Global Information Assurance Certification Paper

Graham Belton
(9th Dec 2004)
GSEC Practical Assignment v1.4c
Option 2 - Case Study in Information Security

Secure remote access using a Juniper SSL VPN

Table of contents

Introduction

Increasingly in today's market there is a need for rapidly deployed secure remote access solutions to a varied portfolio of applications. GB8 Co is a large UK based engineering company which is finding that it is increasingly engaging in joint ventures with other international companies. The IT infrastructure is therefore often shared or individual components of the IT solution are supplied by different companies. There are often special security considerations for these kinds of joint operations.

This paper outlines how GB8 Co provided a secure remote access environment for a project within a short time frame utilising a Juniper SSL vpn. It covers the initial requirements, the options that were available at the time and their limitations, the reasoning behind selecting the Juniper SSL vpn, steps taken to configure and secure the installation and a discussion of relevant security concepts surrounding this.

The existing situation

The GB8 Co remote access methods have evolved in an uncoordinated fashion over the past few years in the absence of an overall remote access strategy. The main corporate remote access solution is based around a Nortel Contivity IPsec VPN gateway which is available only to users who have a company supplied laptop preinstalled with the corporate tailored Microsoft Windows XP image and the Nortel Contivity VPN client software. The GB8 tailored Windows XP image comes preinstalled with Symantec Anti virus software and regular patching is managed via Microsoft Systems Management server. Authentication is handled by an RSA\ace radius server and secure ID key fobs. The RSA\ace radius server maintains a local user id database in the current implementation. There is no Active Directory integration.

In addition to the Nortel Contivity solution GB8 Co uses Microsoft's OWA, (Outlook Web Access) for employees to access email via https over the internet. The Exchange servers are running Microsoft's Exchange 2000 server platform. A portal environment is available both internally and via the internet through DMZ based servers utilising https. This is based on Plumtree software and for user authentication it integrates into Active Directory. Only certain applications are available via the GB8 Co portal environment.

A Juniper SA3020 SSL VPN Instant Virtual Extranet (IVE) has recently been installed but its development and configuration is at an early stage. It has been hurriedly implemented and is serving only as a method for a small number of users to access a particular web based corporate database. Security has not

been a major consideration in its deployment. It does not have any of the following built in security in place, a digital certificate from root a certification authority, any form of checking to determine which hosts are allowed to connect, any form of IP range restrictions or any restrictions on which servers could be accessed.
The new project which is mobilising to a contractor yard in China at short notice has the following specific requirements.

- E-mail. In particular they need to use the full Microsoft Outlook client. The project working practices rely heavily on personal folders (pst's). The Exchange server will reside on the internal GB8 Co UK network behind firewalls.

- Access to selected data which is stored on the corporate Windows 2000 file servers which reside within the internal GB8 co network behind firewalls and are not accessible via the internet. The project staff must be able to upload and download files. These are mainly Microsoft Office documents.

- The corporate intranet which is not made accessible on the public internet.

- Certain Plumtree portal based web applications. The Plumtree portal is accessible via servers located in a DMZ utilising https over the internet but is limited in functionality.

The Project staff will be provided with laptops by a partner company. (For the purpose of this document they will be referred to as Company 2). They will be pre-configured to a standardised Microsoft Windows XP image which will be different from the standard GB8 Co image. The Company 2 image comes pre-installed with Symantec anti virus scan software which is configured to update its anti virus definitions automatically from the Symantec liveupdate website.

Access onto the internet is to be provided via the Company2 network. The bandwidth capacity and reliability of the connection is unknown at the start of the project. There will initially be no IT support personnel available on-site.

IPsec VPN or SSL Vpn?

When considering the possible solutions Microsoft OWA and the Plumtree portal were dismissed as they did not meet the requirements. The OWA does not permit the use of locally stored .pst files and the OWA interface is not widely liked by the user community. The Plumtree portal does not provide access to the required applications. Neither would enable access to the files located on the corporate windows file server.

That left us with the two alternative VPN solutions. The Nortel Contivity Ipsec vpn or the Juniper SSL vpn (IVE). There is much debate about the pro's and con's of each solution and many would argue that they both have a place in our current thinking. In different situations each may be the better solution.
A detailed comparison of the two is out of the scope of this document but some background information is useful.

The IPsec VPN operates at the network layer creating a secure encrypted tunnel from the source machine over the public internet to the internal network. Encryption occurs at the IP packet level. The experience for the user is much like being on the corporate LAN. The fact that the full range of applications and network access is available to the user can be seen as a benefit but can also be seen as a drawback. A basic security principle is to give the users access only to what they need, and no more.

Generally remote users are likely to be connecting across untrusted networks, networks that we have no control over. It is not always straightforward to maintain operating system patching levels and anti virus definition levels on machines that are connected only sporadically via a VPN. With the Ipsec vpn arguably there is more of a threat from worms and viruses on the host pc being able to spread to infect devices on the network unless measures are put in place to prevent this such as host checking which can be configured on most IPsec vpn gateways to deny the connection if the machine does not meet certain requirements.

In terms of authentication the RSA secure key fob authentication which the Nortel Contivity solution is utilising is an established and widely used technology .It is an example of the concept of two factor authentication, i.e. "Something you *know* and something you *have*". To simplify slightly, the secure key fob generates a unique code every sixty seconds. This is based on a unique symmetric key combined with an algorithm to generate the unique code. The authentication server is also able to compute the same code for each secure key fob at the same time and allows access based on this match. The authentication server computes the previous minute's value and the next minute's value and also allows these as a match. This is to allow for a slight variation in clock settings. If a previous or next value is used then the system adjusts to correct the variation. The code is used in conjunction with a separate pin or password which the user must remember.

The IPsec VPN requires a specific piece of client software to be installed on the remote machine. One drawback of this, apart from the fact that it needs to be installed on every machine that needs to connect is that the client software needs to be kept up-to-date. Keeping software up to date on roaming user's machines always presents problems because they often cannot come into the office to plug into the LAN to download large updates and they may not be prepared to connect for long enough remotely to download these. A certain amount of IT

knowledge is often required of the end user to understand the importance of updates. This is one main area in which it differs from the SSL VPN.

The SSL VPN works at the application layer, encrypting traffic at the application level from the source application to the SSL gateway device. Because all web browsers today can handle SSL there is no need for extra client software and the SSL VPN can be accessed across operating systems and via different vendor's web browsers. Configuration changes only need to be made in a single place, on the device itself to affect all connecting users. If the SSL VPN device makes use of extra applet type applications as well as the standard web browser then these can be configured to push out to connecting clients automatically as new versions are released.

Though both VPN solutions have their pros and cons the Ipsec VPN was ruled out primarily on policy grounds. In an effort to retain control of the IT infrastructure and protect the integrity of the network and its data the GB8 co security policy prohibits the connection of non GB8 Co devices onto the company network and therefore prohibits the installation of the Contivity vpn client software on non GB8 Co devices. The Ipsec solution would have required that laptops be supplied by GB8 Co which was not a negotiable option.

The Juniper SA3020 SSL VPN device (IVE) was therefore deemed to be the best solution. With this device it is possible to be very selective about what is made available. It can provide access to only the intranet resources and the portal applications which we specify, not the entire network or subnet. The user can run locally hosted applications such as Microsoft Outlook over the secure SSL connection communicating securely with a back-end server residing behind firewalls in the internal network. It can also provide access to the corporate windows 2000 file server either through a web like interface with ftp style functionality or through netbios drive mapping. In theory it looked good but it was at an early stage of development and it needed to be secured. Whilst nothing is truly secure we needed to pay attention to security in our proposed solution and take steps to make it as secure as possible.

HTTPS, SSL and the digital certificate

The SSL communication protocol has been around for many years. It is an example of a Public Key Infrastructure (PKI) and it uses the concept of a Private and public key pair. Essentially these function on the basis that what one key encrypts the other key can decrypt. HTTPS over SSL is widely used today for secure communication on the internet. A good definition is provided by http://whatis.techtarget.com/.

"A Web protocol developed by Netscape that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange"

The communication process is initiated by the client which makes a request for a secure page to the server. The server responds to the request with its certificate and public key. The client receives the public key and verifies it against the certification authority. If verified the client generates its own randomly generated symmetric key which it encrypts with the server's public key and sends to the server. The server can then decrypt the symmetric encryption key with its own private key. Communication then takes place with data being encrypted with the symmetric key.

Although it is by no means inconceivable that the SSL encryption could be broken it is in widespread use for banking transactions and the like and can be deemed adequate.

The SSL digital certificate should be signed by a Certificate authority (CA) otherwise there is no guarantee that the issuer of the certificate is who they claim to be. The Root Certificate authority is responsible for verifying that the issuer of the certificate is who they claim to be. The certificate contains such information as issuer name, subject details, email address & period of validity. The certificate also contains a hash to verify that the certificate has not been tampered with. The Root CA is the top level of the trust tree in the PKI infrastructure. It works on the premise that the root CA is trusted to have verified the issuers credentials and to be able to manage these securely.

Initially our IVE device was running with the default vendor created digital certificate which cannot be validated by a trusted Root Certificate authority. This meant that connecting users were getting the standard "invalid certificate" type notification when connecting to the URL which they were required to OK, An irritant to the end user as well as being less secure.
A certificate was ordered from a trusted Root Certificate authority to replace this. This provided us with a level of verification that the site was genuine.

Security on the Juniper device

The IVE has a number of security settings which we felt we needed to consider. We were particularly concerned about the Exchange server as a possible route into the network and the file browsing of the Windows 2000 file server. We decided to concentrate on securing the device using as many methods as we

could making use of a “strength in depth” approach. The more methods you have of securing something the less likely it is to be cracked. There is no point in having one very secure access method into your device if you leave others open. The potential attacker will always opt for the easiest route. Importantly though security has to be balanced with usability. If we make it too difficult for users to connect and use the system then we defeat the object of the whole exercise.

In terms of the normal vulnerabilities which we may expect a standard web server to be vulnerable to the IVE mitigates against these because it masks the dns name of the actual web server and acts as a proxy between the client and the web server itself. This does not mean that we do not have to secure or harden our web servers. They should be hardened as much as possible and be maintained to the latest patch levels. There are some readily available baseline configuration checking tools which can be used to harden a web server to varying degrees. For example, the Center for Internet Security (CIS) benchmark tool can be used to check a server configuration against multiple levels of industry standard secure configurations. It can be found at the below URL

http://www.cisecurity.org/

The Microsoft IIS lockdown tool can be used to harden a Microsoft IIS server by, amongst other things removing or disabling unnecessary services. It can be found at the below URL.

http://www.microsoft.com/technet/security/tools/locktool.mspx

Role based privileges

The IVE device allows for separate roles to be created each giving different levels of access. The single existing role had a simple configuration with none of the security features activated other than basic authentication. We added a new role as we wanted specific access separate from the standard user role and better security. We were impressed at the number of options that the IVE provides to enhance its security. The options we decided to implement are listed below.

Host Checker

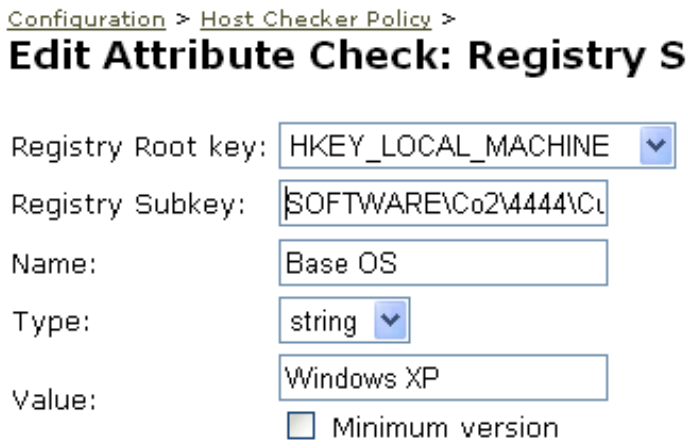
We wanted to restrict connectivity to only the Company 2 Windows XP imaged machines. We were able to go some way to ensuring this by using IVE host checker.

The host checker consists of an activeX component that is configured to run on the users PC automatically when they sign into the device. It can be configured

for example to search for the presence of a particular registry key or a particular vendor's firewall or anti virus software.
It can also be configured to process detailed rules containing multiple conditions. For example the presence of a particular registry key plus a particular Active directory group membership assuming Active Directory authentication is being used.

We decided to configure ours to search for two things. Although our solution is not foolproof since registry keys can obviously be added and removed and antivirus software is quite generic we felt that it offered a good level of checking.

Firstly a registry key was selected that the host checker would verify before allowing the connection. A search of the Windows registry revealed a number of company 2 specific keys which we could utilise. One of these was selected and added to the host checker rule.



Secondly we wanted to ensure that the Symantec anti virus software was present and running. We only wanted machines connecting to the device that were running anti virus software, in this case Symantec's antivirus. We included this in the host checker rule giving us two-factor checking of potential hosts. If either isn't present the connection will be refused. This rule works by checking if the antivirus software is running as a process on the host machine rather than checking the registry.

Session length, idle timeout and warning

Session length, idle timeout, warning are important. If we configured the session length to be too long and did not set a timeout then we would be more vulnerable to the session being hijacked. Suppose the user leaves their web browser open and walks away from the desk. The session is still running even if the user has typed in another URL. An intruder could get onto the session simply by using the back button on the web browser. This is even more of a concern if you do not implement any form of host checking because users may connect to the IVE from any machine, for example from a public web cafe or a hotel.
These session length considerations needed to be balanced with usability. It is unacceptable and highly frustrating for the user to be disconnected without warning, say every 5 minutes because their session has expired. On the other hand it is unacceptable from a security perspective to set the session length too long as this leaves us more open to careless user activity and possibly attacks. We decided on a max session length of 45 minutes with an idle timeout of 15 minutes. The reminder time was set at 5 minutes before the session expires. This activates a prompt for the user who is able to continue the session.

Allowed servers and port restrictions

For Microsoft Outlook to function it needs to be able to communicate with the exchange server inside the corporate network. On the IVE this is facilitated by a windows or java based “secure application manager” applet which runs on the user’s pc and directs application traffic across the secure SSL connection as determined by rules which the administrator has configured. The applet can be set to either download automatically as soon as the user is authenticated by the IVE or the user may be required to click on a link in order to download it. The applet can also be configured to uninstall itself when the user signs out which is a useful security measure as it means no trace of the application is left that a potential intruder could use in order to gain information about the network.

The secure application manager applet works with Microsoft Outlook and Exchange by listening on port 80 for Microsoft Exchange requests. Microsoft Outlook can forward all RPC requests to Exchange over http if a particular registry key is set in Windows. The secure application manager sets this key. Then the IVE receives the http requests and distributes them to the Exchange server as plain RPC requests. The Exchange server sees the traffic from the IVE as normal RPC traffic from Outlook.
When the secure application manager applet is stopped the registry key is reverted back to its normal setting but even if it were not the client would not experience any problems connecting to another Exchange server across a LAN. The registry setting merely specifies an order which Outlook uses so it would first

try RPC over HTTP, then when this did not succeed it would revert back to normal RPC.

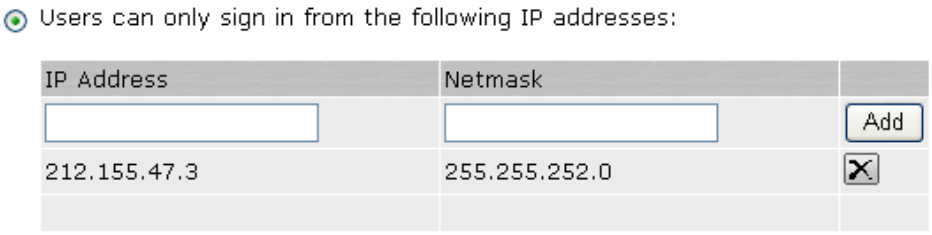
Configuration of the secure application manager allows for restrictions on which servers are available down to the port and protocol level on these servers. It would be careless to allow full access to the servers on every port. This could leave us potentially vulnerable to, for example, port scans and malicious software that targets particular ports. Some research into Microsoft Exchange communication revealed we would not easily be able to restrict the Exchange communication to just a few ports.
Firstly TCP port 135 is required as it's used for Microsoft RPC (Remote procedure call) requests. After the RPC request has completed and the client is connected we discovered that the Microsoft Exchange server assigns two random ports for connecting to the information store and the directory. We therefore found that we couldn't restrict this further unless we configured the Exchange server to use a statically mapped port for the Exchange services. The Microsoft recommendation is to assign static ports in the range 5000-65535. Using ports lower than 1024 (below the ephemeral port range) is not recommended as it may cause undesirable results. At this time we have not statically assigned the Exchange ports though this could be done in the future once we have assessed the impact.

For the Windows file browsing the IVE offers two alternatives. Either browsing via a shortcut URL type interface on the actual IVE page or netbios drive mapping where the user actually maps a windows network drive to the share as if they were on the LAN. The second option utilises the secure application manager, netbios traffic is directed via the SSL connection. We felt more comfortable with the first option. It was straightforward to add a shortcut to only the single Windows share that the users needed access to. The Windows ACL's of course also serve to control access. For the user the share appears as a URL type shortcut and subfolder levels expand as the user clicks on them. To work on a file the users need to download it to their local machines then upload it again. The option exists to allow the users to add further shares to their custom page. We chose not to allow this as all their data was in a single share. We found that the users needed time to get used to this method of file access as initially they were concerned that two people would simultaneously be working on a file then upload it one after the other. They had become accustomed to the file locking behaviour of normal windows file access. The IVE helps with this problem by automatically adding a time and date variable on the end of the file name when files are uploaded. This can be overridden.

IP restrictions

The IVE allows for restrictions on IP address ranges which are allowed to connect. We are able to specify a range of IP addresses with the subnet mask

which can access the device. Although IP addresses can be spoofed this is an additional weapon in our portfolio. It is only practical if you are able to specify a range of IP addresses that are not going to change. DHCP addresses would need careful consideration here. Also, as most networks will utilise address translation to translate internal IP address into routable public IP addresses this needs to be taken into account. In our case we were able to configure the device to allow connectivity only from the Company 2 external NAT address. If we wanted our resources to be accessed from any internet connected computer then obviously the IP restrictions would not be an option.

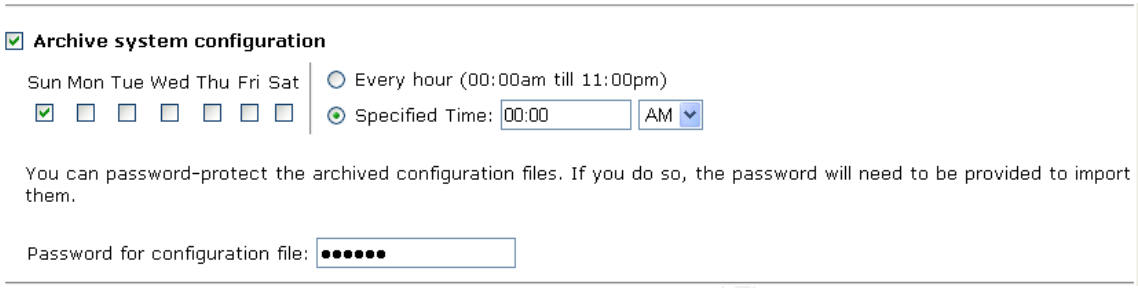


Authentication

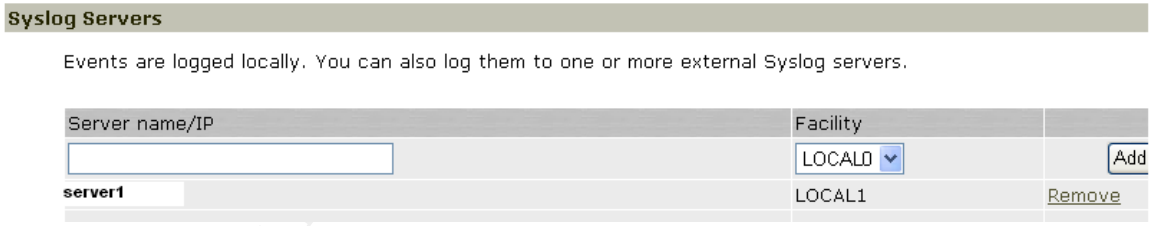
The IVE can be configured to use a number of authentication methods including radius, Active directory LDAP or NTLM, or it can maintain its own account database. We opted to use Active directory LDAP authentication using the already established corporate Active directory. This meant that we could easily control access via Active directory security group memberships and simple LDAP "memberof" conditions configured on the IVE. We were also able to easily incorporate the device into the existing processes for granting and removing user access. These processes dictate that requests for access are logged in a call logging system thereby creating an audit trail of the requests. All requests for access are subject to managerial approval and access can only be granted by authorised members of the security administration group. There is a standard support model in place with a central IT Service Desk and processes for identifying and disabling unused user Windows user accounts. The Active directory infrastructure is fault tolerant and there are disaster recovery procedures to ensure it is recoverable. On the IVE It is possible to configure a primary and two secondary LDAP servers which protects against the possibility of one domain controller being unavailable at any given time. In addition to this the Active directory gives us sensible account controls by enforcing the standard Windows domain account policy settings, for example on password length, age, history, complexity and account lockout thresholds.

Configuration backup and external logging

In the event of a disaster we needed to be sure we had an up to date copy of the configuration of the IVE. For this we utilised the “Archiving to FTP server” option on the device. This allows for the device configuration files, the user access logs, administrator access logs, and event logs to be FTP’d to an FTP server at specified intervals. We opted for a weekly FTP of the system configuration to an external FTP server. A password can be set on the configuration file to avoid anyone tampering with it.



We wanted the user access logs to be readily available so that we could interrogate them as required without needing to log onto the IVE as an administrator. We also wanted a backup of the logs in case of a disaster type event on the IVE. We decided to export them to an external syslog server. This was achieved using the excellent Kiwi Syslog Daemon v7.1.4 software which is produced by Kiwi Enterprises. This runs on the Windows platform. It was a simple matter of inputting the Syslog server name or IP address and specifying the facility on the IVE to configure the IVE device to send its logs to the external Syslog server.



Documentation for users

A comprehensive user manual document was produced for the end users. In particular this stressed the importance of signing out of the IVE session using the “Sign Out” button to end the session rather than simply exiting the browser. We wanted to educate them on the importance of not leaving sessions running.

Meeting requirements

On a simple level we may conclude that the IVE solution has met the original requirements as it has enabled the functionality that we intended without the need to deploy a full network environment. Initial feedback about the IVE solution has been good. With minimal financial outlay the project has been provided with a tailored remote access solution but from a security perspective how does it stand up?

It may be useful to evaluate the solution in terms of the three widely used basic principles in information security, Confidentiality, Integrity and Availability.

In terms of confidentiality we may ask the question. “Are the transactions conducted in a confidential manner” The SSL encrypted communication ensures that communication is sufficiently confidential between the user and the backend server. The use of a root CA certificate has enhanced this.

In terms of integrity we may ask questions about the integrity of the data which they are accessing. “Is it accurate, or has it been altered”? We have implemented various measures as defined above which should help to keep out potential intruders. The Active Directory authentication is the first method of authentication to ensure we only grant access to the intended users. The host checking and IP address checking are other methods we have implemented to ensure that only the desired users have access. These all contribute to the integrity of the data.

In terms of availability we may ask the question, “Is it available?” and, importantly “available to whom?” The IVE services are available, 24 hours per day, the configuration is backed up weekly so can be restored quickly to ensure it is kept available. The Active directory authentication infrastructure is available 24 hours per day and is backed up. The IVE logs are stored off the main device on a syslog server. The restrictions outlined above help to ensure that they the IVE is available only to authorised users. The timeout settings are an important part of availability, set them at a too unrestrictive level or not at all and you increase the risk of the data being available to the wrong users. User education is important in ensuring availability to only the authorised users. They must be educated to sign out properly from the IVE and also use the Windows “Ctrl + Alt + Delete” sequence to lock their workstations. This is of increased importance given the fact that workers from multiple companies are likely to be in the vicinity and perhaps office security may not be as strong on certain remote sites as it would be in a corporate main office.

In terms of vulnerabilities the IVE device is not vulnerable to many of the common operating system specific vulnerabilities e.g. those that target Microsoft IIS server. The IVE device will instead be subject to its own specific vulnerabilities. As with any system it is vitally important to keep the device maintained up to the latest patch operating system and patch levels and to monitor closely any vendor released communications on vulnerabilities and implement workarounds and fixes in a timely fashion.

References

Course Material, Track 1 Security Essentials Version 2.2. SANS Institute. 2004

RSA Securid Authentication, Products. RSA Security.
URL: http://www.rsasecurity.com/node.asp?id=1156 (20 Sep 2004)

An HTTPS definition. Whatis.com.
URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214006,00.html (12 Sep 2004)

SSL Certificates HOWTO. Tldp.org
URL: http://www.tldp.org/HOWTO/SSL-Certificates-HOWTO/x64.html (12 Sep 2004)

Phifer, Lisa. VPNS: "Tunnel Visions". Information Security Magazine. Aug 2003.
URL:
http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss21_art83,00.html (10 Oct 2004).

Port assignments. IANA.org
URL: http://www.iana.org/assignments/port-numbers (10 Oct 2004)

Parsons, Ian. "SSL VPNs", Group test two, Product Section, SC magazine. Oct 2004.
URL:
http://www.scmagazine.com/products/index.cfm?fuseaction=GroupTestDetails&GroupId=15010 (17 Oct 2004)

Parsons, Ian. "Ipsec VPNs", Group test two, Product section, SC magazine. Nov 2004.
URL:
http://www.scmagazine.com/products/index.cfm?fuseaction=GroupTestDetails&GroupId=15265 (20 Nov 2004)

Laubhan, Jeff. "Secure Authentication and Access to your Critical Resources", Rainbow Technologies.
URL: http://www.bizforum.org/whitepapers/rainbow-3.htm (26 Nov 2004)

Setting TCP/IP Ports for Exchange and Outlook client connections through a firewall, Microsoft Help and Support, Article ID 155831, Rev 1.0. Oct 2004.
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;155831 (26 Nov 2004)

Other Information

Kiwi Syslog Daemon, Kiwi Enterprises.
URL: http://www.kiwisyslog.com/info_syslog.htm (26 Nov 2004)

KB 19015 “What are the major TCP port numbers used by the Neoteris IVE?”
Knowledge base, Customer support centre, Juniper Networks.
www.juniper.net (14 Oct 2004).

KB 19013 “How does the Neoteris java applet work with native Outlook?”
Knowledge base, Customer support centre, Juniper Networks.
www.juniper.net (14 Oct 2004).