Week 6 You Decide -

Cryptographic Tunneling and the OSI Model

Anthony Meunier

DeVry University

SEC 360

Week 6 You Decide – Cryptographic Tunneling and the OSI Model

From studying the scenario for Sunshine Machine Works and its review of the company information systems use security policy, it is clear to see that a virtual private network (VPN) must be implemented to meet and exceed all of the requirements for security and business continuity and longevity that management desires. In this case there is a strong desire for work to be done externally, away from the main office premises. Naturally a concern exists when accessing data over the air in this manner, especially when much of the data is sensitive business information such as customer account information. By establishing a VPN, employees will be able to connect to the local intranet via remote access methods and the utmost security methods will be applied to this access of data via the VPN tunneling methods that make it so secure. Remote access basically requires this form of security because it is fairly easy for prying eyes to tap into unsecure connections, such as at a local Wi-Fi hotspot. By using a VPN, all of this traffic is tunneled through an encrypted information highway which is unlikely to be cracked by anybody trying to snoop in on these transactions. First, understanding the principles of cryptographic tunneling is essential to fully understanding how a VPN can then operate. In addition, exploring the protocols associated cryptographic tunneling is equally as important.

The OSI model dictates how these data transactions function and also sets the basis for how something like cryptographic tunneling by way of a VPN can be so secure. Essentially we flow through the layers of the OSI model in order to set a system of checks which ultimately restrict information access to only users that are deemed authorized. Therefore authentication is a big factor in establishing a cryptographic tunnel, as only those authorized can then flow through the tunnel to send and receive information from the internet servers. VPNs can operate on, or utilize, different layers of the OSI model in order to achieve the encryption level that they are known for. Examples of this include a Data Link Layer VPNs, Network Layer VPNs, and Application Layer VPNs. In each of these types we see a different function of the OSI model: in Data Link VPNs there would be 2 private networks which both are connected at the layer 2 level of the OSI model and thus all ensuing traffic across this layer at both sides can be segregated at the layer level. Inherently there is no encryption in this method but rather just the segregation of traffic. In Network Layer VPNs, layer 3 of the OSI model is applied and thus “tunneling” and encryption are applied. This is achieved through various protocols such as IPsec tunneling (which provides encryption, authentication, and negotiation), and encryption or L2TP and GRE protocols. The Network Layer VPNs are very strong all around because they provide the encryption and tunneling desperately needed for maximum security while also being low enough in the layer stack to provide strong and seamless connectivity to all of the applications built above it. Finally, Application Layer VPNs are unique in that they are built only to use with specific, matching applications. For instance there are SSL and SSH based VPNs at this level, and for SSL there would be encryption between any web browsers and any servers they connect to that are running SSL as well. SSH is the more go-to protocol because it can encrypt which also helps it establish VPNs for other application layer protocols with examples being HTTP and FTP; in addition SSH is also used widely to establish secure login sessions between network devices. While this level of security and authentication is what we desire, one of the drawbacks to Application Layer VPNs is that they require specific actions by the user to enable the devices to implement/connect with the VPN which removes some of the seamlessness offered by the Network Layer VPNs. Overall the Network Layer and Application Layer VPNs are the strong suits for Sunshine Machine Works and really either would be suitable for the company’s IT and security needs. The decision really comes down to whether you want the encryption and tunneling to occur at the application level (which would require serves to be on the same page) or the network layer, which may be a more seamless handoff. Both implore strong protocols with encryption and tunneling which is critical for remote access to a company’s important business data.

References

Breithaupt, M. M. a. J. *Information Security Principles and Practice*. [VitalSource Bookshelf version]. Retrieved from <http://devry.vitalsource.com/books/9781256058328/id/app03>

VPN Types Based on OSI Model Layer. N. D. Retrieved from <http://book.soundonair.ru/cisco/ch10lev1sec3.html>