (ping) reply    id=0x0010, seq=1/256, ttl=253 (request in 7)
9 13.201963     192.168.1.10        192.168.2.10              ICMP        114 Echo (ping) request  id=0x0010, seq=2/512, ttl=255 (reply in 10)
0 13.297598     192.168.2.10        192.168.1.10              ICMP        114 Echo (ping) reply    id=0x0010, seq=2/512, ttl=253 (request in 9)
1 13.308635     192.168.1.10        192.168.2.10              ICMP        114 Echo (ping) request  id=0x0010, seq=3/768, ttl=255 (reply in 12)
2 13.371967     192.168.2.10        192.168.1.10              ICMP        114 Echo (ping) reply    id=0x0010, seq=3/768, ttl=253 (request in 11)
3 13.382489     192.168.1.10        192.168.2.10              ICMP        114 Echo (ping) request  id=0x0010, seq=4/1024, ttl=255 (reply in 14)
4 13.446012     192.168.2.10        192.168.1.10              ICMP        114 Echo (ping) reply    id=0x0010, seq=4/1024, ttl=253 (request in 13)
5 20.020017     ca:01:06:7d:00:00   ca:01:06:7d:00:00         LOOP         60 Reply
6 20.643900     ca:04:07:26:00:00   ca:04:07:26:00:00         LOOP         60 Reply

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: ca:01:06:7d:00:00 (ca:01:06:7d:00:00), Dst: ca:01:06:7d:00:00 (ca:01:06:7d:00:00)
> Configuration Test Protocol (loopback)
> Data (40 bytes)

0000  ca 01 06 7d 00 00 ca 01  06 7d 00 00 90 00 00 00   ...}.... .}......
0010  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....

Ready to load or capture        Packets: 56 · Displayed: 56 (100.0%)        Profile: Default
```



```
Source        Destination      Protocol  Info
                               ESP       ESP (SPI=0xa8ec935e)
20.0.0.1      30.0.0.2         ESP       ESP (SPI=0x9d0910bd)
30.0.0.2      20.0.0.1         ESP       ESP (SPI=0xa8ec935e)
20.0.0.1      30.0.0.2         ESP       ESP (SPI=0x9d0910bd)
30.0.0.2      20.0.0.1         ESP       ESP (SPI=0xa8ec935e)
20.0.0.1      30.0.0.2         ESP       ESP (SPI=0x9d0910bd)
30.0.0.2      20.0.0.1         ESP       ESP (SPI=0xa8ec935e)

⊞ Frame 1: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
⊞ Ethernet II, Src: ca:01:16:c4:00:1c (ca:01:16:c4:00:1c), Dst: ca:00:20:8
⊞ Internet Protocol Version 4, Src: 13.0.0.1 (13.0.0.1), Dst: 23.0.0.2 (23
⊟ Encapsulating Security Payload
     ESP SPI: 0xa8ec935e
     ESP Sequence: 21

0000   ca 00 20 88 00 1c ca 01   16 c4 00 1c 08 00 45 00    .. ..... ......E.
0010   00 78 01 bc 00 00 ff 32   95 95 0d 00 00 01 17 00    .x.....2 ........
0020   00 02 a8 ec 93 5e 00 00   00 15 0f 47 85 6f 2c 95    .....^.. ...G.o,.
0030   e0 c0 72 1b 30 71 d1 77   66 cc 25 fc e2 0a 0c 56    ..r.0q.w f.%....V
0040   84 2f a2 b8 57 b7 a7 f2   cb d1 f8 6d cf 4d f6 ed    ./..W... ...m.M..
0050   0f ae ff 50 d8 e0 4f 8c   89 be 78 43 c5 c9 2c ba    ...P..O. ..xC..,.
0060   05 44 2a bb 95 ac ce c4   e7 a9 25 8c 7f 1a 08 d5    .D*..... ..%.....
0070   c9 81 99 8d c8 36 d5 6f   92 43 f2 c9 ac c7 3b 3a    .....6.o .C....;:
0080   a5 54 65 42 da 85                                    .TeB..
```