Global Information Assurance Certification Paper

Securing the Perimeter – a Case Study

GSEC Practical Assignment 1.4b Option2

Stephen Boyd

July 2003

Abstract

Earlier this year we replaced an internet firewall no longer supported by the vendor and dial-up remote access system were replaced with a managed secure Internet gateway service and a virtual private network (VPN) as part of a major upgrade in security. This paper concentrates on the VPN implementation, but includes the Internet gateway service implementation as both the design and implementation were interlinked and the combined effect was to secure the networks perimeter.

These projects reduced the assessed risk to the agencies internal network from "High" to "Low".

The Organisation

This paper concerns a medium size government agency in Australia. Most of the staff are located in one city, but there are several interstate offices connected via a WAN using primarily frame relay links. There are a number of very remote interstate and overseas locations where conventional telecommunications services are limited (dial-up speeds of 9600 bps on a good day). In several of these locations the only option available to connect these offices to the network is a two-way satellite service. In others we are dependent on the incumbent Telecom or ISP upgrading their infrastructure before we can obtain reasonable Internet bandwidth.

There are a number of staff who travel regularly and require access to corporate IT services while travelling. A significant number of staff work from home. Generally this is on an ad hoc basis rather than formal 'Home Based Work'.

Government policies relating to IT Security are detailed in the Protective Security Manual (PSM) [1] and several instructions from the Defence Signals Directorate, particularly Australian Communications Security Instruction (ACSI) 33 [2]. The highest level of information processed on the systems discussed in this paper is 'Protected'. While information of this classification requires substantial protection, the solution adopted is based on a mixture of open-source and commercial off the shelf software and is equally applicable to many commercial environments.

The agency (A) has close ties with two other organisations (lets call them B and C). In both cases there are joint project teams. Staff in these teams move between the two organisations premises and there are applications which everyone in the project team needs access to. The relationship with B is much closer than that with C – in the former case it is driven by the CEOs, while the relationship with C is primarily at the business unit level.

The provision of IT services to agency A and agency B has been outsourced to the same provider.

My role in these projects was as IT security advisor and project manager of the firewall replacement and the initial phases of the VPN. I am developing a linux based Live CD for accessing the VPN.

Before

When this project commenced there were a number of known problems with the network from both business and security perspectives.

The firewall isolating the corporate LAN from the Internet was old and used software that was no longer supported by the vendor.

Remote access was provided via a dial-up remote access service using a toll-free 1800 service. Connection speeds were a significant limitation and a couple of key staff had 128 kbps ISDN connections installed to resolve performance issues. Remote access was costly, performed poorly (especially for staff overseas) and as the dial-up links were not encrypted they could not be used for sensitive or classified information.

Supporting the joint project teams required connections to the networks in agencies B and C. In both cases A's LAN had been extended into the other organisations building via a fibre optic link. Networks A and C were linked by a router so staff in C could access a server in A and the firewall port has been opened to allow staff in B to access one application in A's network.

While the agencies main web servers were located in a DMZ, two semi-autonomous parts of the agency operated web servers located inside the network perimeter and the firewall was configured to allow access from the Internet. As we were to discover later, one of these servers also made http connections to other web servers on port 80. While this presented a significant security risk, it was an essential part of a web service we delivered in co-operation with a number of other organisations.

Identified security issues included:

- an unsupported firewall, which had a large number of redundant rules reflecting changes over a number of years
- two web servers located inside the network rather than in the DMZ,
- the dial-up remote access service didn't use any form of encryption.
- users emailing sensitive information via the Internet,

- the router linking A and C did not comply with the IT Security Policy.

A Threat and Risk Assessment had assessed the overall risk level for the agencies network as “High”.

During

Business Case

The key drivers for these two projects were:

- To ensure the network met the requirements for a Protected level network[1] as required by the agencies IT Security Policy,
- To join FedLink, an inter agency VPN used primarily to route email between agencies [3],
- To provide a number of network services to the remote offices which currently were not part of the WAN,
- To replace the dial-up remote access system with a faster, more reliable service,
- To improve the delivery of web services (the existing link to our ISP sometimes saturated during periods of high usage of our web servers).

Part way through the project the ground rules changed – the joint team with B was to expand. They would have staff in both organisations buildings and needed to have access to systems on both networks (and no, they didn’t have a budget that would allow us to build a completely new network!)

The business case for both projects was primarily based on cost savings that would flow from the use of a different ISP and the reduction of dial-up costs once the VPN was operational.

Security Objectives

- Replace the aging firewall with one that complied with the requirements for a Protected level Gateway[2]. (In practice this meant that the agency either

---

[1] This requirement comes from the organisations IT Security Policy. The requirements are detailed in ACSI 33.

[2] A prerequisite for joining FedLink is having the Internet gateway certified at the protected level. The requirements for this are detailed in the Gateway Certification Guide[5].

purchased a firewall from a list of products evaluated under the Common Criteria[4] and then implemented appropriate intrusion detection and reporting procedures or they used a managed service based on such products. In late 2002 there were two ISPs with a suitable managed service – the Agency selected one of them.)

- Replace the dial-up remote access system with one which ensured the confidentiality and integrity of information transferred between systems,
- Use the existing network directory for authentication preferably via the current dial-up system's Radius server,
- Provide several layers of security between the Bad Guys on the Internet and the internal network,
- Restrict remote users access to the internal network without overly restricting their ability to work,
- Use products that have been independently evaluated under the Common Criteria wherever possible.[3]

Choices

This section of the paper briefly discusses several of the key decisions made during the planning design phases.

DMZ location

Once the decision to move to the managed service was made, the detailed design started. A key issue was whether to relocate the web servers to the ISP's premises or retain them in-house. The eventual solution was to retain them in-house and have an additional 100 mbps link to the ISP to ensure the DMZ traffic and internal network traffic remain separate.

What about the web servers inside the network?

One of the two rogue web servers was decommissioned while the other was relocated to an existing server in the DMZ while leaving the back-end databases in place. Keeping all the data behind the firewall achieves two security objectives – there are extra layers of security between any Internet based attacker and the database, and it improves availability (as there is far less to restore on the DMZ server if it is compromised).

---

[3] An independent evaluation provides a high level of assurance that the product will function in the manner the vendor claims, provided it is implemented as specified.

Which VPN?

> A Virtual Private Network (VPN) allows two private networks to be connected over a publicly-accessible network. Some people confuse this definition with that of an encrypted tunnel, but it is not necessarily the same thing. A VPN often *is* composed of an encrypted tunnel, but it is not a requirement to the definition. In fact, there are certain VPN configurations that do not require a tunnel at all. In other words, a VPN is just the extension of a private network over a public infrastructure. [6]

There are numerous 'VPN' solutions available, including:

- Telecom or ISP services which simply isolate traffic using dedicated frame-relay or atm circuits or features in the ISP's infrastructure. The Virtual Private Network Consortium refer to these as '*trusted VPNs'*.[7]
- Router based networks where the router encrypts a site-to-site link.
- Tunnelling protocols such as L2TP that will link two networks but don't necessarily use encryption.[4]
- Encrypted tunnels based on either proprietary protocols or on open standards such as IPSec [8], SSH [9] or SSL [10]. The Virtual Private Network Consortium refer to these as '*secure VPNs*'

With apologies to Orwell, it seems that *All VPNs are private, but some are more private than others!*

The agency's requirements for confidentiality and integrity, coupled with the need to support users connecting via the Internet eliminated any options that were not based on open encryption standards such as 3-DES or AES.

The solution needed to scale easily. The initial design criterion was for 50 concurrent users, with the ability to at least double this if required.

SSL based VPNs are designed to deliver web based applications via the end user's browser. We eliminated them since some of the required applications are not browser based and an SSL based system would not support servers. It is worth noting that the Defence Signals Directorate (DSD) specifically recommends against the use of SSL for many applications since there is no guarantee as to the integrity of the client [11].

The use of an IPSec tunnel solution allows HelpDesk staff to use remote control software to resolve problems with a remote PC in the same way as they do on the network.

---

[4] Layer 2 Tunnelling Protocol is defined in RFC2661 [15]. It does not include encryption but can be used in conjunction with encryption such as IPSec if required. For example Windows 2000 default tunnelling protocol uses L2TP and IPSec. [16].

We briefly considered using PCs running open-source software such as FreeS/WAN [12] or OpenBSD [13] but considered the support issues would outweigh the cost benefits, primarily because the local support staff had little relevant experience.

Systems such as KyberPASS Secure session [14] that required Public Key Infrastructure (PKI) were eliminated as we considered that they would cause more management issues and were probably overkill.

The selected system uses a Cisco 3000 series VPN concentrator [17] located on its own DMZ segment and a mixture of hardware and software clients. This has the advantage that the same system can be used for the remote offices, home based workers and roaming users. Another advantage of the Cisco solution is the availability of client software for several operating systems including linux, Windows CE and PalmOS.

The hardware clients (PIX 501 firewalls) are used for remote offices and will allow several PCs and a server to share the connection if required.

Roaming and home users are provided with a CD that installs Cisco's software client, a Citrix client [18] and access software for a virtual ISP (iPass [19]).

After

Firewall

The in-house firewall was replaced with a managed service provided by a specialised ISP. Their facilities had already been certified to the level required. The solution uses a number of firewalls and includes intrusion detection, email virus detection and should greatly reduce the residual risk. The connections to the ISP use fibre optic cables that are physically secured to ensure information confidentiality and integrity.

FedLink

The services provided by the new ISP include routing email to other participating organisations through the FedLink intra-agency VPN.

Direct connections to Agency C

For the connection to agency C we elected to use a dedicated firewall (we added one of our service provider's standard firewalls between the router that had opened the back door and our network). In this case, forcing all traffic to traverse the two organisations firewalls would have added considerable latency to every transaction and at least one link in the chain was often close to saturation.

Joint A-B team

This team has staff on a specific subnet on each of the two organisations' networks. They have access to specific applications on the other network through a dedicated firewall. The two groups share servers on a DMZ connected to this firewall. The Citrix servers we initially deployed for the VPN are now being used for the staff located in agency B as well as the remote offices, roaming and home based users.

VPN

The VPN concentrator was located in the ISP's premises using dedicated ports on the firewall. The Cisco 3000 VPN concentrator has two ports - untrusted (encrypted data) and trusted (plaintext). Both are connected to different ports on the firewall (Option B in figure 1).

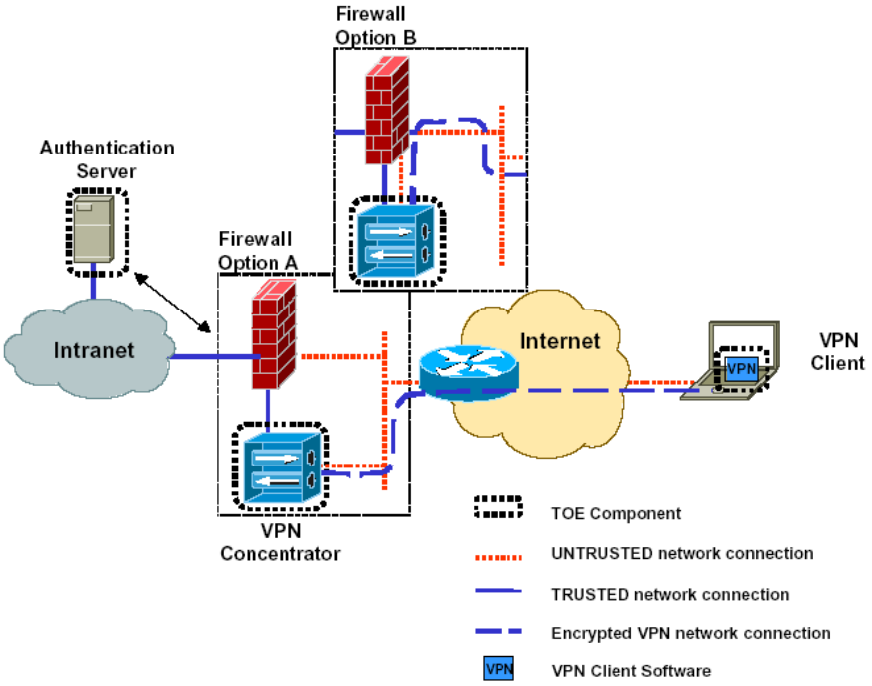

Figure 1 – Location of VPN concentrator in relation to the Firewall is as per option B. Diagram courtesy of Cisco[20]

Sending the plaintext data through the firewall achieves two things: firstly, our ISP can monitor the plaintext using an IDS function in the firewall and, secondly, the firewall rules provide detailed control over the access rights granted to VPN users. Different groups of users can be assigned addresses from different subnets when they authenticate and the firewall grants rights based on this. Having the encrypted data flow through the firewall allows it to enforce limited access controls on behalf of the VPN Concentrator.

Remote Offices

For the remote offices installed to date, the biggest issues result from the 800 ms latency due to the satellite link and the asynchronous nature of the link (512 kbps downlink but only 128k uplink). We will add several other remote offices to the network as soon as their Internet access is installed.

Mobile Users

A pilot of the VPN has completed satisfactorily. Rollout will commence as soon as the paperwork (procedures and user documentation are completed).

A key outstanding security issue relates to ensuring the remote computers do not provide an attack vector into the internal network. This issue is discussed further in Appendix 1.

Did we achieve our objectives?

1. Replace the aging firewall with one that complies with the requirements for a Protected level Gateway.

    - The ISP's facilities are certified as meeting this requirement.

2. Replace the dial-up remote access system with one that ensures the confidentiality and integrity of information transferred between systems.

    - The use of IPSec ensures confidentiality and integrity of the information.

3. Use the existing network directory for authentication probably via the current dial-up system's Radius server.

    - Authentication uses a shared secret to authenticate the client device (PC or PIX 501 firewall) and then authenticates the user's credentials with a Radius server that in turn queries the network directory.

4. Provide several layers of security between the Internet and the internal network.

    - There are several firewalls from different suppliers between the border router and the internal network.

    - In addition there are Intrusion Detection Systems and where possible application level proxies or other data inspection systems.

    - All email is checked for viruses by the ISP as well as by the desktop SOE.

5. Restrict remote users access to the internal network without overly restricting their ability to work.

    - Most functions can be achieved through Citrix or a browser. Firewall rules can be used to fine tune access to specific services as required.

    - Only services specifically approved for remote use are enabled.

6. Use products that have been independently evaluated under the common criteria wherever possible.

    - The firewalls and VPN system are on the EPL. The VPN is still in evaluation and the organisation has accepted the risk that it may not complete the process.

The Future

In order to cater for travellers who don't want to carry a notebook PC we will no doubt be asked to provide access to the system from PDAs and similar devices which currently don't inherently provide a high level of security.

We also intend to develop a 'Live CD' based on linux. This would allow the staff member to boot a trusted environment on an otherwise untrusted PC. This is discussed further in Appendix 2.

The Cisco VPN is still under evaluation for Common Criteria certification. Once this is completed agency A will need to ensure that the implementation matches the configuration that passed the evaluation[5].

Conclusion

The two projects successfully removed several significant vulnerabilities in agency A's network perimeter and improved the communications available to several remote offices that previously had extremely poor network access. Feedback from the pilot users suggests the VPN facilities will substantially improve on the dial-up remote access system it is replacing.

[5] The final version of the Security Target [20] and a certification report are published when an evaluation is completed.

Appendix 1

Security issues with remote worker's computers.

PCs and notebook computers used by road warriors and telecommuters present an additional set of risks to the network. This is particularly so if the computer is connected to an 'always on' ADSL or cable broadband connection or is using a wireless network. An example of a recent attack targeting home computers is the Migmaf trojan which utilised over 1000 home computers to re-direct users to pornography sites [21].

Although the Cisco VPN client includes a 'stateful firewall' (a version of Zone Alarm), this only protects the system while the VPN is enabled. To provide continuous protection an alternate personal firewall product should be installed (eg Zone Alarm Pro). To fully secure the PC it should have all known vulnerabilities patch, be locked down using the industry consensus benchmarks available from the Centre for Internet Security [22] and have current virus detection software.

Ideally these aspects of the security policy should be enforced whenever the PC logs into the VPN. Steins (2003) [23] has an example of a means of achieving this on a Cisco 3000 VPN using Zone Alarm Integrity [24] to enforce the policy.

We are considering modifying the agencies current SOE to utilize Novell's ZENworks to ensure the policies are enforced whenever the PC is connected to the network either directly or via the VPN. ZENworks will also be used to deliver the virus software updates and critical patches.

Computers used for Home Based Work will often be connected via always-on broadband connections. Our preferred solution is a low cost hardware firewall such as a Netgear RP114 [25]. These incorporate a router, 4 or 5 port switch and basic filtering capabilities and are designed to provide a small LAN isolated from the ADSL or cable broadband connection. They offer a better solution than the Cisco PIX 501 if the connection is to be used for both private and business purposes.

Appendix 2 – A Customised Knoppix Live CD

Many of the agencies staff will need access to the VPN in situations where they either don't have access to or can't use an agency provided notebook or PC. In order to cater for their needs we are developing a 'Live CD' based on the Knoppix-MIB linux distribution [26]. This CD should be able to boot in most PCs less than 3 years old and normally will not modify the PC's hard disk.[6]

As the Knoppix environment is entirely resident in RAM (apart from any data swapped to the encrypted swap partition) it provides a highly trusted environment from which to access the VPN. The CD will include a browser, Cisco VPN client and Citrix client. Users can store configuration files and their home directory on either a floppy disk or USB memory drive using an encrypted file system if required.

Knoppix appears to auto-detect a wide range of hardware and the Knoppix-MIB distribution adds the encrypted swap and removable file systems.

The major issue we expect with this approach are the training issues for users unfamiliar with linux and the poor support for internal modems [27]. These limitations will undoubtedly restrict its usage.

[6] Knoppix-MIB will use a linux swap partition if one exists (data is encrypted) and may prompt the user if it needs to create a swap file on a windows partition – in this case the file is encrypted and deleted on shutdown.

References

[1] Attorney Generals Department. "Protective Security Manual", 2000

[2] Defence Signals Directorate, "Australian Communications-Electronic Signals Instruction 33" (ACSI 33) 2000 (http://www.dsd.gov.au/infosec/acsi33/acsi_index.html)

[3] For information about FedLink see http://www.fedlink.gov.au

[4] For information about the Common Criteria see http://www.commoncriteria.org/

[5] Defence Signals Directorate, 2000, "Gateway Certification Guide" http://www.dsd.gov.au/infosec/Gateway/

[6] Ethier, Patrick and Corbeil, Jessie (ed). "ISAKMP and IPsec in the VPN environment", 2000, http://www.secureops.com/vpn/ipsecvpn.html

[7] Virtual Private Network Consortium (See http://www.vpnc.org)

[8] http://www.ietf.org/rfc/rfc2401.txt is one of a number of RFCs that describe IPSec

[9] See http://www.openssh.org

[10] See http://wp.netscape.com/eng/ssl3/

[11] Defence Signals Directorate. "DSD Security Policy Advisory on the Use of SSL" Version 1.0, 7 June 2001 http://www.dsd.gov.au/infosec/publications/SSL_policy.html

[12] Linux FreeS/WAN is an implementation of IPSEC & IKE for Linux (See http://www.freeswan.org/)

[13] See http://Openbsd.org

[14] See http://www.dsd.gov.au/infosec/aisep/EPL/ns.html#Kyberpass41

[15] See http://www.ietf.org/rfc/rfc2661.txt

[16] Microsoft. “Microsoft Privacy Protected Network Access: Virtual Private Networking and Intranet Security” 1999 http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/nwpriv.asp

[17] Cisco Systems Inc. “Cisco VPN 3000 Series Concentrator”, June 2003 http://www.cisco.com/warp/public/cc/pd/hb/vp3000/prodlit/vpn3k_ds.htm

[18] See http://www.citrix.com

[19] See http://www.ipass.com

[20] Cisco Systems Inc. “Security Target for Cisco Remote Access VPN”, Version 1.3, September 2002.

[21] The Age, “Trojan uses home computers as porn proxy”, 11 July 2003, http://www.theage.com.au/articles/2003/07/11/1057783339267.html

[22] See http://www.cisecurity.org

[23] Stines, Michael, 2003. “Remote Access VPN – Security Concerns and Policy Enforcement” http://www.sans.org/rr/paper.php?id=881

[24] See http://www.zonelabs.com/store/content/company/corpsales/intOverview.jsp

[25] See http://www.netgear.com/products/prod_details.asp?prodID=93

[26] See www.knoppix.net for the project’s home page and http://www.bouissou.net/knoppix-mib/doc-html/Knoppix-Mib.html for knoppix-MIB

[27] Walbran, Sean “Linmodem-HOWTO” The Linux Documentation Project March 2001, http://walbran.org/sean/linux/linmodem-howto.html

Last Updated: September 24th, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive