NET-477 Spring 2024-2025

HW#2

Total 100 points

Due Wednesday, Feb 5th, 11:59 PM CST

**ERIC SOMOGYI**

Submit a file, named **<your last name>-<your first name>-HW2.zip** containing the followings:

Part #1 Complete the PKA HW exercise “Site-to-Site VPN in the zipped folder (80 points)

Include a **screenshot** of your PKA configuration below along with answers to the questions below in part#2, also Your PKA file should be submitted along with this document, your lab should have all the tasks completed as indicated in the work area also to get full credit your tests should be successfully verified prior submission.

**Note**: **You don’t need to configure any routing on any routers in this lab (if you do, points will be deducted). All routes are configured for you via static default routes. You only need to focus on completing all the required tasks to build, configure,** and test the IPsec Tunnel.

Part#2 (20 points)

**Answer the following questions:**

1. Which action do IPsec peers take during the IKE Phase 2 exchange? **(5 points)**
2. If you are using Firewalls at each end of the IPSec VPN tunnel what are the protocols that need to be allowed for the tunnel to be established? **(5 points)**
3. When is a security association (SA) created if an IPsec VPN tunnel is used to connect between two sites? **(5 points)**
4. Which term describes a situation where VPN traffic that is received by an interface is routed back out of that same interface? **(5 points)**

**Part#1: Include your screenshots here:**

**First I provided below, my entire command list I used to program the project. I have provided a brief synopsis of the order of the screenshots before the screenshots were pasted.**

**Router 0 - Chicago**

**#enable**

**#license boot module c1900 technology-package securityk9**

**#y**

**#reload**

**#enable**

**#conf t**

**#access-list 110 permit ip 192.168.11.0 0.0.0.255 10.10.10.0 0.0.0.255**

**#access-list 120 permit esp any any**

**#access-list 120 permit udp any any eq isakmp**

**#exit**

**#show access-lists**

**#conf t**

**#int s0/1/1**

**#ip access-group 120 in**

**#end**

**#**

**#crypto isakmp policy 20**

**#authentication pre-share**

**#encryption aes**

**#group 5**

**#hash md5**

**#lifetime 86400**

**#exit**

**#crypto isakmp enable**

**#show crypto isakmp policy**

**#**

**#conf t**

**#crypto ipsec transform-set CompanyABCD esp-aes esp-md5-hmac**

**#exit**

**#show crypto ipsec transform-set**

**#conf t**

**#access-list 110 permit**

**#crypto map ERICMAP 10 ipsec-isakmp**

**#match address 110**

**#set peer 63.100.202.229**

**#set pfs group1**

**#set transform-set CompanyABCD**

**#exit**

**# int s0/1/1**

**#crpyto map ERICMAP**

**#exit**

**#config t**

**#crypto isakmp key NET477 address 63.100.202.229**

**#exit**

**#show crypto map**

**#show crypto ipsec sa**

**#show crypto isakmp policy**

**#show crypto ipsec transform-set**

**#show crypto isakmp sa**

**#show ip int s0/1/1 (to show access group 120 on int)**

**Router 1 - Washington**

**#enable**

**#license boot module c1900 technology-package securityk9**

**#y**

**#reload**

**#enable**

**#conf t**

**#access-list 110 permit ip 10.10.10.0 0.0.0.255 192.168.11.0 0.0.0.255**

**#access-list 120 permit esp any any**

**#access-list 120 permit udp any any eq isakmp**

**#exit**

**#**

**#show access-lists**

**#conf t**

**#int s0/1/0**

**#ip access-group 120 in**

**#end**

**#**

**#crypto isakmp policy 20**

**#authentication pre-share**

**#encryption aes**

**#group 5**

**#hash md5**

**#lifetime 86400**

**#exit**

**#crypto isakmp enable**

**#show crypto isakmp policy**

**#conf t**

**#crypto ipsec transform-set CompanyABCD esp-aes esp-md5-hmac**

**#exit**

**#show crypto ipsec transform-set**

**#conf t**

**#access-list 110 permit**

**#crypto map ERICMAP 10 ipsec-isakmp**

**#match address 110**

**#set peer 63.100.202.225**

**#set pfs group1**

**#set transform-set CompanyABCD**

**#exit**

**#int s0/1/0**

**#crypto map ERICMAP**

**#exit**

**#config t**

**#crypto isakmp key NET477 address 63.100.202.225**

**#exit**

**#show crypto map**

**#show crypto ipsec sa**

**#show crypto isakmp policy**

**#show crypto ipsec transform-set**

**#show crypto isakmp sa**

**#show ip int s0/1/0 (to show access group 120 on int)**

Installing sec license on both router’s confirmation of command and success:

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Crypto map configuration

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

After figuring everything out and getting everything working with the commands I provided,

below is the confirmation of the configurations followed by screenshots of the successful pings.

The first **4** screenshots are of the Router 0 Chicago of showing the results from the following

commands and the next **3** screenshots are of the Router 1 Washington router results. **In the**

**screenshots with my #show crypto isakmp sa command, I have circled the VPN tunnel**

**being IDLE active so it is easier for you to find.** The next **7** screenshots were of the VPN

tunnel confirmation messages that started randomly after I pinged, and it automatically started to

configure after using my command list. The last **2** screenshots are showing successful pings from

each of the devices on each subnet from Chicago to Washington and vice versa.

#show crypto map

#show crypto ipsec sa

#show crypto isakmp policy

#show crypto ipsec transform-set

#show crypto isakmp sa

#show ip int s0/1/1 (to show access group 120 on int)

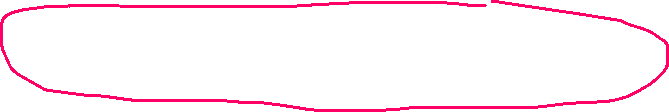
A screenshot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

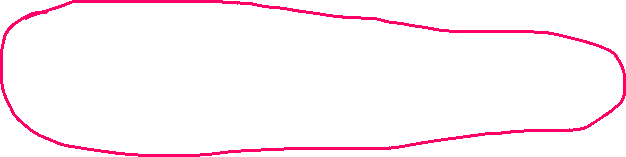


A screenshot of a computer program

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

VPN screenshot 1 starting

**A screenshot of a computer program

Description automatically generatedA screenshot of a computer program

Description automatically generated**

**Part#2: Include your answers here make sure you refer to the question’s number:**

1. The peer routers I used for each end router in the tunnel negotiated and established the security associations which encrypted and authenticated the traffic. As show in my 7 vpn tunnel screenshots, in my 1st screenshot which I have also attached again below for reference, after the line IKE\_P1\_complete, we can see Phase 2 starting on the next line where the Washington router peer is sending back a received packet in the lin “received packet from 63.100.202.229 dport 500 sport 500 Global (I) QM\_IDLE and it starts to process the IPSEC security association requirements and these keys are dynamically generated during the negotiation process which are shows in the other VPN screenshots I attached in part 1. In the 2nd screenshot is where the peer of Router 0 Chicago which is 63.100.202.229, there are several confirmations labeled 1041 which is part of the contents in Message ID 69859174 where there are packets being confirmed from a message the peer sent back to the source router through port 500 that it is communicating with. As seen in my VPN screenshots from part 1, in screenshots 4 through 7, the peer router has send back the results from the transform set that it agreed on. Also, during the Phase 2 exchange, the session keys are randomly generated based on the transform set encryption/integrity algorithm rules I set, which were esp-aes and esp-MD5-hmac for the hashing. Another thing important to note, is the peer and the local IP both have proxy ID’s, and as long as these proxy IDs match during the negotiation phase 2.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Depending on if it’s a NGFW that can perform VPN/IPSec services, so I would be able to program the IPSec VPN tunnel in the actual firewall on each endpoint. But for the purpose of this assignment, what I did was I had to permit the UDP protocol which is used for the internet key exchange negotiations where it exchanges the NET477 key. In the simplest way possible, you would need to permit UDP port 500, which I did on my routers with my UDP permit rule. You would also need to permit ESP protocol on the firewall which I also did in my permit esp rule. If you are using AH protocol, you would need to permit that as well. You would need to set ingress and egress rules for each direction to allow or deny traffic depending on the requirements. To summarize, depending on the setup and requirements, you would want to permit/deny tcp/ip traffic for the from designated source ranges to be accepted and then allow esp/udp traffic from the necessary ports for the tunnels to be established.
2. The SA is initiated and negotiated in the beginning of Phase 2 for IPsec. However, the SAs are created ***after*** the tunnel is created in Phase 1 after negotiating the SA policy and thereafter after the transform-sets and key exchanges are confirmed during Phase 2. “IPsec SA lifetimes are negotiated during IKE phase 2” – quote from class PowerPoint.
3. “A VPN client sending IPsec-protected traffic to another VPN user by allowing that traffic in and out of the same interface. This is also called “hairpinning.” – Source (<https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/vpn/asa-94-vpn-config/vpn-params.pdf>) Pg 2.