Running Head: VPN

VPN: Implementation

Jered McClure

Walden University

VPN: Implementation

Screenshot of Head Office showing configured crypto map enabled on Interface s1/1:



Screenshot of Branch showing configured crypto map enabled on interface s1/0:



Screenshot showing Branch Crypto Configuration and crypto session:



Screenshot showing Crypto map and crypto session of Head Office:



 While email is a valid form of communication, it has its flaw in the fact that files being sent or received must be stored in triplicate through the email system. For instance, if I were to send a 10MB file to my buddy Will, that file would first be stored in a local directory. The file would then be stored on the exchange server, and finally the file would get stored on Will’s machine. In instances where the file is sent to multiple recipients, say an entire department of 100 people, that file would go from being a 10MB file to being a 1000MB file. A single user could, in essence, flood a network with traffic inadvertently doing nothing more than sending a single file.

 VPN connections overcome this limitation by allowing a user to store the file in a shared folder. Each recipient could then connect to that folder and peruse the document as required. In some instances, the 100 recipients may not need access to the file, and only 20 or so users would even look at it. An email could still be sent, but instead of having the document attached, the email would simply stat “go here for the file.”

 At the core of a network, a MLS allow for the implementation and integration of multiple features out of one box. Across a MAN setup, this reduces the amount of hardware to keep track of, while increasing the overall functionality of a network. VLANs, QoS, Routing, Shaping, and Tracking can all be done through a single device.

 However, at the edge of a network, all these features may not be required. Reason being that the internal network has already done the vast majority of work for packet processing. As such, a gateway router would suffice, in most instances. Intention being, edge nodes are likely to have all traffic passing through them. Having their sole purpose be nothing more than routing would ensure that traffic is not bogged down by further functions which core nodes can manage.

 When deciding between VPN, MPLS, or SSL/SSH transport multiple factors must be decided upon before implementation can begin. VPNs allow for the secure connection of two separate networks at low cost (Meyers, 2009). However, VPNs are subject to the wild traffic of the internet, and once the data leaves the core network, it can only move as fast as the intervening routes will allow. This is fine for simple file sharing, but can become burdensome when working with speed sensitive applications.

 MPLS on the other hand is managed at the ISP level (Chadda, 2004). This means that there will be an incurred fee greater than VPN or SSL/SSH combined, usually. However, traffic is sure to get to its destination at the fastest possible speed using the best QoS and shaping offered. When working with applications that must have access to large amounts of data in the shortest possible timeframe, this is the premium way to go.

 SSL/SSH should only be used on data light transfers, or when connecting to remote consoles. There is largely no fee suffered for using these protocols. However, they are absolutely subject to internet traffic, and in some cases are subject to cracking through methods like BEAST (browser exploit against SSL/TLS) (Goodin, 2011). This does not mean they will crack the security, but that it is a possibility. As such, SSL/SSH should be relegated to non-sensitive traffic that is preferred private but is not detrimental to the network at large.

 When file transfer is the key goal, VPN is the go to method most definitely. However, when traffic shaping and QoS over the Internet are a must, the network administrator must pay the bucks and implement MPLS. If privacy is a concern but data loss is not a detriment to the network at large, SSL/SSH is definitely an option. The key thing to remember is that the internet is a jungle, separation of network data is a must or the network is asking to be cracked.

References

Chadda, A. (2004, December). *Quality of Service Testing Methodology.* Retrieved April 24, 2012, from University of New Hampshire: ftp://ftp.iol.unh.edu/pub/mplsServices/other/QoS\_Testing\_Methodology.pdf

Goodin, D. (2011, September 19). *Hackers break SSL encryption used by millions of sites.* Retrieved May 11, 2012, from The Register: http://www.theregister.co.uk/2011/09/19/beast\_exploits\_paypal\_ssl/

Meyers, M. (2009). *CompTIA Netowrk+ Guide to Managing and Troubleshooting Networks* (2nd ed.). McGraw-Hill.