**E/15/211**

**CO325-Computer and Network Security**

**Lab 03: Virtual Private Networks (IPSec)**

**Assignment**

**Part1**

**1. Brieﬂy explain the IPSec protocol and the services it provides.**

IPSec means Internet Protocol security, which uses cryptographic security services to protect communications over Internet Protocol (IP) networks. Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of [cryptographic security](https://www.simplilearn.com/why-you-should-not-use-smartphone-fingerprint-readers-article) services. IPSec is a suite of cryptography-based protection services and security protocols. Because it requires no changes to programs or protocols, you can easily deploy IPSec for existing networks.

IPsec protects one or more paths between a pair of hosts, a pair of security gateways, or a security gateway and a host. A security gateway is an intermediate device, such as a switch or firewall, that implements IPsec. Devices that use IPsec to protect a path between them are called peers.And also IPsec requires a PCI Accelerator Card (PAC) to provide hardware data compression and encryption. A PAC is a hardware processing unit the switch’s CPU controls.IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPsec provides the following security services for traffic at the IP layer:

* Data origin authentication—identifying who sent the data.
* Confidentiality (encryption)—ensuring that the data has not been read en route.
* Connectionless integrity—ensuring the data has not been changed en route.
* Replay protection—detecting packets received more than once to help protect against denial of service attacks.

**2. What is the use of step 3 and step 4 of the conﬁguring process?**

There are two aspects of configuration process, configuration of university firewall and configuration of branch firewall. It is static routing.The format of the static route command is:

**# route [interface name] [destination address] [netmask] [gateway]**

First configure a default static route towards the default gateway.Then configure an internal static route to the particular network. Step3 is used to add a static route to the outside interface to direct traﬃc to the branch network as well as to the university network. And step4 is used to add a static route to the inside interface to route University traﬃc to the main router.

Branch firewall→  **# route outside <branch network# <mask# <branch firewall IP# 1**

Branch Firewall→  **# route inside <branch network# <mask# <core router IP# 1**

Static routing is used to define an exit point from a router when no other routes are available or necessary. This is called a default route. Static routing can be used for small networks that require only one or two routes.

The firewall connects to the internet on the outside. Here always internet is the outside for both university and branch networks. And those both networks are directly connected to the Inside interface of the firewall. So we need to configure a **static route** to tell the firewall that networks can be reached via134.95.56.20/28 router. And if routing is not done, can’t communicate between private networks and the internet.

**3. What is the use of step 5 of the conﬁguring process?**

Step5 is used to create an access list to capture the traﬃc to the branch network as well as university network. First create an ACL and then apply the ACL to an interface.

**# access -list branch -traffic extended permit tcp object**

**# campus\_network object branch\_network**

This configurations for commonly used IP Access Control Lists (ACLs), which filter IP packets based on source address, destination address, type of packet, any combination of these items. In order to filter network traffic, ACLs control whether routed packets are forwarded or blocked at the router interface. The router examines each packet in order to determine whether to forward or drop the packet based on the criteria that we specify within the ACL.The IP ACL is a sequential collection of permit and deny conditions that apply to an IP packet. The router tests packets against the conditions in the ACL one at a time. If no conditions match, the router rejects the packet because of an implicit deny all clause.

There are two types of ACLs. **Standard ACLs** compare the source address of the IP packets to the addresses configured in the ACL in order to control traffic. **Extended ACLs** compare the source and destination addresses of the IP packets to the addresses configured in the ACL in order to control traffic.

**4. What will happen if you skipped step 6 and 7 and why?**

Step6 is used to create an access list to capture traﬃc from the private network to the private network and step7 is used to apply private-traﬃc access group to the inside interface.

**#access -list private -traffic extended permit ip object**

**# private\_network object private\_network**

**#access -group private -traffic out interface inside**

From step6 it creates an ACL to capture traffic from 10.40.0.0/18 network to anywhere in 10.40.0.0/18 through the firewall . After doing step7, it defines networks as inside interface. When considering university network , an ip packet is send and it can broadcast to branch network through the firewall.

But if we skip these step 6 and 7, we couldn’t able to communicate between university network and the branch network because data packets will be dropped in the firewall.

**5.Brieﬂy explain what is ISAKMP and why we need ISAKMP in this process.**

ISAKMP means Internet Security Association and Key Management Protocol. It defines procedures and packet formats to establish, negotiate, modify and delete Security Associations. SAs contain all the information required for execution of various network security services, such as the IP layer services (such as header authentication and payload encapsulation), transport or application layer services, or self-protection of negotiation traffic. ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.

It is distinct from key exchange protocols in order to cleanly separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. However, a common framework is required for agreeing to the format of SA attributes, and for negotiating, modifying, and deleting SAs. ISAKMP serves as this common framework. It can be implemented over any transport protocol.

**why we need ISAKMP in this process:-**

It includes mechanisms that mitigate certain threats – e.g., Denial Of Service (DOS) and anti-replay protection. In ISAKMP, SA and key management are separate from any key exchange protocols; so, in a sense ISAKMP is an "abstract" protocol which provides a framework for authentication and key management and supports many actual key exchange protocols (e.g., IKE). ISAKMP defines header and payload formats, but needs an instantiation to a specific set of protocols. Such an instantiation is denoted as the ISAKMP Domain Of Interpretation (DOI): an example of this for the IPsec/IKE is the IPsec DOI.

**6. What is a transform set?**

A transform set is a combination of individual IPSec transforms designed to enact a specific security policy. for traffic. During the ISAKMP IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow**.** A transform set is a combination of an AH transform, an ESP transform, the IPSec mode (either tunnel or transport mode) IPSec factors.

**7.What is a Crypto map? Explain the minimum requirement for compatibility of two crypto maps.**

A crypto map is a software configuration entity that performs two primary functions, static crypto maps and dynamic crypto maps. In a crypto map you define who (peer address), what traffic (ACL) and how (transform set). The concept of a crypto map was introduced in classic crypto but was expanded for IPSec.

**The minimum requirement for compatibility of two crypto maps:-**

There are two types of crypto maps, Dynamic crypto maps and Static crypto maps.

Dynamic crypto maps:-

* Allow a gateway to accept connections from peers even if not all parameters are known in advance.
* Does not require the configuration of the set peer command,

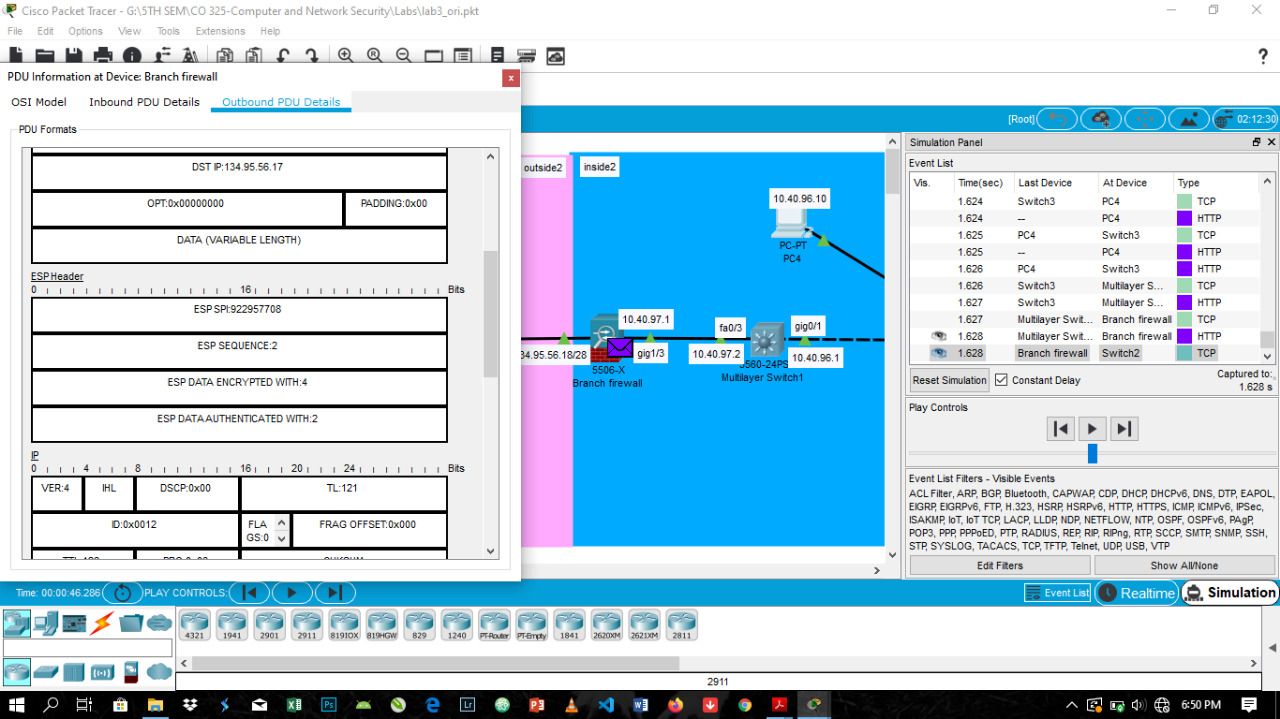
Static crypto maps:- It identifies peer and traffic to be encrypted explicitly.

**8. Send HTTP request from a branch PC to University server with and without VPN. Capture the packets going through the internet and Identify the diﬀerence of the packet structure between two scenarios. If you need you can use diagrams to explain.**

**Send HTTP request from a branch PC to University server with VPN:-**

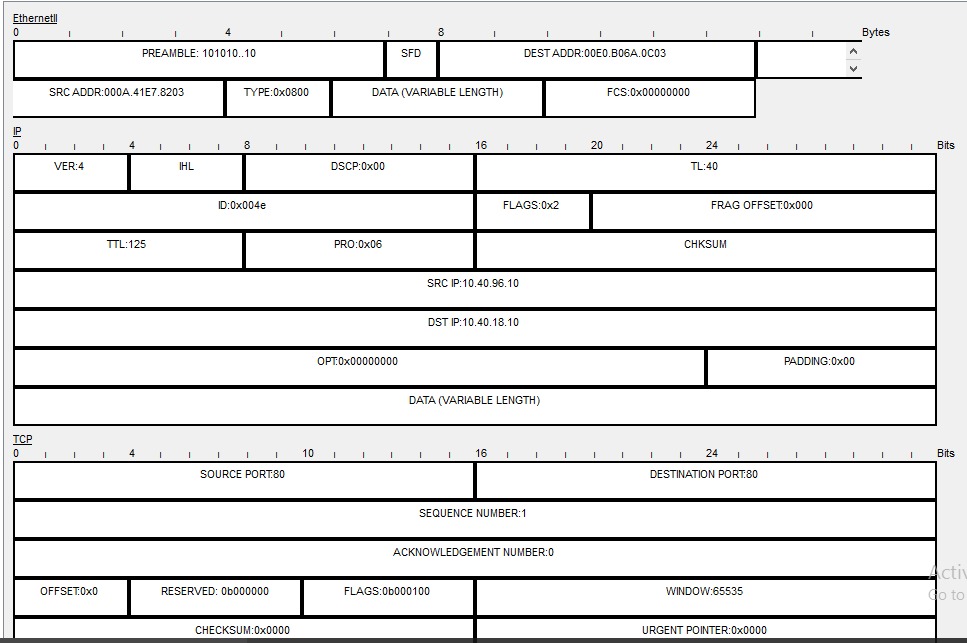
Here branch network is act as the inside and internet is as the outside. Here, when HTTP request is sent, it goes directly from branch firewall to university firewall. So when HTTP request comes from branch PC to University server, HTTP packet should come through the branch firewall. Therefore, when HTTP packet go from inside to outside, that means from branch network interface to firewall , HTTP packet is encrypted and comes out to the internet an encrypted HTTP packet. Here , a segment header, which is known as “ESP Header” is added to the packet. In this figure you can see the ESP header.

When encrypted packet goes from internet to university network through the university firewall, that encrypted HTTP packet is decrypted and header will remove.



**Send HTTP request from a branch PC to University server without VPN:-**

Here branch network is act as the inside and internet is as the outside. Here, when HTTP request is sent, it goes through the router. That is the different in communication with and without VPN.And , as there is no VPN when HTTP request go through the firewall, ESP header is not added. You can see from following figure the outbound PDU of HTTP packet without VPN.



**9. What do you need to change in this example if you only need your UDP packets to be protected on the internet?**

To change the configurations to get UDP packets to be protected on the internet we should change following command

**#access -list university -traffic extended permit tcp object**

As in that command, the word “tcp” is changed into “udp” like below.

**#access -list university -traffic extended permit udp object**

Then we can get UDP packets to be protected on the internet.

**10. Give a summary of the vulnerabilities of technologies you used here that can be used to expose your data and what can you do to improve your system’s security.**

Even though there is available stronger authentication methods like Main Mode with certificates, here in conﬁguring the Internet Security Association Management Protocol (ISAKMP) policies we have used IKE Initiate Aggressive Mode with pre-shared keys. (This feature is best implemented in a crypto hub-and-spoke scenario, by which the spokes initiate IKE aggressive mode negotiation with the hub by using the preshared keys.) In IPSec, it uses IKE protocol (Internet Key Exchange protocol) to ensure the secure connection.

**Issues that we faced in using IKE protocol pre-shared key authentication:-**

**Man in the middle attack**:- In this attack targets IKE’s handshake implementation used for IPsec-based VPN connections.r. In this vulnerability, an attacker may be able to recover a weak Pre-Shared Key as in IPSec VPN uses keys to identify each other in communication. This is Man in the middle attack and this causes for leakage of VPN session data.

**Buffer flow:-**This happens due to a buffer overflow in the affected code area, as a result of programs that may forget buffer location and overwrites adjacent memory locations.

**Password cracking:-** This happens with both IKEv1 and IKEv2 . And here we have used only IKEv1. When a VPN user enters a password, server first encrypts it and compare with stored values. If they match, the person gets access. Therefore, if we use weak passwords in IPSec VPN makes it is caused to offline dictionary or brute force attacks.

**How to improve system security by overcome those issues:-**

**To overcome man in the middle attack**:-We all can ensure that the patch is correctly applied because software providers itself will release a patch for the vulnerability when it happens.

**To overcome buffer flow:-** To overcome this we can check whether features like crypto map, IKEv1 (or IKEv2 .) are configured on the device. Based on the output of the command, we always ensure that IKEv1 (or IKEv2) is disabled on the particular system.

**To overcome password cracking:-** Wecan choose extremely complex passwords when they use IPsec through password based logins. Additionally, we can make sure that VPN uses cryptographically secure key values that can resist brute force or dictionary attacks.

**Part2**

**1. Explain the diﬀerences between Clientless SSL VPN and Lan-to-Lan IPSec VPN.**

Main difference between Clientless SSL VPN and Lan-to-Lan IPSec VPN**.**

|  |  |  |
| --- | --- | --- |
| **Specification** | **Clientless SSL VPN** | **Lan-to-Lan IPSec VPN** |
| Network Layers | Operates at layer3 | Operates at layers 4-7 |
| Connectivity | Connects remote hosts to entire networks | Connect users to specific apps and services |
| Applications | Can support all IP-based applications | Best for email,file sharing and browser based apps |
| Gateway Location | Gateway usually implemented on the firewall | Gateway typically deployed  behind the firewall |
| Security/Control | Broad access creates security concerns | More granular controls require more management |
| Endpoints | Required host-based clients | Browser-based with optional thin client |

Some of the other differences between IPsec and SSL VPNs include the following:

* **Performance:** With modern hardware, the type of encryption used by IPsec and SSL VPNs does not usually cause performance issues, but organizations should use benchmarks to test VPN candidates. IPsec VPNs configure a tunnel between client and server using a piece of software on the client, which may require a relatively lengthy setup process; SSL VPNs that operate through web browsers will usually be capable of setting up connections much faster.
* **Security:** One type of VPN is not necessarily more secure in all circumstances. The most important factor in determining which type of VPN will be more secure is the threat model the organization is basing its VPN requirements on. Each VPN type should be evaluated in the context of the type of attacks the organization is defending against. Security of the encryption algorithms being used is important but so is the security of the other components of the implementation.
* **Data authentication:** VPNs can encrypt all transmitted data, but they can also add data authentication to defend against tampering by using [strong cryptographic authentication algorithms](https://searchsecurity.techtarget.com/video/Say-hello-to-the-future-of-authentication-bye-to-passwords) to verify that data has not been modified in transit between VPN clients and servers. However, they do require a secure key exchange mechanism to enable authentication. While the SSL/TLS protocol incorporates negotiation of key exchange algorithms, IPsec relies on an external protocol, Internet Key Exchange, for this purpose.
* **Attack defense:** The key difference between IPsec and SSL VPNs lies in the difference in endpoints for each protocol. An IPsec VPN typically enables remote access to an entire network and all the devices and services offered on that network. If attackers gain access to the secured tunnel, they may be able to access anything on the private network. SSL enables connections among a device, specific systems and applications so the attack surface is more limited.
* **Client security:** Although the IPsec protocol is a part of the TCP/IP suite, it is not always implemented as a default component of OSes that support TCP/IP. In contrast, SSL VPNs rely on TLS, which is incorporated by default in web browsers, as well as many other application layer protocols. As a result, comparing IPsec and SSL VPNs should include consideration of how clients connect to and use the VPN, as well as how secure those options are. Implementers should consider how clients connect to the VPN, the attack surface of VPN-enabled clients and the VPN user profiles.
* **VPN gateway:** An SSL VPN gateway is likely to enable far more granular configuration options as far as limiting access to specific systems or services on the protected network. Gateways for IPsec VPN products are likely to have far less configurability. While they may have added packet filtering features that enable policies or configurations to limit access to specific IP addresses or subsets of the protected network, care should be taken to avoid adding unnecessary complexity and extra security risks that come with software add-ons. In either case, consider deploying a VPN alongside a [network access control system](https://searchsecurity.techtarget.com/feature/Three-reasons-to-deploy-network-access-control-products) that can enhance overall security by restricting access to network resources based on explicitly defined policies.
* **End-to-end networking:** TLS is used at the transport layer, meaning the network layer where communication is conducted between processes. In contrast, IPsec operates at the network layer where communication is conducted between network nodes with IP addresses. This makes securing end-to-end encryption more difficult when either end of the secured VPN circuit is on a network that uses Network Address Translation ([NAT](https://searchnetworking.techtarget.com/definition/Network-Address-Translation-NAT)) to virtualize IP addresses.