Computer Networks Week 2 Progress Report

VPN Gateway Configuration

Submitted to: Dr. Arshad Farhad

BY

Abdullah Shahid BSCS-2021-07
Muhammad Arslan BSCS-2021-22

Namal University, Mianwali
January 6, 2024

Contents

List of Figures

1 Background:

Today, when network security is of utmost importance, the impulse to establish an effective remote access infrastructure becomes a key component in building up reliable digital communication. Understanding that secure communication channels are a critical necessity in modern network environments, our project has the primary focus on creating an extensive virtual private network (VPN) solution utilizing Cisco Packet Tracer. As we go deep into Internet Protocol Security (IPsec) and the role it plays in our VPN framework, the idea is to build a strong network that ensures valuable information stays secure from possible threats.

2 Abstract:

Talking about the second week of our project, which was set aside for working on a secure remote access infrastructure through Virtual Private Networks VPN with Cisco Packet Tracer at that time, we made some significant progress in understanding and implementing vital security measures, especially concentrating on Internet Protocol Security (IPsec).

3 Related Works:

Cisco IKEv2 for IPsec VPNs provides a brief overview and benefits of Internet Key Exchange version 2 (IKEv2) for IPsec VPN [1]. The setup of IKEv2 systems and authentication mechanisms in Cisco devices is discussed. Assuming that encryption algorithms such as AES should be utilized instead of DES and hashing functions like SHA while increasing the level of security.

Amazon Web Services (AWS) on IPsec gives a general picture of the IPsec protocols and how they ensure safety during network communication. Discusses IPsec usage scenarios from VPNs and elaborates on how IPsec is used by AWS to facilitate secure data transmission via the Internet [2].

4 Security Measures: Exploring IPsec and ISAKMP:

4.1 ISAKMP: A Crucial Component of IPsec

The security architecture of IPsec relies heavily on the Authentication Header (AH) and Encapsulating Security Payload (ESP). However, the key management aspect is addressed by the Internet Key Exchange (IKE) protocol, and specifically, the Phase 1 negotiation process known as the Authentication Header. ISAKMP (Internet Secuirty Association and Key Management Protocol) plays a pivotal role in establishing a secure communication channel by facilitating the exchange of cryptographic keys.

4.2 Understanding IPsec:

Since obtaining a major security framework is what has been desired all along, IPsec is a critical key in that operation. IPsec is a suite of protocols designed to protect Internet Protocol communications. But it includes authentication, encryption, and key management to ensure that the data is transmitted with confidentiality, accuracy, integrity, and authenticity.

4.2.1 What is IPsec?

A way is IPsec (Internet Protocol Security), a suit made of some protocols that are used in securing communications over the internet based on what we normally refer to as the core type, which means basically standardized by internet protocol, or more commonly, the abbreviation 'IP'. It covers network layers and delivers a secure environment using IP networks to exchange private data.

4.2.2 IPsec Encryption:

The process of IPsec is an abstract procedure, as a program executes on encrypting the data so that it scrambles to keep its sense secret from non-authorized parties. The data can be encrypted by an array of encryption keys, and to decrypt the information, there should be some kind of decryption key.

IPsec relies on both asymmetric and symmetrical encryption to pick up speed as well as gain security during information transfer. Asymmetric encryption is a case where the key used in decryption is public while keeping matters private. Symmetric encryption uses one common public key on both sides for data protection and unprotected. IPsec set up a protected link using asymmetric encryption and then changed it to a symmetric one so that the data transfer could be quicker.

4.2.3 IPsec Protocols:

Authentication Header (AH): AH assists in authenticating and verifying the integrity of IP packets that ensure the data has not been altered within Transmission.
Encapsulating Security Payload (ESP): On the other hand, ESP underlines confidentiality by encrypting IP packets' expenditures.

4.2.4 How IPsec Works?

The process of information exchange with computers was made through these steps, as follows:

1. The sender computer verifies its security policy to check whether it needs to protect data transmission. If it does, the computer initiates a secure IPSec transmission to another recipient's computer that is forwarded.

2. Both computers negotiate the specifications that must be met to establish a secure connection. This involves parties agreeing to and defining the encryption, authentication, or SA parameters.

3. The computer sends and receives encrypted data, checking that only from trusted sources will it have originated. It uses validity checks to ensure the content below is reliable.

4. An IPSec connection will be terminated by the computer when the transmission is complete or such a session ends.

5 Implementation in Cisco Packet Tracer:

5.1 Configuring ISAKMP policy to establish IKE Policy:

This step involves the setting of policies relating to Internet Key Exchange (IKE), a protocol used in establishing an encrypted communication channel. In creating the ISAKMP policies, you establish parameters defining aspects such as authentication means and encryption algorithms among other critical parts of the initial phase of IKE negotiation. To securely establish VPN connections, a correctly defined ISAKMP policy is needed. ISAKMP policy configuration on Router0 is shown in Figure 1.

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp enable
Router(config)#crypto isakmp policy 20
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 1
Router(config-isakmp)#lifetime 3600
Router(config-isakmp)#exit
Router(config)#crypto isakmp key arslan123 address 11.0.0.2
Router(config)#crypto isakmp key arslan123 address 13.0.0.2
```

Figure 1: Defining ISAKMP policy configuration using CLI.

5.2 Define IPsec transform set:

So you specify a transform set that identifies the encryption and authentication algorithms to be used when performing second-phase IKE negotiations. The Transform set agrees upon the security process

to be applied to data and provides both confidentiality and integrity. This is a vital step towards the inclusion of security measures depending on what is needed to be covered by the project and how much protection they want. Steps to define IPsec transform set using CLI on router is shown in Figure 2.

```
Router(config)#
Router(config)#
Router(config)#crypto ipsec transform-set myset esp-3des esp-md5-hmac
Router(config)#
```

Figure 2: Defining IPsec transform set using CLI.

5.3 Create Access List:

An access list is a collection of rules that should define under what conditions network traffic could be permitted or prohibited. On the VPN establishment, there must be an access list that indicates IP-secure traffic. These definitions will improve the security and efficiency of what traffic should be encrypted or leapfrogged so that the VPN tunnel covers it, everything can be specified. Creation of access list on CLI of router is shown in Figure 3.

```
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)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 8.8.8.0 0.0.0.255
Router(config)#
```

Figure 3: Defining Access List on CLI.

5.4 Create Crypto Map for IPsec:

Crypto Map, is a configuration that ties the identified transform list and access rule, among other parameters to an interface in particular. For this purpose, they include the configuration of a crypto map that would be attached to an ISAKMP policy previously provided besides transform sets and access list bound with some particular interface such as one related to use on the Internet. This crypto map is a security guide for setting up IPsec protection for the traffic agents. Creation of Crypto Map for IPsec on CLI of router is shown in Figure 4.

```
Router(config)#
Router(config)#crypto map mymap 20 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 11.0.0.2
Router(config-crypto-map)#set peer 13.0.0.2
Router(config-crypto-map)#set transform-set myset
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#exit
Router(config)#
```

Figure 4: Creating Crypto Map for IPsec on CLI.

5.5 Apply Crypto Map on ongoing Interface of Router:

This is to be able to make the crypto map and assign it always for a demarcation point interface where encrypted traffic flows through. So, there is some correlation between security policy configurations and real network traffic when the crypto map applies settings against the router's serial interface. Application of Crypto Map on ongoing interface of router is shown in Figure 5.

```
Router(config)#interface serial0/1/1
Router(config-if)#crypto map mymap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

Figure 5: Crypto Map application on ongoing interface of router.

5.6 Testing and Verification:

The final stage is strict testing to ensure a properly configured VPN setup. It should imply that VPN connections are configured correctly, and traffic is secured and decrypted where necessary hence finally good security will be done. This is a critical one as at this stage all potential problems are identified; security arrangement verification can be made and also ensure that everything falls into place in which it works smoothly yet securely like an efficient VPN infrastructure design.

5.6.1 Display Active IKE Security Associations:

Command:

`show crypto isakmp sa`

Cisco systems utilize the `show crypto isakmp sa` command to list current ISAKMP Internet Security Association and Key Management Protocol SAs. This command elaborates guidelines on the configuration of ISAKMP tunnels such as peer IP address, authentication mode, encryption, and hashing mechanism used in addition to the SA state. It helps to detect and trace ISAKMP negotiations between devices. The real-time overview of active IKE Security Associations, including peer addresses and encryption methods, is shown in Figure 6.

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
12.0.0.1        11.0.0.1        QM_IDLE           1035    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Figure 6: Real-time overview of active IKE Security Associations, including peer addresses and encryption methods.

5.6.2 View Configured IKE Policies:

Command:

`show crypto isakmp policy`

In displaying configured ISAKMP policies, Cisco devices employ the `show crypto isakmp policy` command. First, let's look at the ISAKMP policies since it is also crucial to understand if this device has been properly configured with security so that it could be able to communicate well with its neighbors. A snapshot of configured ISAKMP policies, summarizing encryption and authentication settings, is shown in Figure 7.

5.6.3 Show Configured Crypto Maps:

Command:

`show crypto map`

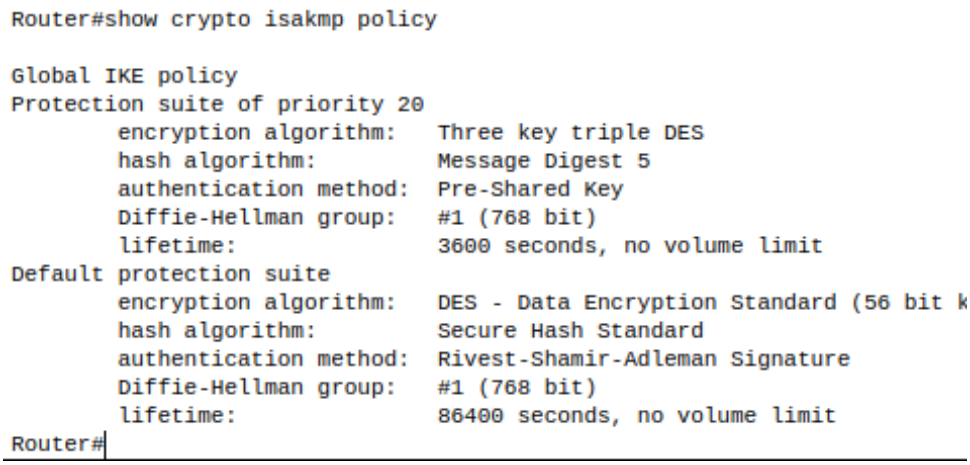

Figure 7: Snapshot of configured ISAKMP policies, summarizing encryption and authentication settings.

So, it is crucial to inspect configured crypto maps in Cisco devices using the `show crypto map` command. Crypto maps describe different attributes to be used in IPsec VPN connections such as ISAKMP policies which are tied with transform sets and access control lists. This command will enable network administrators to verify what crypto maps have been configured and the settings applied besides which interfaces they connect. A visual representation of configured crypto maps, detailing policies for IPsec Security Associations, is shown in Figure 8.

```
Router#show crypto isakmp policy

Global IKE policy
Protection suite of priority 20
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Router#show crypto map
Crypto Map mymap 20 ipsec-isakmp
        Peer = 12.0.0.1
        Extended IP access list 100
            access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
            access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
        Current peer: 12.0.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                myset,
        }
        Interfaces using crypto map mymap:
                Serial0/1/0

Router#
```

Figure 8: Visual representation of configured crypto maps, detailing policies for IPsec Security Associations.

5.6.4 Display Active IPsec Security Associations:

Command:

`show crypto ipsec sa`

The `show crypto ipsec sa` command helps know all the active IPsecre SAs of Cisco environments. This command shows the state of IPsec tunnels related aspects such as source and destination IP ad-

dresses, encryption and integrity algorithms used as well data through these connections. It is an invaluable assistant to control the status and efficacy of secured IPsec communication channels. A snapshot of active IPsec Security Associations, showing established tunnels and encryption details, is shown in Figure 9.

```
Router#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: mymap, local addr 11.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 12.0.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 0
   #pkts decaps: 12, #pkts decrypt: 12, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 11.0.0.1, remote crypto endpt.:12.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x81507F6D(2169536365)

     inbound esp sas:
      spi: 0x955F9D47(2506071367)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4525504/3384)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

 --More--
```

Figure 9: Snapshot of active IPsec Security Associations, showing established tunnels and encryption details.

6 Division of Tasks:

A division of responsibilities between us – a team consisting of two members has been set so that we could work more efficiently and cooperate properly. When you share, the roles and responsibilities among team members it enables most of them to develop focused efforts towards a singular goal. The roles assigned to each team member are as follows:

6.1 Team Member 1 (Abdullah Shahid)

1. Implementation of VPN Gateways: Ensure the correct setting up of VPN gateways connected to specific routers inside Cisco Packet Tracer.

2. Security Measures Deployment: IPsec to enhance VPN infrastructures within the organization.

3. Documentation: Being in charge of writing down the activities carried out from the process of installing, configurations, and any meaningful findings made while doing those tasks as well as coming up with a detailed How we'll use it report.

6.2 Team Member 2 (M. Arslan)

1. IPsec Exploration: an enormous job to understand Internet Protocol Security that is IPsec, its protocols, mechanisms encrypted, or operation flow.

2. Simulation Scenarios: Guide the creation and deployment of end-to-end simulations with multiple scenarios to provide meticulous testing for performance capacities and effectiveness in VPN infrastructure.

3. Challenges and Optimization: This handles the task of ensuring that your configurations are fine-tuned to deal with resource-intensive facets yet are balanced between security and performance.

7 Challenges Faced:

One serious issue faced during this phase was the implementation of security measures especially as regards IPsec since it often required high resources to operate. But to find a balance between these hard security measures and the smooth performance of software components, it does need thoughtful evaluation using optimization strategies. We are also still striving to make adjustments in our configurations to ensure that the increase in security does not come at a compromise on the efficiency of their remote access relationships. One of these challenges shows us how delicate a balance security and performance have to be in the ventures we have worked on right now.

8 Attachment: `(VPN-gateway-configuration-week2.pkt file)`

The additional file that is going to be attached with this report will contain more information and specifics along with an illustrative layout as mentioned above.The attached file, `VPN-gateway-configuration-week2.pkt file`, is a tool of practical guide and adds to the informational content that this document has managed so far.

9 Conclusion:

Seems like the second week is a moment of breakthrough in evolving our project. In addition, researching IPsec details not only enhances our theoretical understanding of this topic but also has a practical application in the case when working on a Cisco Packet Tracer environment. Successful mounting of VPN gateways and the establishment of strong security systems also become a very important factor in building up an effective portfolio for secure remote levels. We can move forward, with higher level simulations becoming possible along with more intricate considerations of secure communication protocols once this week's groundwork is laid.

References

[1] "Cisco ikev2 for ipsec vpns." Accessed: January 6, 2024.

[2] "Amazon web services (aws) on ipsec." Accessed: January 6, 2024.