Lab 03: Virtual Private Networks (IPSec)

Assignment

Part 1

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

IPsec, stands for the Internet Protocol Security or IP Security protocol, defines the architecture for security services for IP network traffic. IPsec describes the framework for providing security at the IP layer, as well as the suite of protocols designed to provide that security, through authentication and encryption of IP network packets. Also included in IPsec are protocols that define the cryptographic algorithms used to encrypt, decrypt and authenticate packets, as well as the protocols needed for secure key exchange and key management.

Services

- Encapsulating Security Payload (ESP) protocol: This defined a method for encrypting data in IP packets
- Authentication Header (AH): This authenticates the sender by digitally signing IP packets and it discovers any changes in data during transmission.

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

In step 3 the command add a static route to the interface direct traffic to branch network. Because of this route the university network devices can directly access the branch network through public network layer2 switch.

In step 4 the command add a static route to the inside interface to route University traffic to the the main router. Because of this route incoming traffic to the network directly forward to layer 3 switch. Then going traffic to the particular device is handled by layer 3 switch

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

In this access-list it permits only TCP traffic (HTTP, HTTPS, SMTP, SSH, Telnet etc) to go from branch network object to university network object. All the other types of traffics are restricted.

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

In step 6 the ACL rule permit ip traffic to go from university private network to branch private network. And in the step 7 it is added to the inside interface. If we skipped these two steps the ip traffic does not go between university and branch network and they will drop at inside interfaces of firewalls.

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

ISAKMP 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.

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. Transform sets combine the following IPSec factors:

• Mechanism for payload authentication—AH transform

• Mechanism for payload encryption—ESP transform

• IPSec mode (transport versus tunnel)

A transform set is a combination of an AH transform, plus an ESP transform, plus the IPSec mode (either tunnel or transport mode).

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:

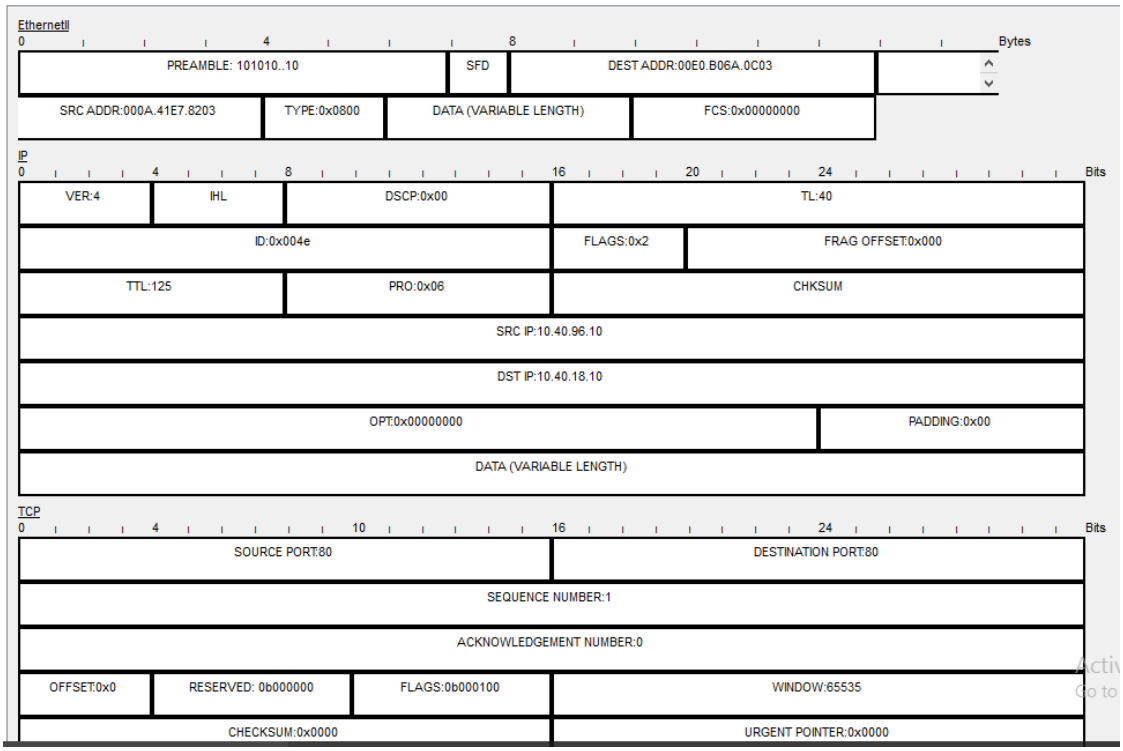
- Selects data flows that need security processing.
- Defines the policy for these flows and the crypto peer to which that traffic needs to go.

A crypto map is applied to an interface.

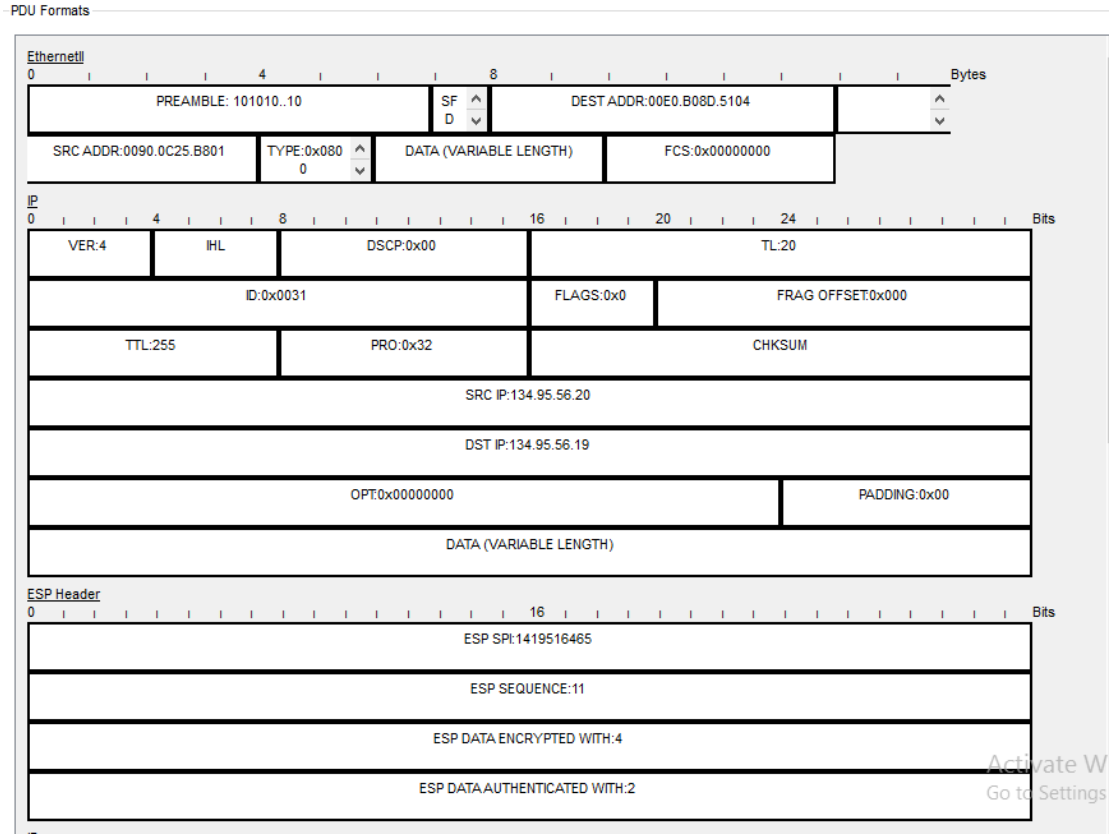
8. Send HTTP request from a branch PC to University server with and without VPN. Capture the packets going through the internet and Identify the difference of the packet structure between two scenarios. If you need you can use diagrams to explain.

When without VPN, the packets are not encrypted. Then in the packet structure there is no ESP header part. But with VPN packets are encrypted and we can see a ESP header in the packet structure other than normal HTTP headers.

Without VPN packet structure,



With VPN packet structure,



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

We can change clientless SSL VPN instead of LAN-to-LAN IPsec VPN. Clientless SSL VPN enables end users to securely access resources on the corporate network from anywhere using an SSL-enabled Web browser. The user first authenticates with Clientless SSL VPN gateway, which then allows the user to access pre-configured network resources. Then all going out UDP packets will be secured. And also when sending data out of the system we can use HTTPS instead of HTTP. Then we have SSL protection.

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.

The world an the Internet will continue to turn. This issue is however very important to us if we are using an IPSEC VPN. At this point, all points to this being a DOS only vulnerability. Our IPSEC concentrator may reboot or lock up. While this is not as severe as remote code execution, it can still break a business if critical network links are impacted.

A vulnerability in the Internet Key Exchange (IKE) version 1 (v1) code of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause an affected system to reload. The vulnerability is due to improper handling of Internet Security Association and Key Management Protocol (ISAKMP) packets. An attacker could exploit this vulnerability by sending crafted UDP packets to the affected system. A successful exploit could allow the attacker to cause an affected system to reload. Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability affects systems configured in routed firewall mode only and in single or multiple context mode. This vulnerability can be triggered by IPv4 and IPv6 traffic.

Also The vulnerabilities of ISAKMP discovered by researchers at the University of Oulu in Finland can cause a denial of service, format string problems and buffer overflows. In some instances, it also can be used by an attacker to execute code.

There are several methods we can follow to improve security of the vpn.

1. Enabling a network lock

Enabling your network lock is quick and easy way to help ensure your connection is secure in case our connection gets interrupted.

In the event of VPN interference, the network lock will automatically prevent our device from accessing the internet. That means our information is able to remain protected while your VPN reconfigures itself. By keeping your network – whether it be your mobile or desktop – under lock and key, we won't have to worry about your IP being exposed. It's a useful feature to have.

2. Preventing DNS leak

When we're connected to the VPN you should automatically be using the secure DNS server provided by the VPN service. Except sometimes we don't; sometimes your computer might use its regular DNS connection, bypassing the VPN. That's called a DNS leak, and it could be monitored by outside forces.

Some VPN clients have DNS leak protection built in, but if yours doesn't you can run a test here. The location it tells you should be your 'apparent' VPN location, not your actual one. If it fails, then there are suggestions on the site that provide a fix.

Using SSL VPN to create secure sessions from a PC browser to one of your application servers, enabling your suppliers, other business partners, and customers to use specific applications on your network. SSL VPNs do not need client software; the sessions use HTTPS.
A router can safeguard our network against web threats by connecting to a cloud-based security service. Unlike local software, software intelligence in the cloud is continuously updated and tuned by the service provider.

Part 2

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

Clientless SSL VPN enables end users to securely access resources on the corporate network from anywhere using an SSL-enabled Web browser. The user first authenticates with a Clientless SSL VPN gateway, which then allows the user to access pre-configured network resources.
Clientless SSL VPN creates a secure, remote-access VPN tunnel to an ASA using a Web browser without requiring a software or hardware client. It provides secure and easy access to a broad range of Web resources and both web-enabled and legacy applications from almost any device that can connect to the Internet via HTTP.

Clientless SSL VPN uses Secure Sockets Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide the secure connection between remote users and specific, supported internal resources that you configure at an internal server. The ASA recognizes connections that must be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.
The network administrator provides access to resources by users of Clientless SSL VPN sessions on a group basis. Users have no direct access to resources on the internal network.

A VPN connection that allows you to connect two Local Area Networks (LANs) is called a Lan-to-Lan IPsec VPN. We can configure route-based VPNs to connect the firewalls located at two sites or to connect the firewall with a third-party security device at another location. The firewall can also interoperate with third-party policy-based VPN devices; the firewall supports route-based VPN.

The firewall sets up a route-based VPN, where the firewall makes a routing decision based on the destination IP address. If traffic is routed to a specific destination through a VPN tunnel, then it is handled as VPN traffic.

The IP Security (IPSec) set of protocols is used to set up a secure tunnel for the VPN traffic, and the information in the TCP/IP packet is secured (and encrypted if the tunnel type is ESP). The IP packet

(header and payload) is embedded in another IP payload, and a new header is applied and then sent through the IPSec tunnel. The source IP address in the new header is that of the local VPN peer and the destination IP address is that of the VPN peer on the far end of the tunnel. When the packet reaches the remote VPN peer (the firewall at the far end of the tunnel), the outer header is removed and the original packet is sent to its destination.

In order to set up the VPN tunnel, first the peers need to be authenticated. After successful authentication, the peers negotiate the encryption mechanism and algorithms to secure the communication. The Internet Key Exchange (IKE) process is used to authenticate the VPN peers, and IPSec Security Associations (SAs) are defined at each end of the tunnel to secure the VPN communication. IKE uses digital certificates or preshared keys, and the Diffie Hellman keys to set up the SAs for the IPSec tunnel.The SAs specify all of the parameters that are required for secure transmission— including the security parameter index (SPI), security protocol, cryptographic keys, and the destination IP address—encryption, data authentication, data integrity, and endpoint authentication.