**Group C- Assignment No. 17**

**Title:**

To study the IPsec (ESP and AH) protocol by capturing the packets using Wiresharktool.

**Outcomes:**

Retrieve IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.

.

**Theory:**

**The IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols

between 2 communica

and conﬁden

ts. The

protocols needed for secure key exchange and key management are deﬁned in it.

**What Ports Does IPSEC Operate On?**

UDP port 500 should be opened as should IP protocols 50 and 51. UDP port 500 should be opened

to allow for ISAKMP to be forwarded through the ﬁrewall while protocols 50 and 51 allow ESP and

AH traﬃc to be forwarded resp

**What is ISAKMP?**

ISAKMP stands for Internet Security Associa

components of an IPSEC VPN that must be in place in order for it to func

the public traﬃc that is being forwarded between the client and VPN server or VPN server to VPN

server.

**What are ESP and AH?**

No, ESP is not Extra-Sensory Percep

stands for Authen

**Encapsula**

ESP gives prot

area indica

wherea protected

data packet has been signed for integrity, and an Encrypted area which

indicates the informa

tunneled, ESP protects only the IP data payload (hence the name), and not the IP header.

ESP may be used to ensure conﬁden

integrity, some degree of traﬃc-level conﬁden

-replay service (a form of p

sequence integrity which guards against the use of commands or creden

captured through password sniﬃng or similar a

**Authen**

Authen

protocol suite, which authen

of IP packets (datagrams) and guarantees the

integrity of the data. The AH conﬁrms the origina

contents (both the header and payload) have not been changed since transmission. If security

associa

a

een established, AH can be

dow technique.4

**How Do They All Work Together?**

When properly conﬁgured, an IPSEC VPN provides mu

security mode and integrity of the data that is

being tran

the data has not been intercepted and altered in transit and that they can rely on what they are

seeing.

IPsec Protocols

AH and/or ESP are the two protocols that we use to actually protect user data. Both of them can be

used in transport or tunnel mode, let’s walk through all the possible

Authen

Protocol

AH oﬀers authen

by calcula

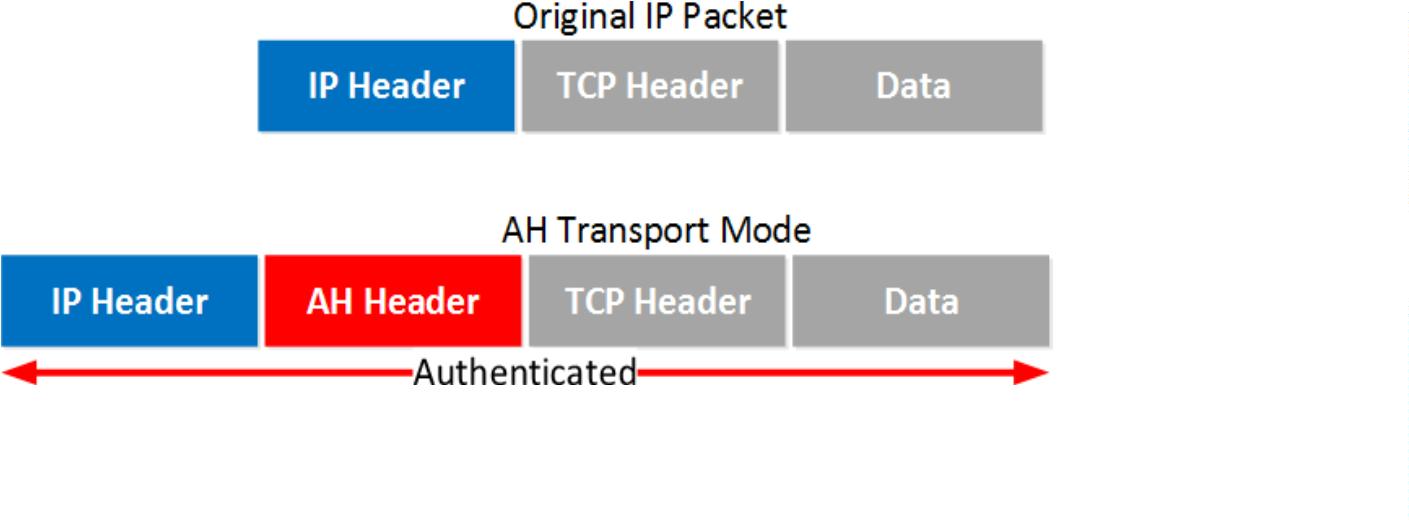
encryp

that can be changed

in transit (TTL and header checksum). Let’s start with transport mode… Transport mode is simple, it

just adds an AH header aﬅer the IP header. Her e’s anexample of an IP packet that carries some

TCP traﬃc:



**And here’s what that looks like in Wireshark:**

Above you can see the AH header in between the IP header and ICMP header. This is acapture I

took of a ping between two routers. You can see that AH uses 5 ﬁelds:

**Next Header**: this iden

**Length**: this is the length of the AH header.

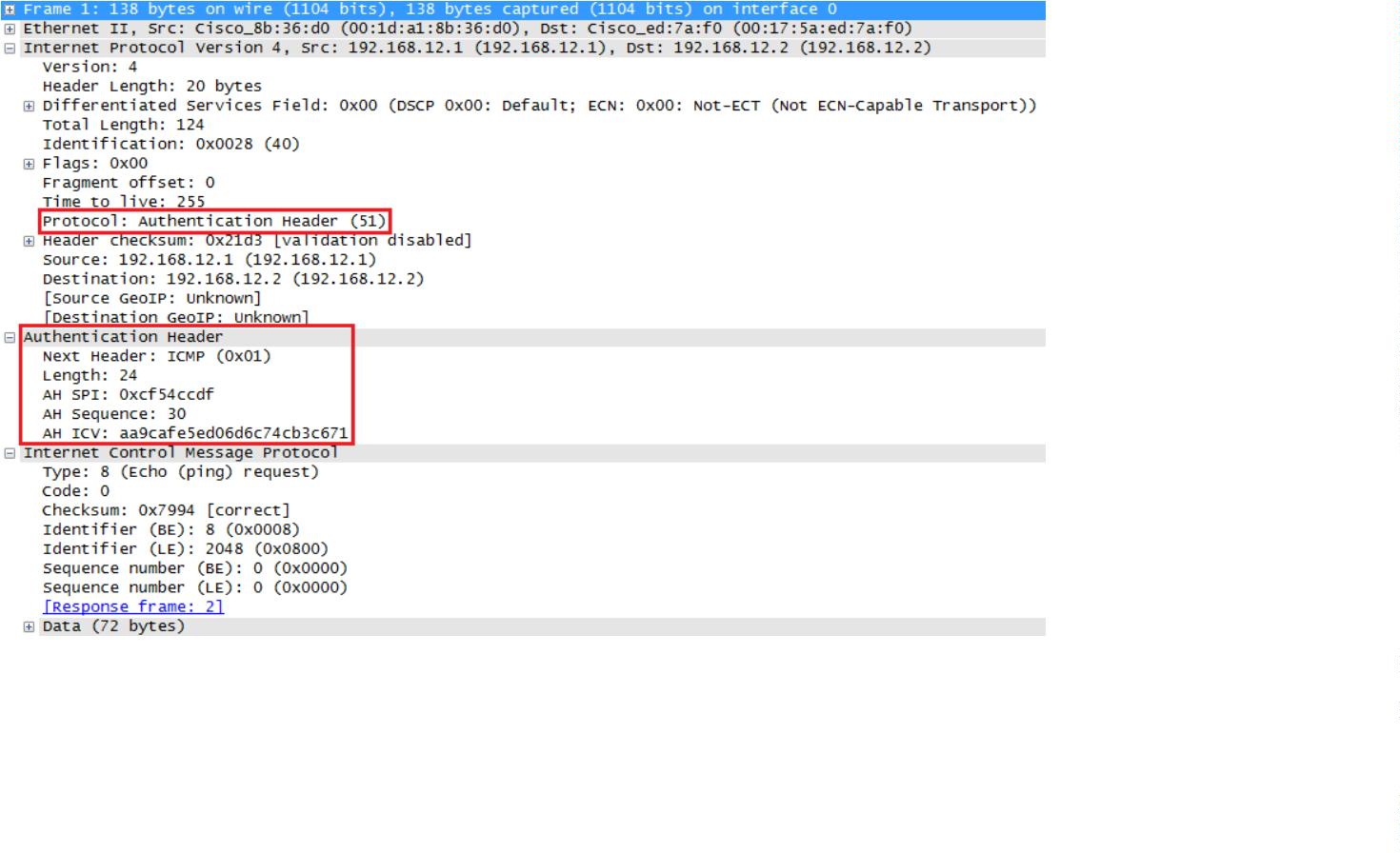
**SPI (Security Parameters Index)**: this is an 32-bit iden

packet belongs.

**Sequence**: this is the sequence number that helps against replay a

**ICV (Integrity Check Value)**: this is the calculated hash for the en

calculates a hash, when it’s not the same you know something is wrong.

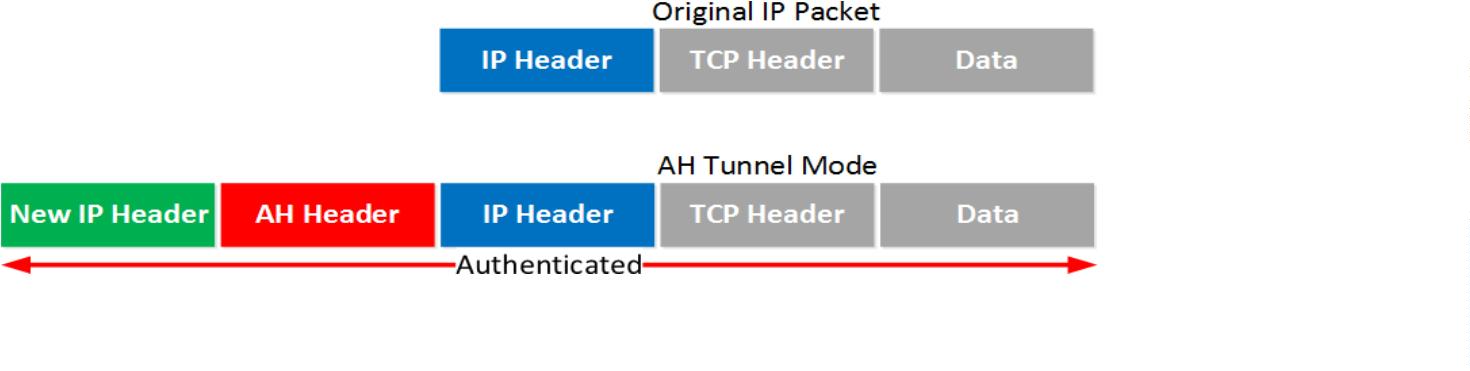


Let’s c

could be useful when you are using private IP addresses and you need to tunnel your traﬃc over

the Internet. It’s possible with AH but it doesn’t oﬀer encryp on:

**The en**



Above you can see the new IP header, then the AH header and ﬁnally the original IPpacket that

carries some ICMP traﬃc.

One problem with AH is that it doesn’t play well with NAT / PAT. Fields in the IP header like TTL and

the checksum are excluded by AH because it knows these will change. The IP addresses and port

numbers however are included. If you change these with N AT, the ICV of AH fails.

Let’s c

ESP (Encapsula

ESP is the more popular choice of the two since it allows you to encrypt IP traﬃc. Wecan use it in

transport or tunnel mode, let’s look at both.

Transport Mode

When we use transport mode, we use the original IP header and insert an ESP header.Here’s what

it looks like:

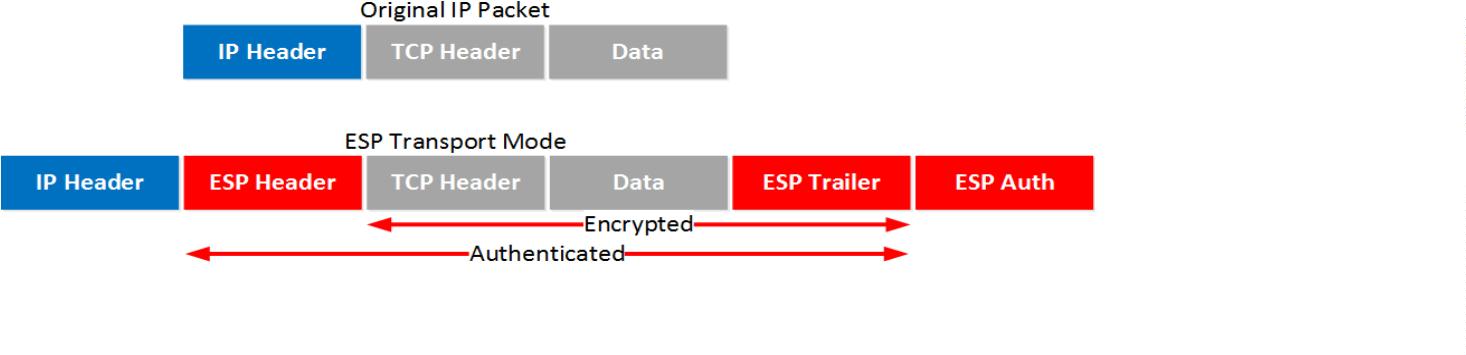
Above you can see that we add an ESP header and trailer. Our transport layer (TCP for example)

and payload will be encrypted. It also oﬀers authen

packet.

but unlike AH, it’snot for the en

IP



**Here’s what it looks like in wireshark:**

Above you can see the original IP packet and that we are using ESP. The IP header is incleartext but

everything else is encrypted.

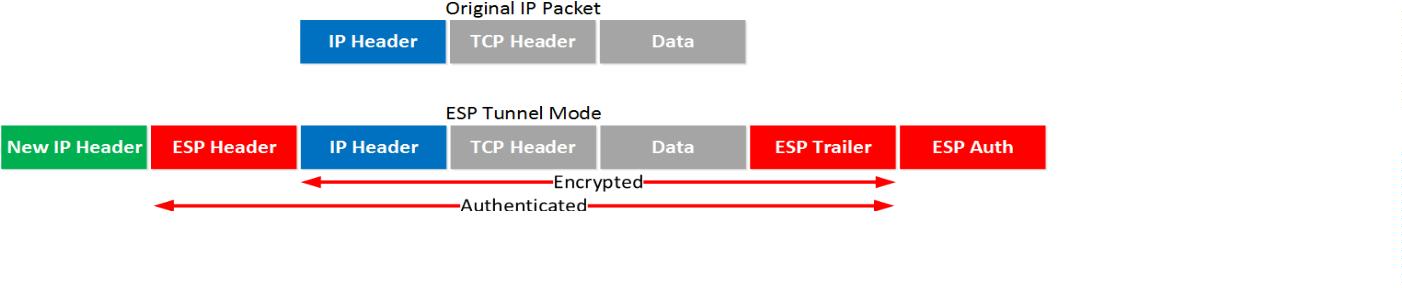
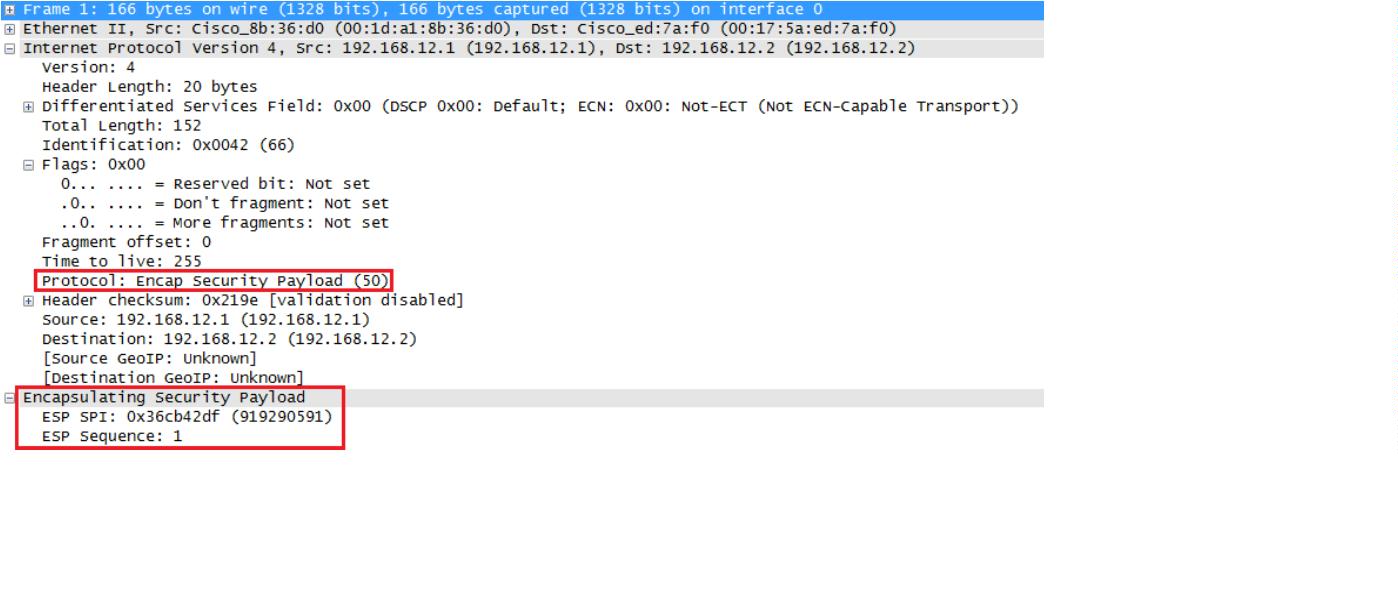
**Tunnel Mode**

How about ESP in tunnel mode? This is where we use a new IP header which is usefulfor site-to-

site VPNs:

It’s similar to transport mode but we add a new header. The original IP header is nowalso

encrypted.



**Here’s what it looks like in wireshark:**

The output of the capture is above is similar to what you have seen in transport mode.The only

diﬀerence is that this is a new IP header, you don’t get to see the original IPheader.

AH and ESP

This one confuses a lot of people, it’s possible to use AH and ESP at the same

out!

Transport Mode

Let’s start with transport mode, here’s what the IP packet will look like:

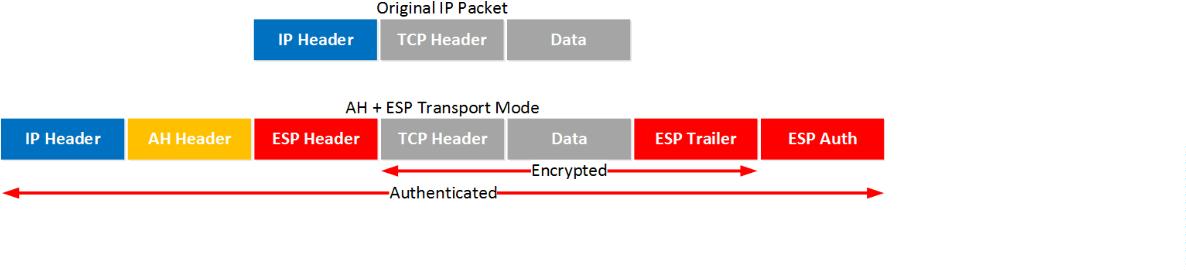
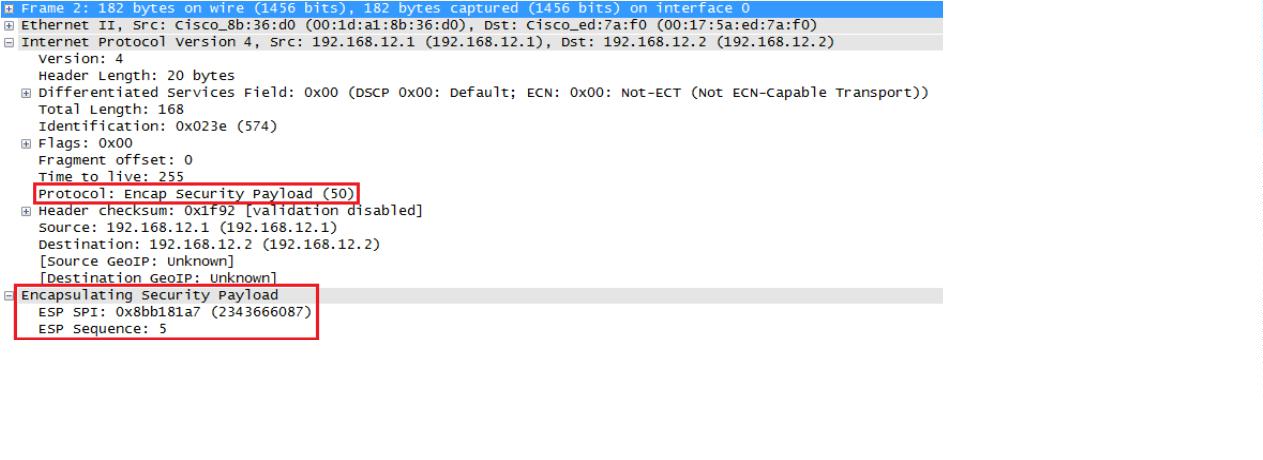
With transport mode we will use the original IP header, followedby an AH and ESPheader. The

transport layer, payload and ESP trailer will be encrypted.

Because we also use AH, the en

IP packet is authen

Here’s what it looks likein wireshark:



Above you can see the original IP packet, the AH header and the ESP header.

**Conclusion:**

Hence we had studied the IPsec (ESP and AH) protocol by capturing the packets

usingWireshark tool.

