**IFT 266 Introduction to Network Information Communication Technology (ICT)   
  
Lab 43**

**Packet Sniffer & IPSec**

Co-authored by Steven Zeck

**After you complete each step, put a ‘√’ or ‘x’ in the completed box**

**Or**

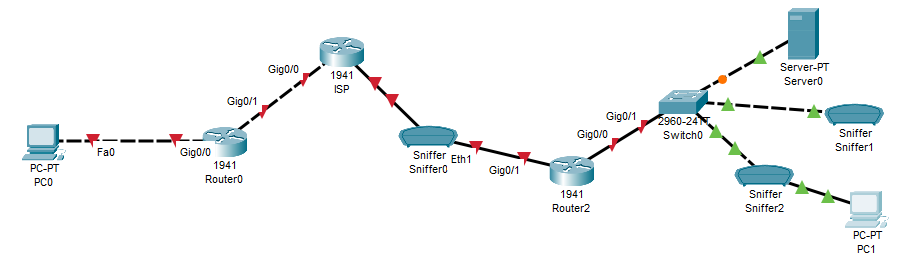
**Insert a screenshot where required**

**Or**

**Answer any open questions**

**Objective:** Wewill simulate network traffic running between two networks via a 3rd, untrusted, network. We will demonstrate what traffic sniffers are able to see, and then create an IPSec VPN to bypass one of the sniffers.

1. Set up the following topology in packet tracer.



You do not need to install additional modules in any devices.

Rename the router in the middle “ISP” (set the display name & hostname to “ISP”)

We will be configuring ports on the routers later, so if you can keep which connection is Gig0/0 and which is Gig0/1 the same as in the diagram that will help later.



# Configure networking on the left network

|  |  |
| --- | --- |
| PC0 | |
| IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.1.254 |

Make sure Router0’s GigabitEthernet0/0 port is the one connected to PC0 and 0/1 is to the ISP

|  |  |
| --- | --- |
| Router0: GigabitEthernet0/0 | |
| IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |

|  |  |
| --- | --- |
| Router0: GigabitEthernet0/1 | |
| IP Address | 172.16.1.1 |
| Subnet Mask | 255.255.0.0 |

Make sure ISP’s GigabitEthernet0/0 port is the one connected to Router0

|  |  |
| --- | --- |
| ISP: GigabitEthernet0/0 | |
| IP Address | 172.16.1.254 |
| Subnet Mask | 255.255.0.0 |

Make sure all the configured ports are up and the connections between PC0 and ISP are green.

Test your configuration:

* From PC0, ping 172.16.1.1 (should be successful)
* If it fails, troubleshoot. Are all 3 ports up? IPs correct? Subnet masks OK?
* From PC0, try to ping 172.16.1.254 (should time out)

Insert a screenshot of your pings to both 172.16.1.1 and 172.16.1.254 below

# Configure networking on the right network

On all 3 Sniffers:

1. Open the “GUI” tab
2. Click Show All/None to set the Event List Filters to ‘None’
3. Click ‘Edit Filters’
4. In the IPv4 Tab, enable ARP, ICMP
5. In the Misc Tab, enable HTTP, HTTPS

|  |  |
| --- | --- |
| Server0 | |
| IP Address | 192.168.2.1 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.2.254 |

|  |  |
| --- | --- |
| PC1 | |
| IP Address | 192.168.2.2 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.2.254 |

Make sure Router2’s GigabitEthernet0/0 port is the one connected to the switch and 0/1 is to the Sniffer

|  |  |
| --- | --- |
| Router2: GigabitEthernet0/0 | |
| IP Address | 192.168.2.254 |
| Subnet Mask | 255.255.255.0 |

|  |  |
| --- | --- |
| Router2: GigabitEthernet0/1 | |
| IP Address | 172.17.2.1 |
| Subnet Mask | 255.255.0.0 |

Make sure ISP’s GigabitEthernet0/1 port is the one connected to Router2

|  |  |
| --- | --- |
| ISP: GigabitEthernet0/1 | |
| IP Address | 172.17.2.254 |
| Subnet Mask | 255.255.0.0 |

Make sure all the configured ports are up.

At this point, all connections should be green. If not, troubleshoot.



# Testing the right side

* On Sniffer2 (connected to PC1), open the GUI tab, then hit **Clear**
* From PC1, ping Router2’s 172.17.2.1 address
* From PC1, open a web browser (under ‘**Desktop**’) and navigate to <https://192.168.2.1/>
* If your ping fails, or web browser times out, troubleshoot.
* Open Sniffer2’s GUI. You should see HTTPS and ICMP traffic. If not, look at Sniffer2’s filters.



### Open the other 2 sniffers. Which other ones have ICMP or HTTPS traffic?

### For any sniffers that don’t show traffic, why aren’t they seeing it?

### Delete the switch and replace it with a PT-Hub (under Network Devices > Hubs)

Reconnect all network cables (you can use the “Automatically Choose Connection Type” option)

From PC1, ping Router2’s 172.17.2.1 address again

1. Now look at all 3 sniffers.  
     
   Are any sniffers showing ICMP activity that weren’t before? Why or why not?

# Configure static routes on the entire network.

**Router0:**

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.254

**Router2:**

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip route 0.0.0.0 0.0.0.0 172.17.2.254

**ISP:**

ISP>en

ISP#conf t

Enter configuration commands, one per line. End with CNTL/Z.

ISP(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1

ISP(config)#ip route 192.168.2.0 255.255.255.0 172.17.2.1



1. Can you ping from PC0 to Server0?  
   If not, troubleshoot.

Clear the events on all 3 sniffers.

From PC0, open a web browser and go to <https://192.168.2.1/>

Sniffer0 and Sniffer1 (and hopefully Sniffer2) should show the HTTPS activity.

If Sniffer2 doesn’t show the activity, change the “Incoming Packets” toggle to the other port.



# Configuring an IPSec VPN

In the networking world, we often send our network traffic through networks that we don’t control. If we are sending sensitive data from one place to another, there’s a chance that some network along the way has been compromised by hackers, foreign governments or is inappropriately storing data that passes through it.

As we saw when we visited a website from PC0, the activity was visible to sniffers along the way. You should assume that all traffic that leaves your network is public.

We can use encrypted protocols like HTTPS or SSH to hide our traffic when visiting websites or connecting to remote consoles. Sometimes though, we don’t have access to these. We may be trying to get two old systems to talk to each other, or we are asked to make sure the connection is secure without knowing how it will be used.

IPSec is a generic encryption protocol. It allows us to establish a secure link between 2 computers, where all the traffic passing between the two will be encrypted. If you set it up between 2 routers, then all the traffic from the subnets behind those routers will be encrypted when it is in transit between the two subnets.

Unfortunately, IPSec has a lot of options that need to be configured identically on each end in order to work. It is also considered “military grade” security, so it doesn’t come enabled by default.

### On both Router0 and Router2, run these commands to enable the IPSec module:

Router#conf t

*Enter configuration commands, one per line. End with CNTL/Z.*

Router(config)#license boot module c1900 technology-package securityk9

Type **yes** when prompted

*Module name = C1900 Next reboot level = securityk9 and License = securityk9*

Router(config)#end

Router#copy run start

Destination filename [startup-config]?

*Building configuration...*

*[OK]*

Router#reload

 Reboot the router with the new module

### We’ve only enabled the module, we still need to set it up on both routers

Router0

Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

Router(config)#crypto isakmp policy 10

Router(config-isakmp)#encryption aes 256

Router(config-isakmp)#authentication pre-share

Router(config-isakmp)#group 5

Router(config-isakmp)#exit

Router(config)#crypto isakmp key donkey address 172.17.2.1

Router(config)#crypto ipsec transform-set router0->router2 esp-aes esp-sha-hmac

Router(config)#crypto map ipsec-map 10 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)#set peer 172.17.2.1

Router(config-crypto-map)#set pfs group5

Router(config-crypto-map)#set security-association lifetime seconds 86400

Router(config-crypto-map)#set transform-set router0->router2

Router(config-crypto-map)#match address 100

Router(config-crypto-map)#exit

Router(config)#int g0/1

Router(config-if)#crypto map ipsec-map

*\*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON*

It’s nearly identical on Router2, but we use the IPs of Router0 and reverse the access-list

Router(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

Router(config)#crypto isakmp policy 10

Router(config-isakmp)#encryption aes 256

Router(config-isakmp)#authentication pre-share

Router(config-isakmp)#group 5

Router(config-isakmp)#exit

Router(config)#crypto isakmp key donkey address 172.16.1.1

Router(config)#crypto ipsec transform-set router2->router0 esp-aes esp-sha-hmac

Router(config)#crypto map ipsec-map 10 ipsec-isakmp

Router(config-crypto-map)#set peer 172.16.1.1

Router(config-crypto-map)#set pfs group5

Router(config-crypto-map)#set security-association lifetime seconds 86400

Router(config-crypto-map)#set transform-set router2->router0

Router(config-crypto-map)#match address 100

Router(config-crypto-map)#exit

Router(config)#int g0/1

Router(config-if)#crypto map ipsec-map

# Test the VPN

From PC0, ping Server0 (192.168.2.1) again.

Be patient, it may take a while (“Request timed out”). You may need to enter the ping command two or three times before it is successful.

The two routers need to negotiate several layers of encryption with each other.

If your pings are still failing after a minute, make sure you entered the settings as shown above and didn’t get any errors.

The highlighted sections are changed between Router0 and Router2.

In the final steps, interface g0/1 on both routers is the one connected to the ISP. If you connected them differently, you’ll have to adjust it.

My pings are succeeding, but how is this any better than before?



### Clear the events on all three sniffers and ping again from PC0 to Server0.

Which sniffers are showing ICMP activity?

On Sniffer0:

* Clear events (if there are any)
* Edit Filters > Misc
* Enable IPSec

From PC0, ping Server0 again.

Insert a screenshot of Sniffer0’s GUI events.   
Make sure to include the event list filters in the picture.

# **Some light reading……What did we do?**

IPSec negotiates several layers of encryption between 2 computers (called “peers”). When it’s all set up, traffic between the peers is encoded so that anyone who sees the traffic while it is en route from one peer to another won’t be able to tell what’s in it.

An intermediate host can tell that *there is some encrypted traffic happening*, and they can see that it is going between the two routers, but they can’t see more than that. While normally, the ISP would be able to tell that PC0 is visiting a website on Server0, with IPSec up the ISP can only tell that Router0 is talking to Router2.

You’ll note that there were a lot of options to configure. The settings have to match exactly on both peers. If there’s a mismatch, the VPN can’t be established. This works best when both peers are the same type of equipment (eg. Cisco routers). Different equipment manufacturers support different settings and trying to get 2 different devices to create an IPSec tunnel is usually very difficult.

Since it’s so complicated to setup, IPSec is usually only used at the router-to-router level, to secure all the communication between two networks. There are products like Cisco Anyconnect that simplify the process for individual users who are working remotely. Anyconnect can be installed on mobile devices or laptops, and creates a secure channel between that laptop and an office network.

On the plus side, once IPSec is setup and working, it tends to keep working without any problems. Both peers should maintain the encrypted connection indefinitely.



## **What were all those configuration options?**

The reason there are so many options is because hackers are clever, and there are lots of ways they can try to eavesdrop or sabotage your initial attempt to setup a connection.

**access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255**

*Cisco switches support* ***access lists****, where we can define which IP addresses are allowed to talk to which other ones. By default, all IPs can talk to all other IPs, so this seems redundant. However, their IPSec configuration also uses this feature to decide when to use the IPSec VPN vs. when to just send normal traffic. The “100” here is the ID of this rule that we will refer to later.*

**Router(config)#crypto isakmp policy 10**

*IPSec has many smaller protocols (AH, ISAKMP, ESP). ISAKMP is used when two peers are trying to setup a new connection with each other.*

**Router(config-isakmp)#encryption aes 256**

*Use the AES algorithm for encryption (the other options on this device are DES and 3DES, which are old and busted algorithms from the 1970s that are easily cracked nowadays)*

**Router(config-isakmp)#authentication pre-share**

*Pre-Share = configure a password on both sides*

**Router(config-isakmp)#group 5**

*This refers to Diffie-Helman Groups, which is an algorithm used when setting up a connection. The higher the number, the more secure the connection. The highest number supported on these routers is 5, so we’re going with that.*

**Router(config)#crypto isakmp key donkey address 172.17.2.1**

*When talking to 172.17.2.1 (the other router) with ISAKMP, our secret password is “donkey” (will need to be configured the same on the other router).*

**Router(config)#crypto ipsec transform-set router0->router2 esp-aes esp-sha-hmac**

*Define a rule for what encryption algorithms are acceptable once we have made contact with our other peer. We name our rule “router0->router2”, but you can use anything.*

*esp-aes:*

*esp = hide the IP addresses of the hosts that want to talk to each other*

*AES = use the AES encryption algorithm to do the hiding*

*esp-sha-hmac:*

*esp = same as above*

*sha-hmac = use the hmac+sha algorithms to do the hiding*

*The dashes mean we want the algorithms to be used together. If the other side can’t do ESP, we don’t want to talk to them at all. Likewise, if the other side can do ESP, but only with old and busted algorithms (esp-des), then that’s just as bad and we don’t want to make a connection. We are offering the other peer a choice; they can use either ESP+AES or ESP+SHA+HMAC. If they can do both, we’ll probably get the first one in the list (ESP+AES).*

**Router(config)#crypto map ipsec-map 10 ipsec-isakmp**

*Define a new ipsec connection that uses ISAKMP. The name will be “ipsec-map”.*

**Router(config-crypto-map)#set peer 172.17.2.1**

*Set the IP of the other side of this connection. It must not be an IP address inside the subnet we are trying to build a VPN to (192.168.2.0/24), since we’re telling the router to only talk to that network over an encrypted connection, and it needs to talk un-encrypted to its peer at the beginning to set that up. That leaves us with the other router’s other (ISP-side) IP address.*

**Router(config-crypto-map)#set pfs group5**

*PFS is another encryption algorithm that uses Diffie-Helman groups. PFS protects some details when the two peers are doing their initial setup. We want to enable it and use the highest-numbered group available (5).*

**Router(config-crypto-map)#set security-association lifetime seconds 86400**

*Sets a max age on the VPN connection. The default is 3600 (1 hour), which means the peers will halt all communication between subnets and spend 5-6 seconds rebuilding the connection every hour. We’ll set it to 86400 seconds (1 day) instead.*

**Router(config-crypto-map)#set transform-set router0->router2**

*Which encryption algorithms to use. We previously defined a set of acceptable algorithms with “crypto ipsec transform-set router0->router2”. If you will be setting up lots of IPSec VPNs, you could give that set a more generic name instead and re-use that set for all your connections.*

**Router(config-crypto-map)#match address 100**

*When to use this IPSec VPN. We link it to the access-list “100” that we created in the first step. The router will use IPSec when it sees traffic coming from the first subnet in that access-list going to the second subnet. All other traffic will be normal (unencrypted).*

Router(config)#int g0/1

Router(config-if)#crypto map ipsec-map

*Tell the router to watch for traffic that may need IPSec on interface g0/1.*

