Lab 03: Virtual Private Networks (IPSec)

Part 1

1. Briefly explains the IPSec protocol and the services it provides.

Internet Protocol Security (IPSec) is a secure network protocol suite that authenticates and encrypts the packets of data sent over an Internet Protocol network. It is used in virtual private networks (VPNs).

IPsec can protect data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. IPsec can automatically secure applications at the IP layer.

IPsec involves two security services:

- Authentication Header (AH): This authenticates the sender and it discovers any changes in data during transmission.
- Encapsulating Security Payload (ESP): This not only performs authentication for the sender but also encrypts the data being sent.

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

Although the Cisco ASA appliance does not act as a router in the network, it still has a routing table and it is essential to configure static or dynamic routing in order for the appliance to know where to send packets.

After the packet passes all firewall controls, the security appliance needs to send the packet to its destination address. It therefore checks its routing table to determine the outgoing interface where the packet will be sent.

By the given 3 and 4 steps it configures the path that the packets will be sent through the inside or outside interfaces of the firewall.

Here static routing is used and it is better than dynamic routing in this purpose. The reason is that one of the purposes of a firewall is to hide our internal trusted network addressing and topology. By configuring dynamic routing support, we might be advertising routes to untrusted networks thus exposing our network to threats.

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

This ACL rule will allow only the tcp traffic, that come from the branch network to the university network or the other way round.

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

When these 2 steps are skipped the tcp packets sent from university to branch are allowed to go through the university firewall but it is not allowed to go through the branch firewall (same goes from branch to university), because it is applied on the inside interface of the firewalls.

These 2 steps are essential to allow the ip address' from 10.40.0.0 subnet, through the inside interface of the ASA. Then only the university or branch traffic can enter to the required network through the firewall.

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

Internet Security Association and Key Management Protocol is a protocol for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent; protocols such as Internet Key Exchange and Kerberized Internet Negotiation of Keys provide authenticated keying material for use with ISAKMP.

Internet Security Association and Key Management Protocol (ISAKMP) is used for negotiating, establishing, modification and deletion of SAs and related parameters. It defines the procedures and packet formats for peer authentication creation and management of SAs and techniques for key generation.

ISAKMP operates in two phases. During phase 1, peers establish an ISAKMP SA – namely, they authenticate and agree on the used mechanisms to secure further communications. In phase 2 this ISAKMP SA is used to negotiate further protocol SAs (e.g., an IPsec/ESP SA).

6. What is a transform set?

Transform sets is a set of protocols and algorithms specified on a gateway to secure data. The three factors that make up a proposal or transform set are data encryption, data authentication and the encapsulation mode. A proposal/transform set is like a profile with a specific combination of protocols and algorithms that an end user may choose to use for their VPN\IPSec security parameters.

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.

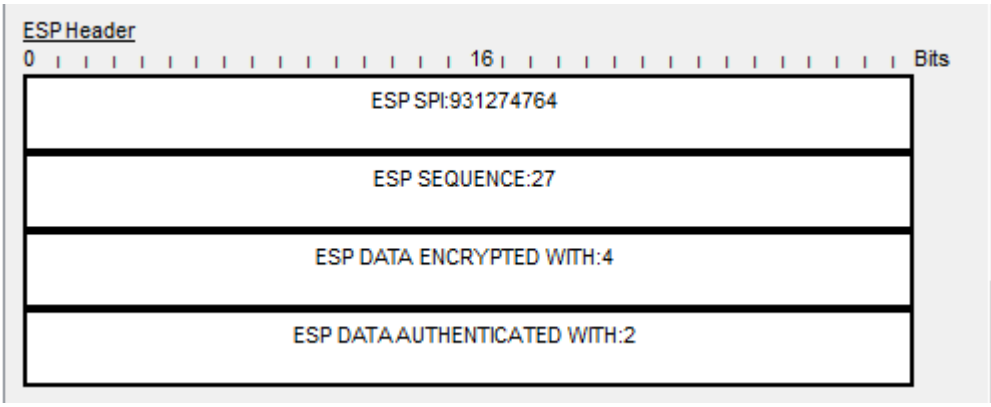
A crypto map is applied to an interface.

Minimum requirements for a crypto map,

- Match address (data flow that need security processing)
- Setting up the peer IP address of the interface that it is going to be use
- Transform set

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.

With VPN, packet is encrypted with ESP at the ASA. So it gets an ESP header like in the below.



But this header will not be added to the packet when it is not having VPN.

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

We need to change the ACL rule (step 5) in the ASA which allows only tcp traffic to allow only udp traffic through the ASA.

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.

1. Man in the middle attack

IPSec VPN uses keys to identify each other. In this vulnerability, an attacker may be able to recover a weak *Pre-Shared Key*. Thus, this attack targets IKE's handshake implementation used for IPsec-based VPN connections. Using these keys, it can decrypt connections.

Ultimately, this will open the door to *Man-in-the-middle (MitM)* attacks. Eventually, this will result in leakage of VPN session data.

When any vulnerability happens due to a flaw in implementation, usually software providers itself will release a patch. For example, when this was reported in Cisco routers using IKEv1, they immediately released the patch for the vulnerability. To mitigate this attack, all we did was to ensure that the patch is correctly applied.

2. Password cracking

Similarly, another problem with IPSec happens with password cracking. Unfortunately, this happens with both IKEv1 and IKEv2 versions. When a VPN user enters a password, server first encrypts it and compare with stored values. If they match, the person gets access.
Unfortunately, using weak passwords in IPSec VPN makes it vulnerable to offline dictionary or brute force attacks.

Recommend customers to choose extremely complex passwords when they use IPsec through password-based logins. Additionally, we make sure that VPN uses cryptographically secure key values that can resist brute force or dictionary attacks.

3. Buffer overflow

Buffer is nothing but a temporary storage space. At times, a program may forget buffer location and overwrites adjacent memory locations. This vulnerability happens due to a buffer overflow in the affected code area.

Here, attacker would first send UDP packets to the affected system. As a result, it allows attacker to execute arbitrary code and obtain full control of the system.

Again, this is a flaw in the implementation. For example, when this vulnerability was reported in *Cisco ASA Software*, they immediately came up with security fixes.
Here, the method of fix involved couple of steps. First 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 affected system.

Improve the systems' security

- Add higher Diffie-Hellman key group (for example group 5)
- By using IKEv2 configurations you can use more secured sha groups (for example sha-2)

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. SSL is already supported by the remote user's browser, so it needs no extra software and is simpler to configure. This simplicity, however, comes at the cost of being more vulnerable to security threats.

Lan-to-Lan IPSec IPSec VPN connects networks in different geographic locations (such as distant office networks). But IPsec requires third-party client software, it is more complicated and expensive to set up and maintain.