Global Information Assurance Certification Paper

Deploying a Secure VPN:

A Primer for Small Organizations

Harlan Hoult
August 15, 2004
Practical Assignment Version 1.4b, Option 1

Table of Contents

Abstract

With the wider availability of high speed internet, the popularity of remote access using virtual private network (VPN) technology is becoming more widespread. Once the domain of large organizations, the decreased cost and ease of deployment has meant that smaller organizations are able to benefit from the technology. The downside is that many small organizations may not have the resources available to properly and securely deploy a VPN solution. This guide is intended to discuss the highlights of planning and deploying a secure VPN solution. It is not intended as an in depth analysis of different protocols and implementations.

Introduction

A VPN supplies network connectivity over a possibly long physical distance; In this respect a VPN is a form of a Wide Area Network (WAN). The key feature of a VPN however is its ability to use public internetworks such as the internet to emulate private network links. This is accomplished using a variety of protocols and technologies that are intended to protect the privacy and security of the transmitted data. [1]

Often VPNs are presented as an easy-to-setup low-cost solution for remote access, reducing costs and increasing employee productivity. The “sizzle” is sold with little consideration given to the less glamorous side of ongoing maintenance or the risks involved. Often the “mechanics” of the VPN are addressed by a vendor, but it is important to realize that a secure VPN should be a full VPN Solution.[1] This includes things such as risk analysis, a well thought out security policy, user training and education and ongoing monitoring. There is a wide variety of choices available – from vendor specific to open source technologies. There is no one VPN solution that will fit every organization’s needs, and in fact an organization may choose different solutions to meet varying requirements. When you look at all of the topology, connection types, protocols, authentication methods, the options become overwhelming. When you are evaluating VPN solutions, there are some fundamental issues that need to be addressed: cost, performance reliability and security. Security should be the one uncompromising piece of any VPN decisions. It doesn’t matter how fast or inexpensive the solution if the risks outweigh the benefits.

The importance of proper planning and development of specific policies and guidelines cannot be overstated. One outcome of thorough planning is to make the selection process easier. Eliminating solutions that do not meet your requirements can significantly reduce the choice of viable options. Whichever solution is selected, it should ensure Confidentiality, Integrity and Authentication.

Risk Overview

While a VPN solution can provide benefits to an organization, it must be recognized that it does not come without risks. Often a network, particularly for a small organization, is a well known entity and access is tightly controlled. The infrastructure has predictable availability, performance and security. Security is typically controlled

by physical access and probably network perimeter security consisting of a firewall. Expanding the network outside of the single physical location opens the private network to access outside the physical perimeter.[2] Deploying a VPN opens three locations for access and attack.

1. The VPN server where users connect to the private network. This gateway is an attractive target for denial of service as well as intrusion into the private network.
2. Data traveling across the public network. Data in transit is subject to threats such as spoofing, hijacking, sniffing and man-in-the-middle attacks.
3. The client machine used to access the private network. In all likelihood the easiest target in the system.

A VPN deployment needs to look at each of these points and understand how the selected solution will protect each one.

Planning

Proper planning is a requirement for successfully deploying a secure VPN solution. These documents will be used at every step in planning, deploying and maintaining your VPN policy and will consist of your risk analysis, organization's security policy and your specific VPN policies. If these documents already exist in your organization, ensure they are followed. It may be necessary to add to or modify them to include VPN and remote access.

If your organization does not have a security policy or it does not cover the use of a VPN, your first step will be developing or extending your security policy. There are many sources that can assist you with developing your security policy. While every organization is different in regard to its security policy, there are some items that need to be addressed in regard to a VPN. In general the first step is to identify the items that are at risk and what they are worth, then identify methods that will protect those assets. If you have not performed a risk analysis, there are many good resources to help you accomplish this important task.

After the policies are in place, you can begin identifying the resources that will be accessed remotely. This list of resources to be accessed can help guide the decision about whether or not to deploy a VPN as well as what would be the proper solution. If you determine that people only need remote access to their email, it may be cheaper and better to set up some method of web-accessible email rather than a full VPN deployment.

The risks and how they will be mitigated after the deployment of a VPN need to be fully addressed. Perhaps prior to the deployment of a VPN, security of files located on a server are addressed by limiting physical access to the building and the use of a firewall to protect the perimeter. After the VPN is deployed, physical security may prove to be impossible – is the file being copied to a client machine that is located at an employee's home or perhaps on a laptop that will be traveling throughout the world?

For your VPN policy, there are some specific topics that will need to be addressed. Ideally you will develop a document that spells out your remote access policy. This separate document can be distributed to end users that will be using and implementing the VPN technology. This document should include appropriate use as well as ramifications of improper use. This is reviewed in more detail at the end of the document

Key VPN Policy Items

Some of the key items that should be included in the VPN policy that relate specifically to a VPN deployment are listed below.

Identification and Authorization

These are functions that identify and authenticate the users as legitimate and authorized to access your network resources. The goal is to create a connection only for users that have been authorized to connect to the network

Part of the policy may be listings of groups and users and what they need to access. For example, a sales rep may need access to his email and the company price list. A system administrator may need access so she can perform maintenance on the network. This would be a high risk activity that would require a higher level of security than the sales rep. At first it might seem to make sense to have the same security level for all users; however, that may not be prudent. The technical expertise and amount of training will probably be higher for a system administrator. That can translate into a solution that is more technically advanced. It also implies that the administrator should have a better knowledge of “safer computer”, such as email best practices and web surfing strategies.

Access Control

You need to have methods that control which information or assets the user can access after being properly authenticated. More than likely the organization already has these controls in place. An example would be an organization using Active Directory with protected file structure. Does the VPN system need to integrate with the existing system or will it be a separate system? In order to develop an effective policy, the organization must have an understanding of or mechanism for classifying documents, how sensitive they are and which documents need to be protected. Decisions must be made as to which documents can be accessed through the VPN. This list may change for different VPNs. For example, a site-to-site VPN may not have this restriction, whereas a client-to-site VPN may not allow financial documents to be transmitted. These restrictions can either be programmed in or simply be a written policy. It is also important to define acceptable use of a resource.

Accountability

The organization needs to have processes in place to make sure that the policies are being followed. Recording and logging security related events is a key piece.

Developing policies and procedures on how you will monitor and audit remote access is critical.

Object Reuse

It is important to put mechanisms in place so that information cannot be reused or scavenged by unauthorized users after the legitimate use by another user. For example, when a legitimate user has been on the system using a public computer. Was login information retained by the web browser? Was a document downloaded then printed by someone in an "internet café"?

Another example is stolen equipment. Is there a reporting process so that any compromised accounts are immediately locked or reset? It may also prove helpful to use file encryption such as EFS on computers used outside the office.
Another concern is the disposal of surplus equipment – are hard drives adequately wiped before being disposed of or donated?

Accuracy

When remote users views data via the VPN, they assume that the information is secure and what they are viewing is in fact what was transmitted.

Reliability of service

Business needs should dictate the minimum failsafe and redundancy requirements for the VPN. These requirements can vary for different users and VPNs. For example, a site-to-site VPN may be a more critical connection than a site-to-client connection.

Completed Security Policy

When finalizing the security policy, keep in mind that it must be attainable and effective against the identified risks. The policy must be something that can be shared and understood by the people it impacts. This is where a separate policy for end users is a benefit. Expecting an end user to digest the organization's full security policy or pick out what applies to them is impractical. In the end, the persons connecting via VPN are responsible for following policy. Technology itself cannot ensure security – end users with proper training and understanding of the policy are needed to be successful. A well written security policy can be used as the basis for a good "security culture".[3]

A VPN security plan also needs to be specific – not just a group of high level policies. For example, a security plan may state "AV software must be updated regularly", but a VPN policy should address how this will happen. There should also be a specific policy for each solution – requirements for a site-to-site solution will be different from a client-to-site solution. In the final analysis, securing the actual remote system is easy – you need effective policies to provide good security. After it is completed, the policy should be thoroughly reviewed to ensure that it meets the objectives of Confidentiality, Integrity and Availability.[3]

Once the security policy and VPN guidelines are in place, you can begin to look at the myriad solutions available and verify that they can meet the criteria you have set. If a favorite solution cannot meet one or more of the criteria set in your policy, it should be removed from the list unless there is consensus that there is a compelling reason to change the policy. If that decision is made, the written policy must be changed.

Physical Connection

Most likely your VPN will use some sort of an existing public network to connect to your organization. Common methods of connecting are Digital Subscriber Lines (DSL), Cable Modem, Integrated Services Digital Network (ISDN) and wireless. Connections can also be used together. For example, a client is staying at a hotel and uses the wireless network to access the hotel's DSL connection to the internet. The two biggest security risks associated with the physical network are sniffing and redirection. The difficulty of sniffing a network depends on the connection type. An unsecured wireless connection is a trivial connection to sniff while a T1 connection is more difficult. In order to sniff the network traffic on a physical wire, you need to have either direct or close access to the wire that is carrying the traffic.

Gaining direct access to the wire can be done by installing some sort of sniffing software on the computer using the VPN, on a computer at the ISP that is carrying the traffic, by compromising another computer along the data path, sniffing traffic as it moves across equipment such as a switch or physically installing a tap. If you only have close access to the wire, often redirecting can be used to sniff traffic.[4]

There are several ways to achieve redirection.
ARP poisoning – there are several ways to use ARP to redirect traffic past your computer. You can send out an ARP packet that claims you are the router. This will likely flood your computer because everyone will think you are the router. Another method is to send out an ARP packet claiming that you are a different machine.

ICMP Redirects - Many operating systems support ICMP Redirects where you tell a machine to forward packets through you rather than the local router.

ICMP Router Advertisements - A different variation of ICMP that does much the same as redirects. It convinces a machine that you are the correct router.

For all of these to work, you have to configure your machine to forward all traffic to its correct destination. The best defense against sniffing by any method is the use of secure encryption for all data sent via VPN. Additionally some VPN protocols are less susceptible to redirecting. [5]

The choice of which technology will be used to make the physical connection often has less to do with security concerns and more to do with what is available in a location. Your organization may feel that DSL is more secure but cable broadband may be the only technology available at the location. When planning a deployment, it

is important to know the vulnerabilities of what connection type is selected, and then be certain that proper security measures can be put into place.

Topology

Where the pieces of the VPN solution reside on the network can have profound security implications. At some point the secure tunnel must have a beginning and an end. Once data is outside the tunnel and unencrypted, it is susceptible to successful sniffing and interception and redirection. This means that you definitely want to terminate the tunnel in a location that puts it beyond the eye of unauthorized users.

Often the tunnel will terminate at the remote access server. In order to provide maximum protection, this server will be located inside the firewall. While this provides additional protection for the server, there is a definite downside. All of the traffic inside the tunnel effectively bypasses the firewall and the security it provides. For example, assume the client machine has been compromised and is generating traffic that in all likelihood you would not allow inside your firewall because of the threat to your network. Once the client connects, the infected machine is considered trusted and has full access to your network and any traffic is encrypted and set past your firewall. While it is true that any machine inside the firewall can become an attacker, the risk is greater for a machine that "lives" most of its life outside the normally secured border.

There are a few ways to minimize or eliminate this risk. One is to have the tunnel terminated before the firewall so all traffic has to clear the firewall. You must be aware of where this termination occurs so that unencrypted traffic is not visible to the outside. This problem also points to the importance of end-point machine security, which will be covered later.

Some vendor solutions use a gateway that restricts traffic between the tunnel and the network. The final solution to the topology layout will involve working closely with whatever VPN solution is chosen and the hardware used to secure the network.

VPN

With your security policy as a guideline and your choice of physical connection made, you can look toward the technologies that you will use to actually construct your VPN. This can become a confusing process because of the different protocols and technologies involved. A VPN is actually a combination of different protocols and standards that are combined to build the virtual circuit that will be used to transport data. The major components pieces of a VPN are:

- The tunnel that will be used to connect users or sites over the public network.
- Authentication and authorization to insure who is connecting to the network, and verifying the resources they can access.
- Encryption of data to protect against interception.

When deciding on what solution to use, it is important to verify that each component as well as the completed VPN will meet the requirements put forth in the security policy. If the security policy dictates that all traffic meet certain encryption standards, you must ensure the protocol chosen is able to meet the requirements. The total VPN must also be analyzed in addition to each component

Tunneling

Tunneling is a process of using an internetwork infrastructure to transfer data for one network over another network. The tunneling protocol encapsulates the frame in an additional header. The payload can also be of a different protocol. For example, IP/SPX packets can be encapsulated, then routed over an IP network such as the internet. This header also contains routing information so the encapsulated payload can traverse the internetwork. When the encapsulated packet reaches the other end of the tunnel, it is de-capsulated and the original frame is routed to its final destination. This whole process of encapsulation, transmission and de-capsulation is what makes up the tunneling process. The path through which the encapsulated packets travel is called a tunnel. For a tunnel to be established, both the tunnel client and the tunnel server must be using the same tunneling protocol. [6]

The internetwork can be any network including an existing private network. Most VPN solutions are intended to run over public networks such as the internetwork. For remote access, using the internet for the internetwork over which to operate the VPN represents the biggest cost savings and provides the most flexibility for user access.

There are a variety of network protocols implemented specifically for use with VPN tunnels. Some are based on standards (usually emerging standards); others are proprietary.[2] Often, vendors will take a standard and modify it to provide what they believe is the best solution. Not surprisingly, for either category the newer standards tend to provide better security. It is beyond the scope of this paper to look in depth at even the most common protocols in use. Also, the vulnerabilities and security concerns vary with implementations and versions. Instead, I have tried to provide a checklist of sorts with some questions to be asked as well as some of the more common exploits.

- Is the technology actively being supported? With the seemingly endless parade of exploits, it is important any protocol chosen be updated in case a vulnerability is found.

- Does the protocol support encryption to provide the data security deemed necessary? Some protocols may only support 40 bit encryption. Your VPN policy should provide guidance on encryption strength needed.

- Does the protocol support the authentication protocol that is desired? If using two factor authentication and using EAP for authentication, the tunnel protocol must support it.

- Does the protocol support computer authentication as well as user authentication? This can provide additional authentication security.

- Will the protocol work across the existing internetwork? Some protocols will only work over an IP networks while others will work with non-ip networks such as ATM, Frame Relay and X.25

- Does the protocol provide adequate data integrity? This may take several forms. One ensures there is no data modification between sender and receiver. Another confirms that the data is actually sent by the user who claims to have sent it. This protects against man-in-the-middle attacks and redirection.

- Does the protocol provide protection against simple replay attacks? If an attacker is able to sniff the network traffic are they able to simply send the same data to the server later and trick it into thinking the legitimate user is requesting access?

- Is there a need for keys to be defined and managed?

- Can the protocol run scripts or otherwise perform checks on the client machine before completing authentication? In an attempt to try and verify the remote systems integrity, technologies are being put into place to check on virus software status, as well as other conditions prior to fully authenticating a remote machine.

- Is there a client that needs to configured and managed on the remote machine? Often times, a remote client has features making it possible to establish requirements such as the client have antivirus software or personal firewall software installed in order to connect to VPN gateway

- If NAT is in use, will the selected protocol support it?

- Will the protocol work with existing firewalls?

- Are there clients available and maintained for all expected platforms that will be used?

- When you select a protocol to use, you must also specify which version. For example, earlier versions of Microsoft's PPTP implementation have well-known exploits. [7] For some protocols exploits involve forcing the protocol to use an earlier or less secure implementation. For example, you may want to use 128 bit encryption, but the protocol supports 40 bit encryption. If there is a way to force the client or server to "downgrade" to 40bit encryption, it may become a target.

Your security policy and the differing requirements for your organization will create a longer list than presented here. It is important to carefully analyze each choice to make sure it meets your requirements, particularly the security requirements as defined by your organizations security policy.

Encryption

Many of the tunneling protocols do not in and of themselves provide encryption, but instead rely on other means to encrypt the data. Because potentially sensitive information will be traversing public networks, it is import to protect the confidentiality of the data while in transit. There are many different algorithms in use. Most people are only concerned with key length – the idea that the longer the key, the more secure the encryption. While this is often the case, there are other factors that play a role in the overall strength of an algorithm. Evaluating the security of an encryption implementation is tricky – especially if it is a proprietary solution. I would recommend reviewing http://www.schneier.com/crypto-gram-9902.html#snakeoil and http://www.interhack.net/people/cmcurtin/snake-oil-faq.html for additional information that can prove useful when reviewing vendor's claims. Again, be sure that whatever encryption method is chosen will meet the requirements of your security policy.

Authentication

One of the most important parts of security for any VPN solution is identifying the user. There are several types of authentication available. Not all varieties will work with all tunneling protocols or operating systems. Authentication methods fall into three main categories:[8]

1. Something you know – password or PIN.
2. Something you are – a personal trait such as fingerprint. Usually referred to as biometrics.
3. Something you have – a key or token.

Each method has its own security risks and can be compromised. Some authentication methods are subject to playback attacks where network traffic is sniffed and is then replayed. The server does not know whether or not the legitimate user is logging on or not. Some implementations do not protect against repeated "trial and error" attacks. The ease with which they can be compromised varies with the authentication method and its implementation. The cost and complexity of deployment vary with the different methods.[8] Once again, the policy developed is a critical guide in selecting the authentication method to be used.

Passwords can be cracked, sniffed, stolen or learned through trickery such as the increasing number of phishing attacks. A password which is too simple is subject either simple guessing or dictionary attack. If the password is too complex, the user will have to write it down or otherwise save the password. Using password phrases allow increased password length but allows for easier memorization.[9] It is important that a password policy be part of your remote access policy. If you already have a password policy in place for your organization, it might suffice for your remote users. Another problem is that when a password is compromised, the user often is not

aware of it. This means the attacker can have long term access to the account without the user being aware.

Something you are – or biometrics is not a failsafe method. “Cloning” can be used against some devices. For example, showing the picture of the face to a facial recognition device can fool some systems. Methods have also been used to fool fingerprint and iris scanning devices. One of the challenges with biometrics is when they are compromised, how can they be changed?

While it may be more difficult, tokens are not immune to compromise. One advantage of a token is the user knows fairly soon if it is missing. It is not always necessary however to steal the token. Magnetic stripe cards can be copied using readily available hardware. Some USB devices can be compromised so the “secured” data can be read and used by the attacker.

To help reduce the risk of a single authentication factor from being compromised, it is possible to implement two factor authentication. An example of a single factor authentication is the standard user name and password supplied at login. This may be strong enough for low value data. Two factor authentication is stronger, but more expensive to deploy. A simple example is an ATM Bank card. Separately, the PIN or card do not allow access – the user must have both pieces to successfully authenticate with the cash machine. Common two factor authentication methods used with VPNs are Etokens, smart cards, PKI and digital certificates and biometrics.[8] In order to decide which methods to deploy, refer back to the VPN policies to ensure the methods chosen meet your requirements.

In addition to user authentication, it is also possible to require machine authentication. If a password is compromised and logon is attempted from a different machine, access is denied. Conversely, if a machine is stolen it can be blocked from gaining access to a network.

As stated previously - when evaluating your choices make sure they meet the requirements put forth in your VPN policy.

Authorization

Authorization provides the ability to limit the networks services and resources to different users. The method used will be tied closely with how you chose to authenticate users and what systems you already use on your network to control resource access. For example, if using Active Directory to manage resources and users, this will be the most efficient means of providing authorization for remote users. Once again, your VPN policies will be your guidelines.

Auditing and Monitoring

Auditing and monitoring are crucial for the proper administration of the VPN solution. Auditing and monitoring requirements should be developed during the planning

process in order to verify that the solution implemented can meet the requirements. For example, an administrator may need to know who connected to the system, for how long, and what resources they accessed. Unusual activity may indicate system misuse or other system problems. Real-time monitoring of equipment showing unusually high activity may show equipment failures or misuse. Specify how event logs will be recorded and what reports will be required.

Depending on monitoring and reporting requirements, it may be necessary to deploy a separate monitoring server that records the necessary data. An example would be deploying a RADIUS server not used for authentication, but only used for monitoring activity.

Simply having the data available is not sufficient. Plans must be put in place to monitor the system on an ongoing basis. In the event of a system compromise, this data will be critical in determining how the attack occurred and what data may be compromised.

After a solution is selected and deployed, monitoring must be done to keep track of any vulnerabilities or updates made available. Unlike a machine that might have additional layers of protection such as a file server VPN traffic and servers are exposed on the public network and are open to attack. Be vigilante in ensuring all of the pieces are kept up to date to minimize their exposure to attack.

Securing Endpoint Machines

With a VPN solution, the most difficult part to control is the client's machine. When developing a VPN policy, it is important to include policies regarding the user as well as the computer they will use to connect to the main site. Combination of a lack of easy physical access by the technology worker and often without a fulltime connection the remote machine is challenge to keep secure. Only a combination of technology, user education and properly written and enforced policies allow for any hope of success.

Technology

Technologies that attempt to secure the endpoint are rapidly evolving. There are two general approaches. One is an attempt to "validate" a machine before it can attach to a network. This process can involve checking items such as Anti-Virus are up to date, service packs and patches are installed as well as other criteria that are defined by the organization. Once the criterion is met, the machine is allowed access to the network. The idea being that if a machine is protected to the current standard of the balance of the machines on the network it is not a greater risk. In theory, it is believed it is not infected or vulnerable to known exploits.
The second approach is to block undesirable traffic – intrusion prevention. Both techniques are relatively new and have their own pros and cons. Defense in depth will probably see a blending of the two approaches in the future.

In addition, it is important to specify minimum requirements for the remote machine. While the requirements are probably similar to the other machines on the network, they will also have additional criteria in order to provide adequate security.

Operating System Requirements [10]

When selecting operating systems that can be used for remote access there are several considerations to keep in mind.
Is the operating system still supported by the vendor? If a secure operating system cannot be maintained it should not be allowed to connect to the organizations network.
Is there a VPN client available? For example, if you have chosen to deploy L2TP + IPSec, is there a client available that is being maintained?
Does the Operating System support the other required software?
Is virus protection available?
What if you chose to deploy a software firewall – is there a version available?
Can you effectively manage the machine remotely? In all likelihood, gaining physical access to the machine will not be practical.

Personal Firewalls

Unless a remote machine is always connected to the remote network, there will be times it will be visible on the internet. For a dial up VPN connection, the time period might be very short, but the machine will still need to be protected. For an always on connection, the firewall becomes a critical piece in protecting the organization. A firewall can help prevent Trojans, hijacking of data and the introduction of "backdoors" on the client machine that can be used against the trusted network.

In addition to specifying which firewalls to use, configuration should also be defined. Is there certain traffic that will be blocked – such as file sharing?

Anti-Virus Software

Two primary considerations when deploying anti-virus software for remote users is how to keep the signature files updated and verifying that this is happening timely and correctly. There also needs to be a method to manage and ensure the software is properly configured and is working correctly. Simply doing an initial install is not a guarantee of continued protection.

Password Protection

Password cracking software is widely available so it is important remote users follow well thought out password policies. Policies can also address what passwords can be stored on the remote system.

Policy and Education

Technology alone cannot mitigate all risks. The proper policies and user education is a critical component. Because they have physical control over their machine local users are, in effect, remote "administrators". There are several key areas to be

addressed by your organization's VPN policies. These must be clearly communicated to the end users.

If the organization provides a computer, who is allowed to use that computer? Are family members allowed to use the computer, and are they allowed to install their own software on the computer? In addition, if the organization is providing connectivity such as a DSL connection, who is allowed access at the client's end and are there guidelines for its use? With the ease of setting up home networks, it is easy to share a common connection giving little Johny the opportunity to use his computer and the companies bandwidth access to all the music he can find.

An even more complicated scenario is when a personal computer is used to connect to a company network. Are there requirements for virus protection, operating system, patching requirements, etc? How are these requirements enforced and who supplies the items needed to meet the requirements? This can mean items such as antivirus software, hardware firewalls, operating system upgrades and more. If there are software conflicts who is responsible for providing end user support. Most organizations would prefer to avoid the potential quagmire and simply provide access and machines for personal that require remote access. [10]

Another option would be to provide something like web access to email so people who do not need access to the organizations resources remotely can check their email.

Conclusions

In order to mitigate the risk of, and reap the benefits of a VPN, the vital first step adequate planning consists of risk analysis, security policy, VPN policy and a needs and benefits assessment. These documents should be used in all decisions relating to vendor and protocol selection.

The weakest points of any VPN are typically the two endpoints, in particular the end users machine. Technology alone cannot mitigate the risk. End user education and an effective and enforceable policy are necessary.

Virtual Private Networks can provide real advantages to many organizations. It is important to look past the "sizzle and hype", however, and recognize there are inherent security risks no matter what system is deployed. The organization must be aware of these risks so as to make an informed decision, whether they are willing to accept the risks.

References

1) Jenner, Simon. “Virtual Private Networks (VPN) the insecure solution”. 12 July 2003. URL:http://www.trinitysecurity.com/reference/bulletin/Trinity-VPNs%20The%20insecure%20solution.pdf
(19 June 2004)

2) McDonald, Christopher. “Virtual Private Networks: *An overview”. URL:* http://www.intranetjournal.com/foundation/vpn-1.shtml
(19 July 2004)

3) van der Walt, Charl. “Introduction to Security Policies, Part One: An Overview of Policies”. 27 August 2001. URL: http://www.securityfocus.com/infocus/1193
(19 June 2004)

4) Graham, Robert. “Sniffing (network wiretap, sniffer) FAQ. Version 0.3.0. 15 January, 2000. URL:
http://www.linuxsecurity.com/resource_files/network_security/sniffing-faq.html
(4 June 2004).

5) Whalen, Sean. “An Introduction to ARP Spoofing” Revision 1. April, 2001 URL: http://packetstormsecurity.org/papers/protocols/intro_to_arp_spoofing.pdf
(4 June 2004).

6) Multi-Tech Systems. “VPN Technology Guide”. 13 January 2004. URL: http://www.multitech.com/DOCUMENTS/Tutorials/tech_guides/vpn/page1.asp
(7 July 2004).

7) Schneier, Bruce. “Security Flaws Found in Microsoft’s Implementation of Point-To-Point-Tunneling Protocol (PPTP)”. 1 June 1998. URL: http://www.schneier.com/pptp-pressrel.html
(4 May 2004)

8) Rainbow Technologies, “Two-Factor Authentication – Making Sense of all the Options. 2 February, 2002. URL: http://www.itsecurity.com/papers/rainbow2.htm
(7 July 2004)

9) Gralla, Preston. “How Passwords and Authentication Systems Work”. How Intranets Work. 1996 URL:
http://thor.info.uaic.ro/~busaco/teach/docs/intranets/ch18.htm
(19 June 2004)

10) DISA Field Security Operations. “Secure Remote Computing Security Technical Implementation Guied”. Version 1, Release 1. 14 February 2003. URL: http://csrc.nist.gov/pcig/STIGs/secureremotecomputing-stig-v1r1-021403.doc.
(10 July 2004)

Microsoft. “Remote Access VPN Security Considerations”. 2004. URL: http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sag_vpn_us07.asp
(5/4/2004)

Shinder, Deb. “Comparing VPN Options”. 10 June 2004. URL: http://www.windowsecurity.com/articles/VPN-Options.html
(19 June 2004)

Poonam Arora, Prem R. Vemuganti, Praveen Allani. “Comparison of VPN Protocols – IPSec, PPTP, and L2TP”. Fall 2001. URL: http://security.ittoolbox.com/browse.asp?c=SecurityPeerPublishing&r=http%3A%2F%2Fece%2Egmu%2Eedu%2Fcourses%2FECE543%2FreportsF01%2Farveal%2Epdf
(10 June 2004)

Rudis, Bob. “Protecting Road Warriors: Managing Security for Mobile Users (Part One)”. 21 April 2004. URL: http://www.securityfocus.com/infocus/1777
(10 June 2004)

Adtran. “Understanding Virtual Private Networking”. September 2001. URL: http://www.adtran.com/adtranpx/Doc/0/EU0GPR0PEFB139RF038BE81ID8/EU0GPR0PEFB139RF038BE81ID8.pdf
(4 May 2004)

VPN Consortium, “VPN Technologies: Definitions and Requirements”, July 2004. URL: http://www.vpnc.org/vpn-technologies.html
(19 July 2004)

Golen, Pawel. “Virtual Private Networking”. 14 August 2002. URL: http://www.windowsecurity.com/articles/Virtual_Private_Networking.html
(19 June 2004)

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event