E/15/220

Malihtha K.H.H.

CO325 - Lab 03 – Assignment

3.1) Part 1

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

In computing, 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 includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. 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*).[1] 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.

The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) and Secure Shell (SSH), both of which operate at the Transport layer. IPsec can automatically secure applications at the IP layer.

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

In university firewall,

Step 3 define static route which send inside(university network) traffic going to branch network to branch firewall outside interface.

Step 4 define static route that send branch network traffic coming to inside(university network) to university core router.

In branch firewall,

Step 3 define static route which send inside(branch network) traffic going to university network to university firewall outside interface.

Step 4 define static route that send university network traffic coming to inside (university network) to branch core router.

So step 3 and step 4 configurations handle university network and branch network traffic coming to firewall by forwarding to next hop address.

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

Define access rule that only permit tcp traffic between university network and branch network.

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

If we skip step 6 and 7 , the outside traffic coming into firewall will not go to inside because the firewall does not allow any traffic from a lower security interface to a higher security interface unless it is explicitly permitted by an extended access list. So in step 6 and 7 we permit any traffic coming from private network to private network. Here we add whole private network because if we add another branch it will be easy because we didn't want to add another rule to permit that traffic.

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

ISAKMP (Internet Security Association and Key Management Protocol) and IPSec are essential to building and encrypting the VPN tunnel. ISAKMP, also called IKE (Internet Key Exchange), is the negotiation protocol that allows two hosts to agree on how to build an IPsec security association. ISAKMP negotiation consists of two phases: Phase 1 and Phase 2.

Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data. IPSec then comes into play to encrypt the data using encryption algorithms and provides authentication, encryption and anti-replay services.

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 that occurs in IKE phase 2 quick mode, 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)

Transform sets equal 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:

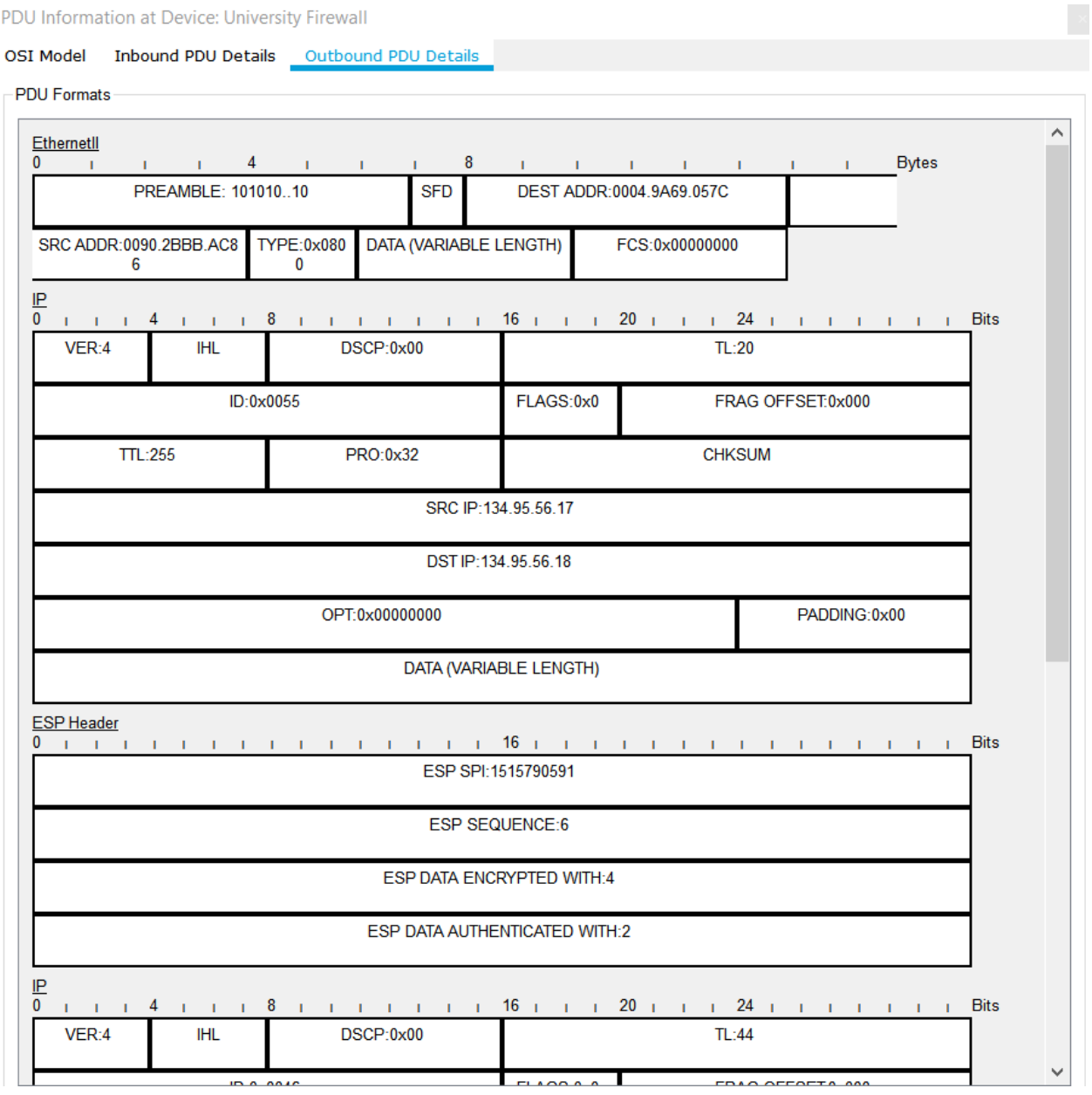
- Selects data flows that need security processing.
- Defines the policy for these flows and the crypto peer to which that traffic needs to go.

A crypto map is applied to an interface .The concept of a crypto map was introduced in classic crypto but was expanded for IPSec.

Minimum requirements for compatibility of two crypto maps is 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 packet has ESP header like 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?**

access - list branch - traffic extended permit tcp object
campus_network object branch_network

access - list university - traffic extended permit tcp object
branch_network object campus_network

Above rules change as,

access - list branch - traffic extended permit udp object
campus_network object branch_network

access - list university - traffic extended permit udp object
branch_network object campus_network

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. **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.

2. **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.

3. **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.

Improve the systems' security by,

- 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)

3.2) Part 2

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

IPSec VPN:

This is done by ip security. ip security rules are added at two servers and a tunnel is created. all the data flow is through the tunnel. it is more secure. that no other system can interfere through the tunnel. But IPsec requires third-party client software, it is more complicated and expensive to set up and maintain.

Clientless SSL 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.