Global Information Assurance Certification Paper

Deploying a VPN Client with Security in Mind – A Case Study
GSEC Practical Assignment Version 1.4b
Joe Gonzalez
12 December 2002

Abstract

Virtual private networks (VPN) are widely deployed. Much has been written about the benefits of VPN and how to configure a VPN termination device, or switch, for both branch-to-branch and employee remote access applications. However, not much has been written about the VPN client software itself – that software that installs on a user's home computer and connects to the switch – in particular, the security aspects surrounding its usage and deployment.

This case study describes the subject company's efforts to deploy a VPN solution with emphasis on the VPN client software instead of the configuration of the switch. It discusses the risks identified with the VPN client software and the steps taken to mitigate the risks. Finally, it makes recommendations others can use to deploy VPN client software with security in mind.

Description of Problem (before snapshot)

Background

The subject company operates in the health sector with 1,000 employees at its head office complex and a small number of 2-person offices located nationally, in Southeast Asia, Central and South America and Europe. The company's dial-in solution permits access to data files, e-mail, the mainframe and corporate intranet. In addition, special groups, such as board members and business partners, can access specific services.

The company Executive strongly supports a "default deny" computing stance. For example, the corporate desktop features a secure operating system, restricted access to the C: drive and no installed compact disks. Internet content is scanned. Java and ActiveX are blocked as are executable files attached to e-mail messages. The network is protected using firewalls, intrusion detection and a DMZ. Host computers are regularly patched and logs captured to a secured log server. Employees working from home must have installed anti-virus and firewall software. Policies outline acceptable practices for e-mail, internet access, password usage and handling of corporate files. Employees must sign a form agreeing to conduct their affairs in accordance with policy.

The dial-in solution, while satisfactory for a time, began to pose a number of problems. First, employees working from home, and quickly adopting high-speed internet access, were increasingly frustrated by having to switch to slower dial-up modems to connect to corporate resources. Secondly, employees connecting from worldwide regional offices were incurring long-distance costs of $12,000 per month, per office. Thirdly, once a dial-up connection was made, it was not possible to track through logs if the caller was an employee, board member or business partner. Finally, corporate data was being transmitted electronically in plain text making it vulnerable to breaches in confidentially, integrity and authentication.

Given increased pressure from employees using high-speed internet access and the opportunities to avoid long-distance costs and encrypt transmitted data, it was determined that a virtual private network (VPN) solution should be explored. Improved remote access for employees, cost-avoidance and security are generally considered the most significant VPN benefits.

The Nortel Contivity 1500 switch was the selected product due to past relationships with the vendor, the product's excellent reputation and its reasonable cost.

The project team consisted of three experienced networking professionals with the less-experienced author acting as the project leader responsible for project management, research, development and implementation. Project team

members evaluated options and provided in-depth networking and security expertise.

In the research and development phase of the project, a Contivity 1500 switch was configured in a lab environment. The objective of the phase was to become familiar with the switch, its features, and how it operated. Architectural alternatives, such as whether to place the switch in front of or behind a firewall, were assessed. The switch was scanned from its public interface to assess what someone attempting a break-in could see.

The VPN client software was examined by installing it on a laptop computer and connecting it directly to the switch's "public" interface - the Internet interface - using a crossover cable. Later, testing would continue with the switch connected to the Internet and the laptop to an Internet Service Provider.

During the examination of the VPN client software, a number of client-specific risks were identified. These risks and the options available for mitigating the risks are the subject of this document.

Identified risks

The following client-specific risks were identified during the research and development phase of the project.

1. The VPN client software displays vendor information.

The VPN client software displays vendor information as follows:

- "Contivity VPN Client" and "Nortel Networks" appear on dialogue screens;
- "Nortel Networks" appears in the computer's Start menu;
- "Nortel Network" appears as the folder name under the "Program Files" folder.

From a security perspective, the information gives a hacker an immediate advantage because the hacker's information gathering phase has been made easy. Having gained access to an off-site computer with the VPN client software installed, the software now provides a vendor name and the IP address (or DNS name) of the switch – the target to attack. Attacks can now be directed at the vendor's known vulnerabilities.

2. The VPN client software must be distributed to employees.

Although rather obvious, this observation did raise two questions. First, how should the software be distributed to possibly hundreds of employees? And secondly, how should the software be returned to the company?

From a security perspective, the concern was that the software, once provided an employee and installed on a computer, would remain available to anyone who could gain access to it before it was returned to the company, if returned at all. It could then be installed on a computer not owned by the employee and used to attack the company.

The software could be distributed on floppy disk, however, at over four megabytes, it was too large for one disk. Using a product such as WinZip to create a self-extracting compressed file to overlapping floppy disks was technically possible. Placing the software on compact disk was also possible. However, both options would require that someone creates the disks or CDs, distribute them to employees and then manage the inventory. This process would result in increased administrative cost and could become complex as newly released software was subsequently made available to employees. Clearly, this task could become onerous, especially for a company of 1,000 employees.

3. The VPN client software requires configuration after installation

After installation, the user must create a profile prior to creating the VPN. The Profile wizard requires the user to supply authentication information. The information is used by the Internet Key Exchange protocol to authenticate devices and users.

For example, the user must know if authentication will be based on user name and password, digital certificates or group. If by digital certificates, the user must select Entrust, MS CAPI or VeriSign. If by group, the user must supply a group name, password and authentication type (Challenge Response Token, Response Token only or Group Password Authentication).

From a security perspective, this meant that authentication information had to be securely communicated to employees. If communicated by e-mail, the employee would likely print the e-mail. If communicated verbally, the employee would likely write the information on paper. In either case, a paper copy of the information could remain available for any one to read after it was used to create the profile. Someone working from the home computer could start the VPN software and then use the information to impersonate the user. If modified, the new authentication information would again have to be communicated to employees.

4. The VPN client software can be modified after installation.

Once installed, someone could modify the VPN client software.

From a security perspective, this could lead at best, to a support call because the employee's credentials are being rejected to at worst, a hacking attempt by someone who has manipulated the software's parameters and is attempting to log in.

5. VPN exposes corporate information assets to the Internet

Since VPN uses the Internet to connect to the company network, corporate information assets are exposed to the Internet.

From a security perspective, a compromised home computer could be used to gain access to corporate resources. Particularly worrisome are remote administration Trojan viruses. These types of viruses allow an intruder to start and use applications installed on the compromised computer, such as VPN client software. Other type of malicious software could enable someone to view data stored on the computer or eavesdrop during a VPN session. This Internet threat was not present with the existing dial-up solution.

6. VPN client software offers a "Save Password" feature.

The VPN client software provides a user with the option of saving a password. This option is frequently provided by the Windows operating system for other applications, particularly when using Internet Explorer to access secure Internet sites. Now, the VPN client software itself was providing the option.

From a security perspective, the risk was that employees would permit the VPN client software to save the password. Then, anyone who could turn on the computer, access the Internet and start the VPN client software would be able to connect to the company. Employees using secure operating systems would partially mitigate this risk because someone would have had to already log into the computer to gain access to the VPN software. However, most users use insecure operating systems or do not employ strong usernames and passwords in the home. Therefore, the risk is only partially mitigated.

The company had addressed this issue procedurally - users were instructed to disregard the option and not save passwords within software. However, this approach was weak because it could not be enforced or audited.

7. Inability to segregate users.

A problem with the dial-up solution, the inability to segregate groups of remote access users (employees, Board members and business partners) remained a security issue. Now, access via VPN would be added to dial-up access further compounding this problem. From a security perspective, there were two issues to consider.

First, the current dial-up solution permitted any group to access any application with only the end-application's built-in security to authenticate users. For example, a business partner having connected by dial-in or VPN could then attempt to access mail or intranet servers, services intended only for employees. Only the mail or intranet server's domain security would prevent partners from gaining access (since partner user names did not have domain rights to these servers).

Secondly, when viewing logs it was not possible to distinguish an employee from a Board member from a business partner because only the remote user's IP address appeared in logs. Therefore, it was not possible to determine by an examination of logs if, for example, an employee was attempting to access a server reserved for Board members.

8. There is uncontrolled access to workstations

VPN (and dial-up) permit access to corporate resources from uncontrolled workstations in off-site locations such as the home, airports or hotels. These workstations are not subject to the same access controls used in the workplace. For example, in the workplace, the usual practice is to prevent access to workstations using locked doors, building security or a secure operating system.

From a security perspective, the risk is that anyone gaining access to a workstation can attempt access to corporate resources. This could happen, for example, if the home worker left a logged-in workstation unattended for a period of time.

9. VPN implementation risked increased administration cost

Users connecting with VPN were required to authenticate with their user name and password. These credentials had to be maintained in a database that could be accessed by the switch. From a security perspective, this meant that another corporate repository of user names had to be established and safeguarded. The repository would require on-going administration as users were added, changed or deleted. Access rights would have to be assigned to user accounts, ownership of the repository determined and administrative procedures updated. For example, Personnel and network administration procedures would

have to reflect that a new employee's user name would have to be added to an additional repository to permit VPN access.

Mitigating identified risks (during snapshot)

After identifying the risks posed by VPN, an in-depth review of the VPN client software was conducted with particular attention to the elements that could be customized. It was discovered that customizing the VPN client software and invoking certain switch features would result in a mitigation of identified risks. This section presents those elements by identified risk.

The Contivity 1500 client software utilizes three files that can be customized: Baynet.tbk, Setup.ini and Goup.ini. The Baynet.tbk is used to configure a user profile. It has eight customizable elements. The Setup.ini and Group.ini have 25 and 3 customizable elements, respectively. After installation, the Baynet.tbk files remains as the user profile. The Setup.ini and Group.ini files are deleted, their elements having been stored in the computer's registry.

1. The VPN client software displays vendor information.

This risk concerned providing a hacker with an immediate advantage by having viewed the vendor name in the software's dialogue boxes or file system structure. This risk can be mitigated in two steps.

In the first, two parameters are modified in the Setup.ini file replacing "Nortel Networks" with a generic term such as "VPN". The two parameters are: [1]

Folder Name=VPN	the folder name in which files are stored
Product Name=VPN	the name appearing on the computer's Start menu.

In the second, the vendor name is removed from dialogue boxes. This is accomplished by replacing two bit map files with equivalent files having no vendor names. The files to replace are eacdlg.bmp and eacstats.bmp. The specifications of the bit map files and their folder placement for installation are presented in the cited document.[2]

2. The VPN client software must be distributed to employees.

This risk concerned how to distribute the VPN client software to employees. Distributing the software by floppy disk or CD were rejected because of the effort required to create and manage the inventory of either medium. The medium selected for distributing the VPN client software was the web, specifically, the company's public web server.

The public web server operated under Internet Information Server (IIS) and was part of an NT domain in the company's DMZ. The VPN client software was placed in a folder of the web server. An NT domain group containing

[1] Nortel Networks, p.28-29, p.35.
[2] Nortel Networks, p. 40-41.

employee names was given the NTFS read right to the folder. A virtual folder was created in ISS and linked to the folder holding the VPN client software. The virtual folder's security was changed from "Anonymous" to "Basic" and Secure Sockets Layer (SSL) was invoked.

To obtain the VPN client software, employees visit the web site using their off-site computer, specifying the virtual web folder name in the web address (for example, www.mycompany.com/vpnclient). Employees are prompted for their user name and password because SSL is invoked for the web address. The credentials are verified to the domain's primary domain controller. If accepted, the VPN client software can then be downloaded to the home workstation via an SSL session.

The scenario was replicated to distribute customized VPN client software to Board members and business partners. The VPN software for each group was placed on the web server in separate folders. The NTFS read right was assigned to the respective domain groups containing the user names of Board members and business partners. A unique IIS virtual folder name was created and linked to the folder. The virtual folders' security was changed from Anonymous to Basic and SSL was invoked. Board members and business partners were able to visit their respective web links (www.mycompany.com/board or www.mycompany/ partners) and download the VPN client software after their credentials were authenticated.

Nortel's Contivity VPN client software numbers some 12 files. To ease the distribution of the VPN software client for users, Nortel suggests creating a single self-extracting executable file using the software "Package For the Web" available from http://support.installshield.com/pftw.[3] This suggestion was implemented and proved beneficial because users had only to download a single file.

In addition, the Package for the Web software permitted the addition of a password to the self-extraction process. Therefore, a password was required to begin the self-extraction. Passwords corresponding to the respective customized client software were distributed to employees, Board members and business partners using separate procedure documents. Although not the strongest way of delivering a password, this approach was chosen because the intent was to prevent an unauthorized person from the general public, who had successfully obtained the software from the web site, from being able to start the installation.

This scenario mitigated the following risks.

- The software was accessible from the web site only to authorized users by virtue of authenticating their credentials.

[3] Nortel Networks, p. 41.

- The self-extraction process could be started only with knowledge of the password providing another layer of protection.
- After downloading, the VPN client software resides only on the user's home computer. Copies of the software are unavailable for others, not the case had the software been distributed on floppy disk or CD.
- The operational cost and nuisance of creating and managing an inventory of floppy disks or CDs, including how the software would be returned after installation, is avoided.
- The VPN client software could be easily replaced and re-distributed when an updated version became available.

3. The VPN client software requires configuration on installation

This risk concerned how to securely distribute authentication information to users in order to configure client profiles after the VPN client software was installed.

This risk can be mitigated using the Baynet.tbk and Group.ini files, which provide a mechanism for including authentication information within configuration files. Placing this information within configuration files means that it can be delivered to users with the VPN client software instead of by other means, such as e-mail or procedure documents.

How the configuration files are configured depends on the authentication schemes adopted within a company. Baynet.tbk distributes authentication type information and Group.ini distributes passwords. The subject company chose to authenticate off-site devices using a group name and password, which is also defined in the Switch. Users were authenticated to an NT domain using Radius (Remote Authentication Dial In user Service).

Note that the Baynet.tbk file contains the group name used to authenticate off-site devices. The group's corresponding password appears in the Group.ini file. Other parameters, specifying that user credentials be authenticated using Radius, appear in Baynet.tbk.

Baynet.tbk[4]

[Employees]	Profile name. Corresponds to name in Group.ini.
UseTokens=0	Specifies user name \ password authentication type
TokenType=3	Specifies Radius authentication
UsePAPGroup=1	Specifies Radius authentication
GroupName=EMP	Group name defined in switch

[4] Nortel Networks, p.25-26.

Group.ini[5]

[ProfileNames]	Heading (always “Profile Names”)
Employees	Profile Name(s) in this file; must appear in Baynet.tbk
[Employees]	The Profile Name in ‘heading” form
GroupPW=YYYYY	Password of group in Baynet.tbk and switch

The group password appears in clear text until the VPN client software is started the first time on the computer, at which time it is encrypted within the registry. Group.ini is then deleted.

As previously mentioned, placing authentication information in configuration files helps to mitigate this risk because the information does not have to sent to users through less secure means, such as e-mail or procedure documents. However, there is still risk of interception because it is possible to see the configuration files with the other files comprising the VPN client software. In addition, the files are easily viewed with any text reader. Two additional client features help to reduce this risk further.

The first, already mentioned in item 2 “The VPN client software must be distributed to employees”, concerns distributing the VPN client software as a single self-extracting executable file. The second concerns modifying parameters in the Setup.ini file to fully automate the installation. These settings complement the self-extracting file because after the files extract, the client installation begins automatically and completes without user intervention, including re-booting the workstation. Users do not have to click “setup.exe” to start the installation after the files have extracted.

The Setup.ini parameters are:[6]

[Options]	Heading (always “Options”)
SkipScreens=1	Skips installation dialogue screens
ForcedReboot=1	Automatically reboots system after installation
SkipLicenseAgreement=1	Automatically accepts license agreement.

These two features, the self-extracting file and automatic installation, result in the hiding of configuration files from the user. Users do not see or are even aware that authentication information is being deployed with the VPN client software. Someone seeking to attempt a hack will be denied the opportunity because they will be unaware of the existence of the configuration files.

[5] Nortel Networks, p.35.
[6] Nortel Networks, p.34.

In summary, this risk is mitigated because authentication information is distributed within configuration files and the self-extracting file and automatic installation hide the configuration files from users.

4. The VPN client software can be modified after installation.

This risk concerned users' ability to modify the VPN client software after installation.

This risk can be mitigated using the Setup.ini file.[7] The parameter: NoChangeProfiles=1, permits a change to a user name, password or dial-up phone number but denies the ability to modify or create profiles.

This option mitigates the risk because users are unable to change or add profiles, knowingly or unknowingly.

5. VPN exposes corporate information assets to the Internet

This risk concerned the exposing of corporate information assets to the Internet.

This risk can be mitigated by requiring users, as a matter of policy, to have installed on their computers up-to-date anti-virus and firewall software. This approach does have two weaknesses. First, even a computer with up-to-date anti-virus software can be compromised by a newly released virus or worm because the software's signature files will not recognize the new virus or worm. Secondly, verifying policy compliance is infeasible because auditing home computers usually falls outside the realm of a company's auditors.

However, a parameter set within the switch does provide protection from the Internet. The parameter is called "split tunneling" and setting it to "Disabled" prevents access to or from the Internet while the VPN is connected, effectively mitigating this risk. In the context of split tunneling, Nortel documentation states "To completely eliminate security risks, you should not use the split tunneling feature." [8] Disabling split tunneling for the "Base" group is recommended because subordinate groups will inherit the setting.

[7] Nortel Networks, p.29.
[8] Nortel Networks(2), p.151.

6. VPN client software offers a “Save Password” feature.

This risk concerned users’ having the ability to save their password within the VPN software.

This risk can be mitigated using the Group.ini file by setting the parameter: NoSavePassword=1.[9] Setting this parameter will deny users the ability to save a password within the VPN client software settings.

7. Inability to segregate users.

This risk concerned the inability to segregate and track the differing groups of users accessing remotely. This risk can be mitigated using a combination of switch and VPN client features.

First, at the switch, a group is created for each type of user accessing remotely: employees, Board member and business partner. Each group is assigned a unique name, password and IP address pool. Possible IP address pool assignment are shown in the following example:

172.45.25.1 to 172.45.25.254 – Employees
172.45.26.1 to 172.45.26.254 – Board members
172.45.27.1 to 172.45.27.254 – Business partner

A customized VPN software client is created for each group – Employees, Board members and business partner. Each client’s configuration files contain the credentials (group name and password) needed to log into the corresponding group defined in the switch. (Customizing the client with group credentials is discussed in item 3-The VPN client software requires configuration on installation.)

When a user connects, the group name and password in the client are used to authenticate to the switch. After authenticating, the user receives an IP address from the pool assigned the group. In the switch logs, the IP address is associated with the user’s user name providing a tracking ability. This mitigates the risk of being unable to track the type of user.

Since the switch is in front of a firewall in the subject company’s architecture, the firewall is used to permit or deny access to specific applications based on sub-net address. For example, access to the corporate intranet is permitted only for sub-net 172.45.25.0 (the employees sub-net) and access to board documents for sub-net 172.45.26.0 (the Board members sub-net). All other sub-nets are denied access. This mitigates the risk of relying only on the end application to authenticate users and adds defense-in-depth because the firewall and the end-application now jointly control access.

[9] Nortel Networks, p.35.

8. There is uncontrolled access to workstations

This risk concerned the possible access to corporate resources from uncontrolled workstations in off-site locations.

There are seven parameters that can be configured within the switch to help mitigate this risk. Each can be configured for individually defined groups, however, configuring the "Base" group is suggested because subordinate groups inherit the settings. The parameters are:

Set in the Base Group Connectivity Section [10]

Idle Time Out=30 min – disconnects VPN after 30 minutes of idle activity, in the event the user leaves the workstation unattended. This may cause some problems for the user. For example, if the user is typing a long e-mail message and 30 minutes of inactive time elapses, the VPN tunnel will disconnect. Procedures, distributed with the VPN client software should advise users to compose long messages using a word processor while VPN is disconnected and then paste the message into the e-mail.

Number of Login=2 – limits the number of possible connections per user in the event that an attacker attempts to open many VPN connections. Permitting two connections is recommended because if only one is permitted, and the connection breaks because of a technical problem between the user and switch, the user will be unable to re-connect until the 30-minute idle timeout parameter expires. Permitting two connections allows the user to re-connect and continue working.

Users with unreliable Internet connections frequently find two log-ins limiting and often request additional log-ins. However, experience in the subject company has shown that limiting log-ins to two satisfies most users and is a good balance between security and convenience.

Set in the Base Group IPSec Section [11]

Allow Only Contivity Clients – allows only the vendor-specific client to create a VPN. Someone using another vendor's VPN client software is denied the ability to establish a connection.

Banner – displays a banner when the user connects the VPN. Suggested wording is "Access is limited to authorized users of Company X". Using a banner is recommended so that an unauthorized user cannot claim that they were "allowed" to use VPN by virtue of the fact that they were not warned that access was limited to authorized users.

[10] Nortel Networks(2), p.124.
[11] Nortel Networks(2), p.151-152, 155-156.

Display Banner – turns on the ability to display of the banner.

Client Screen Saver Required: Enabled – requires the user to set a screen saver with password protection, or VPN will not connect. This requires the user to set a password protected screen saver in the event that user leaves the workstation unattended. Some users have found this setting to be unwarranted because they feel their homes are secure. It is recommended that the screen saver requirement be added to a company's remote access policy.

Client Screen Saver Activation Time: 15 minutes – sets the required screen saver activation time. In the subject company, an activation time of 15 minutes was deemed reasonable for a home environment. Each company will have to establish their own reasonable time based on perceived risk and the nature of the data being processed.

9. VPN implementation risked increased administration cost

This risk concerned the possible increased administration cost of maintaining another repository or user names and password. Creating another repository of user names, for example, within the VPN switch, was considered highly undesirable, especially given that the subject company had 1,000 employees.

To mitigate this risk it was determined that Radius (Remote Authentication Dial In user Service) would be used to authenticate users to the existing repository of user names. Radius was a widely used and stable authentication system and would result in completely avoiding the costs associated with creating and maintaining a new repository. As well, the Radius parameters could be added to the VPN client software's configuration for distribution to users.

Based on identified risks and available solutions, the baynet.tbk, setup.ini and group.ini files would have the following parameters set:

Baynet.tbk

[Employees]	Profile name. Corresponds to name in Group.ini
UseTokens=0	Specifies user name \ password authentication type
TokenType=3	Specifies Radius authentication
UsePAPGroup=1	Specifies Radius authentication
GroupName=Emp	Group name defined in switch

Group.ini

[ProfileNames]
Employees — Profile Name(s) in this file; Must appear in Baynet.tbk

[Employees]
GroupPW=YYYY — Password of group EMP in Baynet.tbk and switch
NoSavePassword=1 — Denies user the ability to save the password

Setup.ini

[Startup]

[Options]
FolderName=VPN — The folder name in which files are stored
ProductName=VPN — The name appearing on the computer's Start menu
NoChangeProfiles=1 — Denies user ability to change or create profiles
SkipScreens=1 — Skips installation dialogue screens
SkipLicenseAgreement=1 — Automatically accepts license agreement
ForcedReboot=1 — Automatically reboots system after installation

The "Base" group defined in the switch would have the following parameters set.

Idle Time Out=30 minutes
Number of Logins=2
Allow Only Contivity Clients
Banner=Access Restricted To Authorized Users of Company X.
Display Banner=enabled
Client Screen Saver Required=Enabled
Client Screen Saver Activation Time = 15 minutes

Enhanced Security (after snapshot)

The results of the recommendations in the previous section are that the VPN client is distributed with security in mind. The following expresses the subjects addressed in this document in the form of recommendations. They can be applied to VPN software from any vendor (assuming the options are available in the configuration files).

1. Remove vendor references from the VPN client dialogue screens, Start menu and file system.

2. Distribute the VPN client as a single self-extracting executable file from a web site. Protect the software by requiring a password to gain access to the software and begin the self-extraction.

3. Use configuration files to distribute authentication credentials. Hide the configuration files from users by creating a self-extracting executable file and have the software automatically install and re-start the workstation when launched by the user.

4. Deny users the ability to modify the VPN client or create new profiles.

5. Deny users the ability to access the Internet when VPN is connected.

6. Deny users the ability to save their password in the VPN client.

7. Track user groups in logs by assigning unique IP address pools to each group. Use firewall rules based on sub-net IP address to permit or deny access to applications. Distribute customized VPN client software to each group.

8. Set and idle timeout for VPN connections.

9. Restrict the number of logins permitted users.

10. Display a banner to users when VPN connects advising that access is restricted to authorized users.

11. Require users to have a password protected screen saver set on their home workstations (in addition to anti-virus and firewall software). Add this requirement to corporate policy.

12. Leverage existing user name repositories to authenticate VPN users by using an authentication system such as Radius.

These recommendations reduce but do not eliminate the risks associated with the VPN client software. For example, employees travelling with laptop computers pose a continuing risk because laptops are easily lost or stolen. Stolen laptops could be used to attempt to access the company. However, these recommendations provide some relief. In the case of a stolen laptop, once reported, a self-extracting client with revised credentials could easily be made available to users via the web making the clients on the stolen laptops obsolete. This same approach could be used to distribute client software that has been upgraded by the vendor.

Other continuing risks include the storing of sensitive files on home computers, the discovery of passwords using social engineering means or third-party access of files from unattended logged-in workstations before the screen-saver has started.

It is evident that companies must continue to emphasize secure computing practices to employees working from home. However, distributing secured VPN client software improves the security posture of the company.

References

Alcatel. “Virtual Private Network (VPN). An Alcatel Executive Briefing.” Jan. 2002. URL: http://www.ind.alcatel.com/library/e-briefing/eBrief_VPN.pdf (12 Dec. 2002).

Alcatel. “Understanding the IPSec Protocol Suite.” March 2002. URL: http://www.cid.alcatel.com/doctypes/technewbridgenote/pdf/ipsec_nn.pdf (12 Dec. 2002).

Nortel Networks. Configuring the Contivity VPN Client, Version 4.65. Billerica: Nortel Networks, July 2002.

Available in PDF format from: http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?BV_SessionID=@@@@1836340386.1039035884@@@@&BV_EngineID=iadcfklldmgdbhkcginchgcgjg.0&level=6&category=8&subcategory=5&subtype=&DocumentOID=75234&RenditionID=REND34233. (12 Dec. 2002)

Nortel Networks(2). Configuring the Contivity VPN Switch, Version 4.50. Billerica: Nortel Networks, August 2002.

Available in PDF format from: http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?BV_SessionID=@@@@0787399204.1039122754@@@@&BV_EngineID=hadcfldegljebhkcginchgcgio.0&level=6&category=8&subcategory=5&subtype=&DocumentOID=77066&RenditionID=REND34851 (12 Dec. 2002)

Halpern, Jason. “SAFE VPN IPSec Virtual Private Networks in Depth.” URL:http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8bc.shtml (12 Dec. 2002)

Honeynet Project. “Know Your Enemy: A Forensic Analysis. The Study of an Attack”. 23 May 2000. URL: http://project.honeynet.org/papers/forensics/ (13 Dec 2002)

Salamone, Salvatore. “VPN: The Basics.” VPN Core Technology Primer RADIUS Servers. 14 Dec. 1998. URL: http://www.internetwk.com/VPN/paper-3.htm (12 Dec. 2002)