Steven Kim
Mr. Mason
ADV Cisco CCNP P 1, 2
5/15/14
Partner: Matthew Zhao

Lab 11: IPsec VPN

Purpose

The purpose of this lab was to configure IPsec VPN on a network for its security. As much as security is becoming a central issue in the twenty-first century, our job was to implement a security protocol that uses various authentication methods, algorithms, and keys.

Background Information on lab concepts

IPsec - Also known as Internet Protocol Security, an IP protocol that allows the authentication and encryption of an IP packet. This protocol is useful for enhancing the security of a network; it allows the protection of data between host to host, network to network, or even network to host. This protocol runs in the Internet layer of the TCP/IP model and is responsible for protecting the protocols that take place at the Application layer.

VPN - Also known as Virtual Private Network, this connects a private network with a public network and allows hosts from the former to transfer data over to the latter. In companies, VPNs are crucial as they enhance security and provide access to the company's network for employees. This type of network is implemented by point-to-point connections, virtual tunneling protocols, or traffic encryptions.

ISAKMP - Also known as Internet Security Association and Key Management Protocol, this protocol is responsible for managing the various security associations which allow a secure communication to be made within a network. A suitable analogy for ISAKMP and key exchanges is a guide and his travelers; as ISAKMP provides a set of rules for creating and transferring authentication methods and their keys, different key exchange programs establish their own mechanisms and go through the network to transfer authentication methods. Although ISAKMP provides a set of guidelines, the key exchange protocols are able to keep their own mechanisms, for ISAKMP distinguishes itself from other protocols by acting as a "guide." This feature of ISAKMP allows it to be used with all sorts of key exchange protocol. The most common type of key exchange protocol used with ISAKMP is Internet Key Exchange protocol.

IKE - Part of the IPsec protocol, a key exchange protocol that allows the establishment of security within a VPN. There are generally two phases for IKE; the first phase uses the Diffie-Hellman key exchange algorithm to authenticate pre-shared keys, signatures, or public key encryptions while the second negotiates Security Associations (ones mentioned in the description of ISAKMP). As mentioned above, IKE uses ISAKMP as its key exchange manager.

The primary benefits of IKE is automatic negotiations and authentications between devices and the provision of the capability of the network to change keys during an IPsec session.

AES - Also known as the Advanced Encryption Standard, a type of encryption that utilizes the four major rounds: AddRoundKey round, SubBytes round, ShiftRows round, and the Mix Columns round. These rounds are responsible for adding a block onto the key, substituting bytes, shifting the rows in a cyclic motion, and combining the four bytes of the column that replaces the bytes. AES is the main encryption method for IPsec; through these steps, it attempts to secure traffic flowing from one network to another. This algorithm is so secure that it is used by the US government agency.

SHA-1 - Also known as Secure Hash Algorithm, a cryptographic function that constitutes a major part of numerous security applications like SSL, SSH, and IPsec. Its primary role is to encrypt a set of data; for example, when the word 'test' undergoes the SHA-1 algorithm, it is converted to 'a94a8fe5ccb19ba61c4c0873d391e987982fbbd3'. To make sure that the hacker doesn't obtain the password by hacking the computer directly and stealing the password, the computer itself never stores the exact password but stores only the encrypted version. Although SHA-2 was developed and has somewhat replaced SHA-1, SHA-1 is still a commonly used algorithm.

Diffie-Hellman Key Exchange – A type of cryptographical exchange that allows the communication between two separate networks by the exchange of a shared key. The networks do not need to have previously established connections; with the key developed by the Diffie-Hellman Key Exchange, networks can decode each other's respective encrypted messages.

Lab Summary

The overall configuration for this lab was not difficult at all; however, each command was completely new and a bit longer than usual.

As mentioned in Background Information on Lab Concepts, the two phases – ISAKMP Phase 1 and IPsec Phase 2 – are the main components of this lab. Phase 1 deals with

ISAKMP Phase 1

1. Before anything, check if the Security Technology Package license is on the router. Use the command *show version.* Under the Technology column, there will be a “security” section. Check if the word “securityk9” is there.
2. If this word is not there, issue the command *Router (config)# license boot module c2900 technology-package securityk9.* This command will accept the license and set the module as securityk9.
3. Issue the command *Router# copy running-config startup-config* to save the configuration onto the NVRAM. Remember that the command used in step 2 will only work if this command is issued.

IPsec Parameters (on R1)

1. To encrypt traffic from R1 to R3, create access list number 110 by issuing the command *Router (config)# access-list 110 permit ip [network address] [wildcard mask] [network address] [wildcard mask].* With this access list, the IPsec VPN protocol will be triggered only on the two networks in this command. Other networks, by implicit deny, will not be encrypted.
2. Using ISAKMP policy 10, enter the command *Router (config)# crypto isakmp policy 10.*
3. Issue the command *Router (config-isakmp)# encryption aes* to set up the encryption type to AES. As mentioned in Background information on Lab Concepts, this command will allow the user to enter the configuration mode of ISAKMP policy 10.
4. Issue the command *Router (config-isakmp)# authentication pre-share* and *Router (config-isakmp)# group 2.* These two commands will allow the user to set up a pre-shared key and allow the ISAKMP to be a part of DH group 2
5. Issue the command *Router (config)# crypto isakmp cisco address [ip-address]* which configures the key to “cisco.”
6. Now that Phase 1 of ISAKMP has been completed, set up VPN-SET by issuing the command *Router (config)# crypto ipsec transform-set VPN-SET esp-aes epa-sha512-hmac.* This combines the two codes, esp-aes and epa-sha512-hmac.
7. Issue the command *Router (config)# crypto map VPN-MAP 10 ipsec-isakmp* to enter the configuration mode of the given map.
8. Issue the commands *Router (config-crypto-map)# set peer [ip-address], Router (config-crypto-map)# set transform-set VPN-SET, and Router (config-crypto-map)# match address 110* to establish a peer, set the name of the *transform-set* as VPN-SET, and enable the match address to be used with the created access list.
9. Enter the configuration mode of the serial port and issue the command *Router (config-if)# crypto map VPN-MAP*. This command will bind the configured crypto map onto the interface.

For R3, repeat steps 1 to 9.

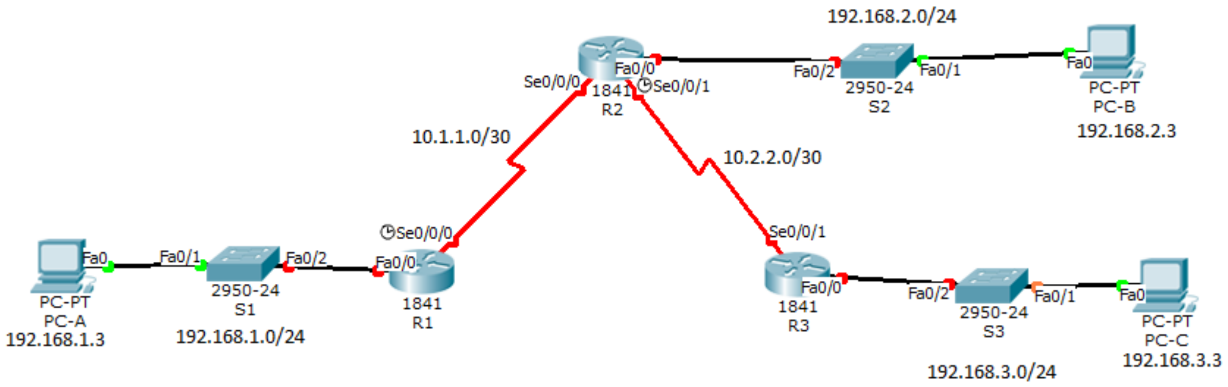
On one of the switches, issue the commands *Switch (config)# monitor session [session-number] source interface [interface]* and *Switch (config)# monitor session [session-number] destination interface [interface].* These two command will allow the switch to duplicate traffic going from the source to the destination and vice versa.

Lab Commands

Router (config)# license boot module c2900 technology-package securityk9	Activates the security module and accepts its license. Once this command is implemented, reboot the router.
Router# copy running-config startup-config	Saves the configuration into the NVRAM of the router.
Router (config)# access-list 110 permit	Sets up boundaries for encryption of data. In this lab,

ip [network address] [wildcard mask] [network address] [wildcard mask]	networks 192.168.1.0/24 and 192.168.3.0/24 were excluded to make sure that IPsec VPN is activated whenever data attempts to be flown from one to another.
Router (config)# crypto isakmp policy 10	Allows the user to enter the configuration mode of ISAKMP policy 10.
Router (config-isakmp)# encryption aes	Literally, sets the encryption type to AES.
Router (config-isakmp)# authentication pre-share	Allows the user to configure a pre-shared key.
Router (config-isakmp)# group 2	Sets the DH key exchange group to Group 2.
Router (config)# crypto isakmp cisco address [ip-address]	Configures the shared key as cicso onto the given IP address.
Router (config)# crypto ipsec transform-set VPN-SET esp-aes epa-sha512-hmac	Allows the given transform-set to be configured using the two encryption algorithms, aes and sha512-hmac.
Router (config)# crypto map VPN-MAP 10 ipsec-isakmp	Enters the configuration mode of the VPN-MAP
Router (config-crypto-map)# set peer [ip-address]	Literally, establishes a peer as the given IP address.
Router (config-crypto-map)# set transform-set VPN-SET	Sets the transform-set as the given name
Router (config-crypto-map)# match address 110	Sets the match address as the access list. This command is necessary for enabling the access list that was created earlier.
Router (config-if)# crypto map VPN-MAP	Binds the crypto map onto the interface.
Switch (config)# monitor session [session-number] source interface [interface]	Duplicates the traffic going from the source port to the destination port. With the destination command, this allows the switc
Switch (config)# monitor session [session-number] destination interface [interface]	Duplicates the traffic going from the destination port to the source port.

Network Diagram with IP's



Configurations

Show run on R1

Show run on R2

Show run on R3

Show run on S3

Problem

The main problem I had with this lab was having to find small typos that seemed insignificant but were in fact influential enough to force me to restart the router. For example, the command *Router (config)# crypto ipsec transform-set VPN-SET esp-aes epa-sha512-hmac* was very troublesome; as complicated as the command was, I often forgot to put the number 512 after 'sha;' this created a completely new

Another major problem I had in this lab was that

Conclusion

Overall, I learned how to configure a protocol that enhances the security of a network. Despite the simple but elusive mistakes that prevented the right key from being implemented, As crucial as security is in all companies, this lab furthered my knowledge of not only an advanced type of security but also its implementation and applications.