4/2/2018

Virtual Private Network Security

Saint Leo University

Network Defense and Security

Instructor: Dr. Omar

Group Members:

Ryan Haug

Ryan Kolesnikov

Keanu Munn

Garrett Taylor

Abstract

Network security has become one of the most paramount issues faced in businesses and federal entities across the World today. Because of this reality, security controls and techniques are constantly evolving and being implemented to secure network resources and assets. The objective of this paper is to conduct an analysis on some of the security features of one of the most commonly used network security technologies called virtual private networks (VPN). First, a general overview of VPN characteristics and benefits achieved from deploying this technology will be discussed. Followed by, a breakdown of one of the security protocols many VPNs use today called IPsec. Finally, an analysis of a common VPN mode called tunnel mode will be provided in this paper.

Introduction

Before going into detail about some of the common security features found in VPN technology, it is important to understand what a VPN is and the benefits it can provide for a business or federal entity towards the effort of securing network resources. The best definition of a VPN is that it is “a mechanism to establish a secure remote access connection across an intermediary network, often the Internet” (Stewart, 2014).

1.0 Characteristics of a VPN

Imagine if a company had a wide selection of employees that either worked from home or those who travelled frequently for the company but needed access to resources only found on the network at the company’s headquarters. The company would have to provide a means for a remote connection from HQ to any public network the employee may being trying to connect from, while also ensuring this connection remains secure and private. For this situation, a VPN would be the perfect tool. VPN’s enable a company to use connections found on the Internet to establish either a remote access or remote-control connection. Remote access is simply the user establishing a connection to the desired network and being able to access network resources. Remote control is different in the sense that a user can “use a local computer system to remotely take over control of another computer over a network connection” (Stewart, 2014). Either way, both instances are useful for a business, but how can this remote connection be secure?

The most practical instance of a VPN is one that uses authentication and encryption technology. When a VPN is deployed the option to use encryption algorithms is available. “A virtual private network can enhance protection to a high degree by

encrypting all traffic between the roaming client and the company network" (Oriyano, 2014). Encryption ensures the data that is transmitted across the remote connection is private and secure. If someone were to eavesdrop on the connection, the data observed would be just a bunch of ciphertext. Additionally, VPNs have authentication mechanisms in place to make sure that only authenticated users can establish a remote connection. Authentication methods can vary, but the most common are username and password, smart cards, token devices, and biometrics. Obviously, the best security method is one that utilizes multi-factorization for authentication. However, the protocols that a VPN uses also help define the security strength of the connection.

2.0 IPSec Overview

The internet connects hundreds of millions of people all across the globe, and it allows for instant communication and access to an ever increasing library of information. Video, data, and voice all travel across the internet, but some of this information is supposed to be confidential and needs to be protected. The main protocol/language that governs the internet is something called IP. IP, or internet protocol, is how data is sent over the internet to users. IP is not in itself secure in anyway, which is why IPSec was created. IPSec is a suite of protocols that bring security to IP, and provide services like data integrity, data source authentication, confidentiality, and protection from attacks like replay. IPSec brings the necessary protection to IP to make the internet a viable source for entities like businesses to conduct confidential communication. It also brings reliance from the healthcare to expand business while still abiding by government regulations like HIPPA in the United States of America. IPSec also gives users comfort in being able to use the internet for services like home banking, insurance, and home

day trading. All of these transactions can take place on the internet with security of the information with IPSec. IPSec first started on IPV4, but has been able to expand to also use the newer IPV6. In addition to sitting on top of IP, IPSec can also be used for TCP, UDP, and ICMP making IPSec truly a protocol with much versatility and the ability to evolve with the ever changing landscape of the internet. Lastly IPSec can be deployed on a Virtual Private Network, where two separate and distinct networks become one with a tunnel that is secured with IPSec. The internet will continue to grow exponentially, and it is crucial that people continue to feel secure with confidential data transmission through the internet, and IPSec ensures this. Every person is entitled to confidentiality of there information, and thankfully the cryptographic algorithms of IPSec help with that. (Doraswamy & Harkins, 2003)

2.1 Cryptography of IPSec

Every system that is connected to the internet can be attacked or hacked in some way. History of the internet has proven that fact, and the attacks will continue to evolve, and get more and more complex. Business employ cyber experts to create countermeasures, and other practices to prevent attacks from getting into the system. The costs of a successful attack almost always outweigh the amount it would cost the business to institute countermeasures. Numerous techniques exist purely for the function of encrypting messages, guaranteeing authenticity, and maintaining integrity of a message. One cryptographic block solves a certain problem, but when chained together they create a cryptosystem. A cryptosystem should be stronger than the threat that it was built to prevent. Thankfully IPSec has an entire cryptosystem built within it. (Doraswamy & Harkins, 2003)

2.2 Block Cipher

Numerous countermeasures can be found in the cryptographic algorithms of IPSec. One type of cryptography that IPSec utilizes is block ciphers. Block ciphers will process data by first diving the data into equal sized chunks with each chunk's size being determined by the block size of the cipher. There is no guarantee that the length of the input will be a multiple of the block size, so block padding might be needed to create a multiple. (Doraswamy & Harkins, 2003)

2.3 Asymmetric Cipher

Asymmetric ciphers are a part of public key cryptography. There exist two keys, one being a public key and one being a private key. One key will do the encryption and the other key will handle the decryption. When given the public key it is computationally just about impossible to figure out the private key. A good public key algorithm will be based on one way functions. (Doraswamy & Harkins, 2003)

2.4 IPSec as it Relates to VPN

Virtual Private Networks are used for remote users to be able to get into their network from a place where they would regularly be unable to log into the network. Virtual Private Networks are crucial for businesses because it ensures that employees are able to do work while on the road, otherwise known as "Road Warriors." Virtual Private Networks are inherently secure because they use the cryptographic algorithms previously mentioned throughout IPSec. IPSec is one of the ways that businesses can use Virtual Private Networks to not only transmit data, but do so with assurance that IPSec will keep the information confidential, and the data will be transmitted with integrity.

3.0 Overview of VPN Tunnel Modes

Tunnel mode is an IPSec Mode used for site to site traffic. This means that it is the most common used for connecting of two sites securely. Take Office A for example. This office has its own network and its own security gateway and its own VPN gateway. Then we have Office B that has all of the same gateways. To safely connect these two networks across the internet we would use VPN Tunnel Mode.

3.1 How Tunnel Mode Works

VPN Tunnel mode works by taking the original payload and original header and encapsulating it within another packet. The VPN then uses one of two headers an AH header or an ESP Header. The AH header provides no confidentially while ESP provides encryption. An additional new IP header is added. This new address is the address of the VPN Gateways. This is done so that the data can now be sent safely between the two gateways. Once the data arrives at the new gateway it is decrypted and routed or just routed depending on the header.

3.2 Difference between AH and ESP

The major difference between AH and ESP is the packet structure. In both cases the packet is encapsulated. In ESP the original packet is wrapped in an ESP header and an ESP trailer which is then wrapped with a new IP header which is the gateway header and an ESP auth trailer to preserve security. In AH the original packet is wrapped with an auth header and then a new IP Header is attached. the most important thing that AH does is protect the entire packet. The ESP header is the most commonly used because it provides encryption. The AH header can be used on its own

or it can be used with the ESP header. Using both would provide a double encapsulation. The IP protocol ID's of ESP and AH are 50 and 51 respectively.

3.3 Why Tunnel Mode is the Most Common

Tunnel Mode is the most common mode used in VPN's for a specific reason. This reason is that businesses have multiple sites that need to operate on the same network. The use case for an office in California and Georgia acting as if they are the same network is a very powerful tool. Being able to encrypt this data across the two businesses is the key. Even though the data is not always encrypted. This method is how a law firm can keep its files secure and use them across multiple locations.

Conclusion

Overall VPN, Virtual Private Network, is a much needed service that businesses need to continue to increase in productivity, and ultimately profit. VPNs provide access for users who are away from the network to access the network through the internet. With this access must come security, and this security can be found in the IPSec suite, and tunnel mode. Both are needed to secure the data that is being transmitted over the internet. Encryption, hashing, and encapsulated packets are the several steps that VPN uses to secure the information that is being sent through the network from a remote access point.

References

Doraswamy, N., & Harkins, D. (2003). *IPSec: The new security standard for the internet, intranets, and virtual private networks*. Upper Saddle River, NJ: Prentice Hall PTR.

Oriyano, S. (2014). *Hacker Techniques, Tools, and Incident Handling.* Burlington: Jones & Bartlett Learning.

Stewart, J. (2014). *Network Security, Firewalls, and VPNs.* Burlington: Jones & Bartlett Learning.

Thomas, J. (n.d.). IPsec VPN Modes – Tunnel Mode and Transport Mode. Retrieved April 02, 2018, from http://www.omnisecu.com/tcpip/ipsec-vpn-modes-tunnel-mode-and-transport-mode.php

Understanding Vpn Ipsec Tunnel Mode and Ipsec Transport Mode – What's the Difference? (n.d). Retrieved April 02, 2018, from http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html