Sarah Tse
ITSS 4V95

Assignment 5: Network Protocols

Total Points: 30
Do your own research and write a report on:

1. **What is IPSec and its framework? How does it work and why do we need it? (15 points)**
   IPSec stands for Internet Protocol Security and is a suite of protocols to secure the Internet Protocol layer of the network stack. We need IPSec because it guarantees confidentiality, integrity and authentication when sending sensitive information over an insecure network. Furthermore, IPsec is a protocol used when maintaining a virtual private network connection.

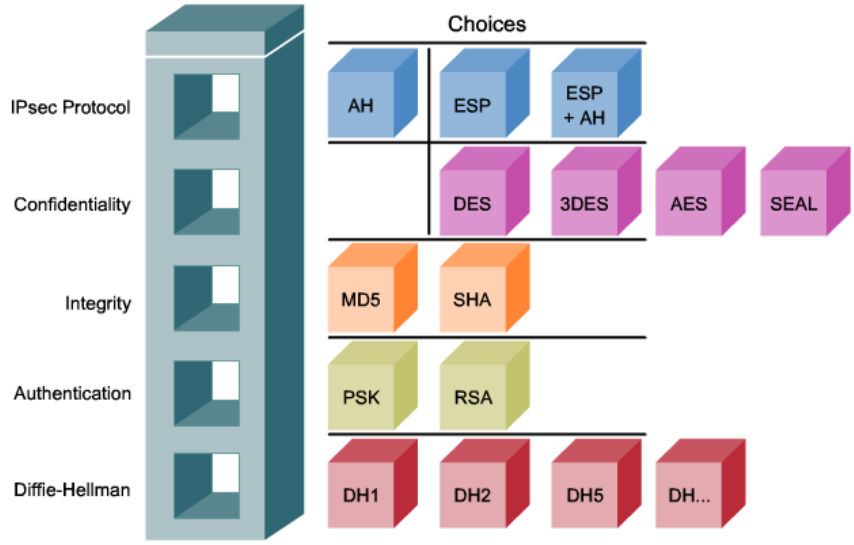

Figure 1 IPSec Framework

The framework can be broken down into the following 5 steps:

1. **Defining Interesting Traffic**
   Within this stage, the sender's computer has a configurable security policy that determines what kind of traffic requires a the IPsec framework. An example would be firewall access lists that determine if certain traffic must be encrypted. This is dependent on the person that oversees the security policy.

2. **IKE Phase 1**
   The Internet Key Exchange Phase 1 process is used to set up the initial security association (SA). An SA is when two IPsec peers establish 5 shared security attributes they would like to use which are the hash, authentication algorithm, group, lifetime and encryption algorithm. The hash, authentication and encryption algorithm, respectively provide integrity, authentication and confidentiality. The 'group' attribute is used to determine what version of the Diffie-Hellman (DH) key exchange to use. DH Key Exchange allows peers that do not have prior knowledge with one another to share keys securely over an insecure channel. Lastly, lifetime defines how long the IKE phase 1 tunnel should last. Generally, the shorter the lifetime, the more secure the channel is, since new keys are generated at a faster rate.

IKE Phase 1 can be implemented in either the main mode, which is longer, or the aggressive mode. The main mode has three 2-way exchanges, with the first exchange being the agreement of the SAs between two peers. The second exchange focuses on using the DH to generate a shared secret and in turn generate a shared key. Additionally, nonces are passed which are signed random numbers and returned to prove the identity of the receiver. The third exchange is where each peer must authenticate one another before the path is considered secure. Once this is done, the Internet Security Association and Key Management Protocol (ISAKMP) session is initiated and IKE Phase 2 starts. Alternatively, aggressive mode can be used which is faster since there is only one exchange with three packets. The initiator will send the SA, Key, Nonce and DH key and the responder will send the same with the addition of the hash (authenticator). Then the initiator will respond with the hash and the IKE SA is established. Once these modes are completed, a secure tunnel or network path is established not to transfer data but to securely send and receive the management traffic of the peers and keep the connection alive.

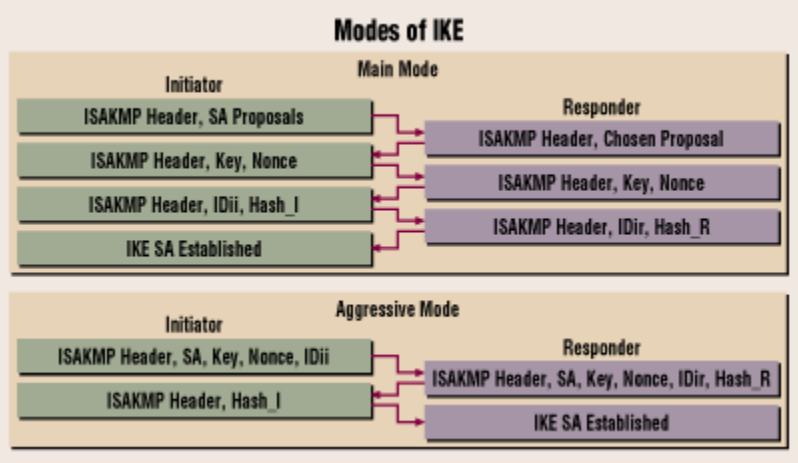

Figure 2 Comparison of Main and Aggressive Mode

3. **IKE Phase 2**

Also known as 'Quick Mode', IKE Phase 2's purpose is to negotiate the IPSec security parameters or transform sets which "is a group of policies that the routers establishing" the session need to match on. The five parameters are:

a. Protocol – The two protocols within the IPSec frame work are the authentication header (AH) and the Encapsulating Security Payload (ESP). AH leaves all data in plaintext but can provide authentication and integrity. ESP is a bit more secure since all data is encrypted and it can provide authentication and integrity.

b. Encryption Type – The options for this parameter are DES, 3DES or AES which are all symmetric key cryptosystems. Data Encryption Standard (DES) is the least secure as it only uses a 56 bit key while Triple DES (3DES) uses 3 different 56 bit keys per 64 bit block, making it harder and longer to decrypt however it takes a significant amount of time. Advanced Encryption Standard (AES) gives the option to use either a 128, 192 or 256 bit key and is the preferred method because it is more efficient than 3DES but still uses larger keys.

c. Authentication – Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1) can be selected for this parameter. Hashes help ensure integrity since they cannot be decrypted. The only difference between the two is that MD5 uses a 128 bit key to produce a 128 bit hash while SHA-1 uses a 160 bit key to produce a 160 bit hash.
d. Mode – AH and ESP can be sent using two different modes: Transport or Tunnel mode. Transport Mode encrypts the payload but leaves the IP address in plaintext. Tunnel mode encapsulates the whole packet and generates a new IP header. The gateways at the sending and receiving side of the tunnel are the ones that strip the new IP header.
e. SA Lifetime – This determines how long the tunnel or connection will stay open and when to re-establish the connection.

In addition to negotiating SA parameters , Phase 2 also establishes SAs and renegotiates SAs. Quick mode can also renegotiate a IPSec SA when the SA lifetime expires.

4. **Data Transfer**
   Once all these steps are completed, data can start flowing through an IPSec tunnel.
5. **Tunnel Termination**
   Lastly, after a set amount of data has been set or the lifetime has expired, the IPSec SA will terminate and keys are discarded. If more time is needed, the whole process may need to start over again.

2. What is VPN and what is it used for? Discuss a general architecture for VPN networks. (15 points)

"A virtual private network (VPN) is anther method used for remote access" where users can access a private network through a public network (Gibson). VPNs add an extra layer of security and access to environments not accessible via the public network. For example, a company's intranet cannot be accessed on an external network. By using a VPN, an employee not physically inside the workplace, is able to access the company's internal resources. VPNs are beneficial for companies because it enables employees visiting a client or working from home to have access to resources. Outside of corporate use, some VPN users utilize the service to access specific content offered in certain countries by opening a connection through a VPN provider.

Generally, there are two main type of virtual private networks, host-to-gateway/remote access and site-to-site VPNs. Host-to-Gateway VPNs are when a user connects to their own network that uses their Internet Service Provider (ISP) to start the VPN connection to the VPN server hosted on a demilitarized zone (DMZ) server. From there the user can be authenticated using RADIUS or LDAP.

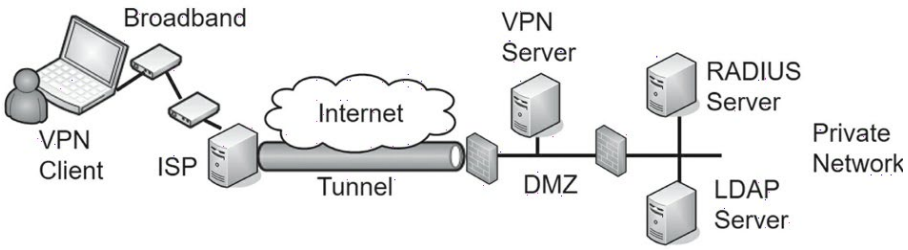

Figure 3 Host-to-Gateway VPN architecture

A site-to-site VPN is typically used when there is a main site and a remote site for a company. Since users are already authenticated to the remote network, they just have to connect to the VPN gateway to start the connection. Site-to-site is typically easier on the user since the authentication is already completed.

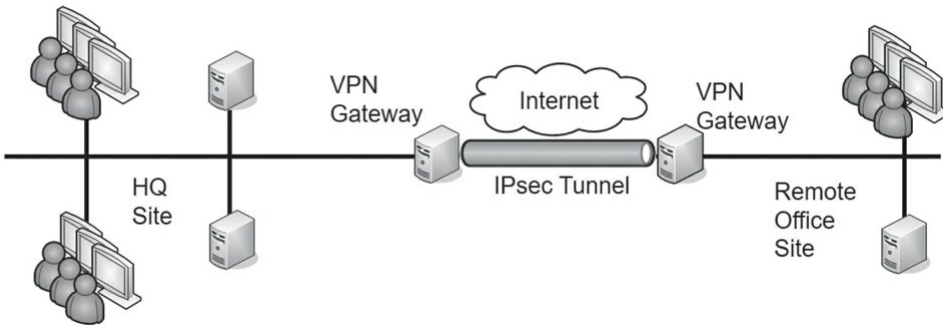

Figure 4 Site-to-Site VPN

What is similar between the two types is that there is a server or gateway that the user is trying to connect to. Through these servers or gateways, data can start communicating through a secure tunnel.

References/Resources

SC Labs. (n.d). CCNA Security Chapter 8 – Implementing Virtual Private Networks. Retrieved from https//sclabs.blogspot.com/2012/11/ccna-security-chapter-8-implementing.html

CBT Nuggets. (2012, Oct. 11). MicroNugget: How to Negotiate in IKE Phase 1 (IPSec). Retrieved from https://www.youtube.com/watch?v=doSW8d2iLFM

Mason, Andrew. (2002, Jan. 4). VPNs and VPN Technologies. Retrieved from http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6

Mmitesha. (2017, Aug 23). Main Mode Vs Aggressive Mode. Retrieved from https://community.cisco.com/t5/security-documents/main-mode-vs-aggressive-mode/ta-p/3123382

Cisco Meraki. (n.d.). IPsec VPN Lifetimes. Retrieved from https://documentation.meraki.com/MX/Site-to-site_VPN/IPsec_VPN_Lifetimes

Gibson, Darril. (n.d). CompTIA Security+ Get Certified Get Ahead: *SY0-501 Study Guide* version 4. YDCA, LLC.