International & Federal INFOSEC Standards & Regulations - Final Paper

Nicholas Somerville

University of Advancing Technology

Table of Contents

International & Federal INFOSEC Standards & Regulations - Final Paper

"A Virtual Private Network (VPN) is a technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider" ("What is VPN?," n.d., para. 1). The point of a VPN for enterprises is to permit remote users access to a company's central network via secure, encrypted tunnels (Beal, n.d., para. 2). Since the tunnel is encrypted, any individual or group sniffing packets sent are incapable of viewing the contents of said packets. While many users may use a VPN service or create a VPN of their own for privacy or anti-censorship reasons (para. 4), VPNs in the business realm act as a cheaper, secure alternative to dedicated hardlines and remote terminal technology (Frankel, et al., 2005, p. 20, para. 2). Modern VPNs have three models (gateway-to-gateway, host-to-gateway, and host-to-host) and use a/symmetric cryptography (para. 2 – 3).

Purpose

This IPsec implementation plan is created to assist any business, small or large, create a secure, yet financially viable, means of having users that work from home, remote locations, or remote offices connect to a company server. The paper should demonstrate the usefulness of VPN services, subscribed or self-made, as well as what resources will be needed, how to subscribe to a service or create own VPN client, a planned to implement strategy, the budget needed prior and after implementation, how to evaluate what's needed, and the benefits of using a VPN. What will be proposed is at least one solution for subscription services and one solution from hosting own VPN client while each solution will be specifically aimed for SOHO settings of independent contractors, where travel is a key function of work to best demonstrate VPNs usefulness. These solutions will be compared against dedicated hardlines and remote terminal technology to better demonstrate such, even though dedicated hardlines for work requiring constant travel is completely infeasible. For the purpose of this demonstration, the small company is question will be referred to SEPT ltd. or Social Engineering and Penetration Testing consulting firm ltd. with ten employees at most. Even though this paper constantly mentions three solutions with no specific choice of which three will be the final, the default to keep in mind is the self-hosted solution. The other two solutions are merely alternatives to consider.

Problem

The problem at hand is that SEPT ltd. hires independent contractors to work as social engineers and penetration testers for clients that hire, while reaping the benefit of being a potentially recognizable collective like Rapid7, but the contractors have no means of filing reports back to the main SOHO securely. While some businesses in a field of traveling contractors prefer sending reports via email, unencrypted no less, a small collective of pentesters should be as responsible for maintaining and understanding how their own server works (until large enough to have a dedicated IT department). Dial-in access requires leased telephone lines, call-trafficking equipment to handle incoming calls, and the cost of toll calls. The use of VPNs eliminates the cost of toll calls, requires a VPN client server vs specific equipment, and connects through an ISP (Engelking, 2000, para. 3 – 6). RDPs, or remote desktop programs, could be just as easily used, but lack in security and would be thus ironic for penetration testers to use in place of VPNs. The best alternative would be tunneling via SSH with asymmetric cryptography, yet still faces the issue of unencrypted packets that could be sniffed by snooping third parties. Thus, a VPN connection is needed for independent contractors of pentesters and social engineers to connect to the main office when on the road.

Proposal

Three solutions are to be proposed and each are viable solutions considering that SEPT ltd. is a small company vs moderately-sized or large. If SEPT ltd. were medium or large, the use of a VPN subscription that wasn't internally created and thus can't be solely trusted would be as bad as a group of pentesters using unsecure means of communication among each other. Two solutions, as previously stated, are to use a VPN subscription service and to create one instead. The latter faces two different solutions where a physical server can be created to act as the VPN client server separate from the main server is use as well as a cloud server solution.

Subscription service. Fahmida Rashid (2014) tested ten different subscription VPN services and found Private Internet Access to be the only VPN subscription service over four stars. Private Internet Access offers three paid-tier plans of $6.95 monthly, $35.95 biannually, and $39.95 annually where all three tiers offer the same exact benefits at different pricing points. PIA gives P2P and VoIP support, uses PPTP, OpenVPN, and L2TP/IPSec, supports 5 devices in use simultaneously, has multiple VPN gateways, has unlimited bandwidth, includes SOCKS5 Proxy, easy set-up, and doesn't retain any traffic logs whatsoever ("Buy Safe and Secure VPN," n.d.). With PIA comes the capability to select from any 8 servers in the US, 25 internationally, and automatic server selection for the server with the least latency from current location. PIA also includes encryption of AES-128, AES-256, or Blowfish, authentication of SHA1 or SHA256, 3-way handshake with RSA-2048, RSA-3072, RSA-4096, ECC-256k1, ECC-256r1, and ECC-521, port forwarding, VPN kill switch to disable Internet connection when VPN disconnects, DNS leak protection, and IPv6 leak protection. PIA is a service great for consumers, but may be a viable option for a small company of independent contractors, assuming trust can be placed in the hands of a third-party regardless of reputation.

Self-hosted server. A company hosting their own VPN client server is not only the cheapest option but also the most trustworthy since the logs written would be by their own server vs a third party. For experienced penetration testers with even a small degree of experience of UNIX/Linux distros, creating a VPN client service with OpenVPN is a relatively easy procedure, but even for those only experienced in Windows will find easy-to-follow walkthroughs for installing and configuring the necessary packages as shown by Jay Redge (n.d.). Granted, the necessities for this solution is networking engineering experience, a desktop, laptop, or modular PC (Raspberry Pi/Arduino), and the cost of additional electricity generated that wouldn’t be a factor in a subscription or cloud service solution. To clarify, network engineering experience will actually be a necessity for cloud service solutions, but as stated repeatedly, this should be a non-issue for a group of penetration testers. Unlike the subscription service model, these last two solutions are highly customizable to the users’ needs and allow for increased knowledge and experience via experimentation.

Cloud-hosted server. Cloud services is an option for numerous reasons. One, physical machines are more prone to system failure/corruption than virtual machines, which are easily portable and replicated to host on a different machine once first machine fails. There are numerous cloud service providers that add this incident response scalability to shift cloud instances from one server to another if a server fails without having to shut down the instance in question. With a self-hosted solution, if the server used fails for any reason, there is no immediate alternative unless a second was configured for just that reason. Two, depending on the activities done on a server, cloud services can be cheaper with maintenance, parts, repair, electricity, space, and portability than the self-hosted alternative (Strom, 2011). However, just like with subscription service, SEPT must depend on their cloud provider to be secure in maintaining hardware. Otherwise, the set-up and use is almost identical to self-hosted option with choosing a UNIX/Linux distro of choice and going through the easy-to-follow set-up process like as if using Amazon Web Services as the cloud service provider.

Requirements

No matter which of the three given solutions are chosen, only one user (see Manager for details) will be needed for the configuration. If the subscription service solution is chosen, what will be needed is a payment account for reoccurring fees, an email address for the VPN provider to send receipt, username, and password information, and a couple of minutes to download and configure the prepackaged VPN application used. If the self-hosted solution is chosen, what will be needed is a machine like a desktop PC, laptop, or modular PC to act as the VPN server, network engineering experience, and a UNIX/Linux distro of choice. If the cloud service solution is chosen, what will be needed is a payment account for reoccurring fees, an email address for the cloud service provider to send receipt, network engineering experience, and a UNIX/Linux distro of choice. While the latter two both require a UNIX/Linux distro of choice and network engineering experience, all three do require payments in some form factor. VPN service providers are paid for subscription, cloud service providers are paid for resources consumed hosting the VM, and the self-hosted option increases the electricity bill of the SOHO used.

Timeline

Adding an implementation itself seems like a waste of time considering that even the latter two solutions of having to create the VPN server will take at most a day to create and implement at best. However, testing for new users may actually take days with constant tweaking if the single user in charge of creating the VPN instance used is unfamiliar with setting their own

VPN instance. In which case, the following timeline is a timeline for evaluation and testing (see section Evaluation for details), not just implementing:

Creating / installing and configuring VPN	Day 1
Connectivity	Day 2
Default Settings	Day 2
Logging	Day 2
Protection	Day 2
Authentication	Day 2
Management	Day 3
Performance	Day 3
Application Compatibility	Day 3
Security of the Implementation	Day 3
Component Interoperability	Day 4

The last five components (management, performance, application compatibility, security of the implementation, and component interoperability) should be evaluated regularly on a monthly basis at most to ensure an efficient, secure VPN. Protection and authentication are not included due to component interoperability having to check the smaller components that would ensure protection and authentication, thus check them by transient properties. Logging should be maintained, but isn’t counted under constant evaluation since logging should be a part of the management aspect. Performance being counted as its own item may seem to contradict this statement, but performance should be checked regularly against any updates from the other consistently evaluated criteria mentioned.

Budget

Budget is not, cannot, and will not be clearly defined. Subscription service is the only solution with the financial amount in black-and-white up front with the most reasonable cost at $39.95 as previously mentioned. However, the budget necessary for the Manager to implement and evaluate this VPN solution is still as unforeseeable since the amount of time the Manager must take to implement and evaluate has to be paid somehow (read reinvest profits into SEPT acting IT department), especially since it would detract from the managers own clients. Putting the additional finance into a management position aside, there are additional costs for the self-hosted and cloud-hosted solutions. The self-hosted solution requires paying for additional security, parts, and time spent maintaining and/or repairing the VPN server in question. While electricity generated can be monitored with an established pattern to better predict future budgets, when parts fall apart and how much time will be needed repairing said parts is unpredictable. Even though it is the most favorable solution, it is the financially most unstable solution.

Comparison. Cloud-hosting would be dependent on the cloud service provider chosen. Since Amazon Web Services, or AWS, was mentioned earlier (due to being the highest rated cloud service provider), a budget can be partially ascertained from the fees stated on their site. Assuming SEPT ltd. wants the cheapest solution, since VPN servers require so few resources, the best option would be t2.micro with one virtual CPU, 1GB memory, and would cost $0.013ph. The monthly costs would be under $10 and over $110 annually. While this solution isn’t as cheap as PIA, SEPT ltd. would have more control and faith in their own solution, which may be cheaper annually than self-hosting in electricity and parts. If the solution to choose solely dependent on budget, PIA would be the best solution. For security, self-hosting would be the best solution. For a compromise that’s scalable, cloud-hosting is the best solution. Unfortunately, there are no clearly discernable budgets in VPN use without an existing bill of which to establish a pattern.

Evaluation

Following the evaluation best set already by the Guide to IPsec VPNs, the aspects should be connectivity (Frankel, et al., 2005, p. 64, para. 2), protection, authentication, application compatibility, management, logging, performance, security of the implementation (p. 65, para. 1 – 7), component interoperability, and default settings (p. 66, para. 2 – 3). Connectivity is an easy aspect where SEPT contractors test whether or not they can connect to whichever of the three solutions chosen. Given that this is a VPN for a group of pentesters, protection, authentication, and security of the implementation should be tested by each contractor using the very skillset of which they are employed. The user to set-up the VPN instance should also be the manager, in which case management, application compatibility, logging, performance, component interoperability, and testing custom settings against default settings should be the sole responsibility of said user.

Manager. This user to set-up and maintain the VPN server will be hereby mentioned as the manager (should also be the one of ten to maintain the SOHO main server acting as the company system administrator and network engineer vs also being an independent contractor). It is their sole responsibility, as the dedicated pentester to also act as the group’s VPN system administrator, to ensure that the VPN in use does not interfere with any other application. If PIA solution is chosen, be warned that the use of BitDefender antivirus is incompatible if the VPN in use is over WiFi and the WiFi connection suddenly drops. All connections should be automatically logged, but the manager should neatly organize each log into a directory with subdirectories of each contractor. The performance should be tested against connection to the main server with and without the use of the VPN so that the VPN can be optimized to offer the performance closest to not using a VPN since VPN use slows traffic. The biggest issue facing the manager is component interoperability regardless of solution as failure to maintain any one component to the industry standard negates the entire point of using a VPN (para. 4). Read as VPN tunnel traffic without encryption or VPN connection without authentication.

Benefits

VPNs are a secure means of connecting to a system remotely while RDP has no means of encryption to keep packets transmitted and/or received as secure. However, VPNs can suffer lag, especially with increased encryption with the use of default ports, whereas RDP doesn't experience this issue since RDPs use the resources of the connected system instead (Laverty, n.d., para. 4). The benefit of the subscription service is ease, despite a need for complete trust, the benefit of the self-host option is faith in own server, despite acting as a single POF if the server crashes with no immediate back-up running, and the benefit of the cloud service option is price, despite still requiring a need for complete trust. All three solutions suffer the same exact drawback that is experience with any VPN use: lag. However, slight lag is immeasurable to great security from high-level encryption. Thus, the benefits outweigh the drawbacks by a substantial margin.

Conclusion

SEPT ltd. is a small company collective of ten independent contractors working as social engineers and penetration testers. With a VPN solution, this group can securely connect back to the SOHO server to file their reports without having to worry about sniffing, IP tracking, breach of data, or bandwidth use from the local network used. Three solutions have been given of subscription service, self-hosting, and cloud-hosting, albeit without an obvious budget for the latter two solutions in general or all three with the Manager implementing, evaluating, and maintaining. The requirements of gear and personnel, evaluation, and timeline of implementation and evaluation were direct enough to deter confusion, yet left broad enough for room for error such as the evaluation timeline. The benefits are direct and greatly outweigh the drawbacks that any business that has employees regularly connect to their network from different locations should be implementing their own VPN solutions. After all, even outside the business realm, who doesn’t appreciate a secure connection with encrypted packets to deter censorship, snooping, and potential attacks?

References

Amazon EC2 Pricing. (n.d.). *Amazon Web Services, Inc*. Retrieved from https://aws.amazon.com/ec2/pricing/

Beal, V. (n.d.). VPN – virtual private network. *Quinstreet Inc*. Retrieved from http://www.webopedia.com/TERM/V/VPN.html

Buy Safe and Secure VPN. (n.d.). *London Trust Media Inc*. Retrieved from https://www.privateinternetaccess.com/pages/buy-vpn/

Engelking, E. (2000, Nov. 17). How can using a VPN benefit your company? *CBS Interactive*. Retrieved from http://www.techrepublic.com/article/how-can-using-a-vpn-benefit-your-company/

Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A., Ritchey, R., & Sharma, S. (2005, Dec.). Guide to IPsec VPNs [PDF document]. *National Institute of Standards and Technology*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

Laverty, S. (n.d.). Remote Desktop Vs. VPN. *Demand Media Inc*. Retrieved from http://www.ehow.com/about_5485544_remote-desktop-vs-vpn.html

Rashid, F. (2014, Jan. 9). Ten VPN Services You Should Know. *Ziff Davis, LLC*. Retrieved from http://www.pcmag.com/article2/0,2817,2403388,00.asp

Redge, J. (n.d.). Host Your Own Virtual Private Network (VPN) with OpenVPN. *Autodesk, Inc*. Retrieved from http://www.instructables.com/id/Host-Your-Own-Virtual-Private-Network-VPN-with-O/?ALLSTEPS

Strom, D. (2011, Apr.). How cloud computing kills clustering. *TechTarget*. Retrieved from http://searchcloudcomputing.techtarget.com/feature/How-cloud-computing-kills-clustering

What is VPN? (n.d.). *What Is My IP Address*. Retrieved from http://whatismyipaddress.com/vpn