Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Remote Access using Telstra Dial IP

This paper will demonstrate how the real-world security problem of remote access to an Enterprise network was addressed and validated (post-implementation) through the Internet Security Alliance's (ISA) Common Sense Guide for Senior Mangers. The ten practices in the guide will be referred against, to illustrate the security environment that existed prior to the project, the criteria by which remote access solutions were assessed (and why the adopted system chosen) and the security improvements the solution has provided...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Jamie Rossato
GSEC, Version 1.4b, Option Two.
Title: Remote Access using Telstra Dial IP

Introduction

This paper will demonstrate how the real-world security problem of remote access to an Enterprise network was addressed and validated (post-implementation) through the Internet Security Alliance's (ISA) *Common Sense Guide for Senior Mangers*[i]

The ten practices in the guide will be referred against, to illustrate the security environment that existed prior to the project, the criteria by which remote access solutions were assessed (and why the adopted system chosen) and the security improvements the solution has provided. In addition, the author will discuss how the actual implementation was conducted and key issues encountered during it.

As a new member reporting to the Enterprise's CIO, the author was made responsible for implementing "a remote access solution that would satisfy the needs of the business". As the project manager I worked with system administrators and telecommunication technicians. Where over a period of four months a number of existing ad-hoc remote access arrangements were supported whilst alternate solutions were investigated & assessed before the selected solution, *Telstra Dial IP*[ii] was chosen and implemented.

Two years on, the solution continues to fulfil all the criteria it was measured against, providing a system a processes that provides an enhanced level of remote access to users, removed a number of vulnerabilities that previously existed and delivered a level of security that previously did not exist.

The ISA Guide

The ISA Guide proffers ten practices managers (businesses) should follow or be aware of. These are:

1. General Management,
2. Policy,
3. Risk Management,
4. Security Architecture and Design,
5. User Issues,
6. System & Network Management,
7. Authentication and Authorisation,
8. Monitor & Audit,
9. Physical Security, and
10. Continuity Planning & Recovery

These practices reflect "ten of the highest priority and most frequently recommended security practices as a place to start for today's operational systems."[iii] and form a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

sound basis from which project managers and system administrators can assess systems either proposed or pre-existing.

Previous Situation

The Enterprise is an Australasian business, which operates mostly along independent divisional lines with few centralised business services. IT systems and support had developed along divisional lines, with equipment purchasing conducted locally and IT personal reporting to divisional management. The business WAN (primarily Frame Relay) was understandably, un-homogenous and fragmented. In addition to this, each division had (to a varying extent) a number of mobile and out of office personnel. These included sales staff, home workers, company executives and small 1-2 person offices where WAN connectivity was considered uneconomic.

To support remote access needs, system administrators employed a number of methods to support these out-of-office users. These included:

- Single analogue modems connected to individual workstations on the network;
- ISDN services with routers installed at the users homes and on the network;
- Turn key remote access products (i.e. Shiva LAN Rover) with a finite in-dial capacity;
- Web enabled exchange services; and
- Email forwarding, either to free internet email accounts (i.e. hotmail) or business supplied email accounts (i.e. ozemail)

While each of these solutions in isolation may have provided remote access, taken altogether they represented a significant security risk to the Enterprise. *Risk* is understood to be a combination of *threat* and *vulnerability*[iv]. The threats to an enterprise organisation are numerous and one of the main threats is unauthorised access to the network, its services and its data. This type of threat is omnipresent and continues to this day – in 2002 ninety percent of respondents (primarily large corporations and government agencies) to the Computer Security Incidents "Computer Crime and Security Survey" detected computer security breaches over the last twelve months.[v] In 2000 (the time of the project) there were over 21,000 incidents reported to CERT, growing to over 52,000 in 2001.[vi] It is also recognised that the number of remote users worldwide will continue to grow – more than 130 million business users by 2004 according to Gartner[vii]. Any network connected to the internet, or supporting remote users is therefore vulnerable to attack from these sources – and like a warehouse with too many entry points, poor perimeter fencing, too few guards, uncoordinated patrolling and management that didn't enforce any rules – there existed within the Enterprise a very real risk that someone was going to break in and steal information and resources- with a very good chance of not getting caught!

The following is a brief outline of some of the issues that existed and why they represented a security risk to the Enterprise.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Cost – For some divisions who had local users, there were few problems (in Australia and New Zealand local calls are untimed), however inter-state and international users often generated huge bills; particularly when they if they encountered poor line performance, drop out (requiring them to call back) or if due to poor configuration of their mail settings in Outlook. To circumvent this problem, many remote users had their business email forwarded onto a private account for browser based access from any computer with internet access - including 'hotmail' accounts. For employees dealing with sensitive company information, having all emails directed unencrypted over the internet (including some that may have been for internal communication only) introduced the threat of a rival business possibly intercepting and reading the information.

Scalability – During periods of peak demand (4pm to 9pm) many users could not access the limited number of modem lines available. System administrators were required to add new services (another cost) and in one instance, a user frustrated with long delays in connecting, installed (without authorisation) a modem on their workstation and connected it to their phone line before leaving for the day so as to avoid the "line busy" signal. This flagrant disregard for network security (introducing a back door vulnerability) highlighted the lack of clear policy on remote access as well as the need for a solution that could meet demand during peak periods.

Manageability – There were many problems in this area – No policy for adding users, nor any mechanism for reporting to IT when users left or transferred between divisions. Often weeks could pass before system administrators were notified. The risk of a disgruntled employee (the threat) accessing the network with their old access privileges (the vulnerability) and conducting a malicious attack was quite possible. There was no central repository of information listing who had access; when it was granted; what they could access, etc. Without such information the ability of system administrators to respond to security incidents effectively was hampered.

Complexity – The various systems in place were not coordinated, and as stated before, no central list of users. Users from different divisions would 'shop around' looking for the best remote access service available. In some instances employees would have multiple remote access accounts in place "in case this other one doesn't work" or one account for 'working from home' and another for 'interstate & overseas travel'. Users from one business found they could access another division's services (and information!) by using that division's remote access, bypassing internal security arrangements.

While each of these proved a case for change, examining at the previous environment through the ISA's ten Practices, further reinforces the risks that existed and the need for change.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

General Management - There was no organisation or adequate resources in place to provide Enterprise level remote access; Poor (or no) coordination between divisions; little in the way of management oversight of remote access use; and cost, rather than information control was the management consideration.

Policy - No Enterprise remote access policy and little in the way of divisional policy – without this there was no authority for system administrators to enforce user behaviour, set neither configuration standards, nor guidance on activity such as how often to audit access logs.

Risk Management - No risk evaluation was conducted that would assist in identifying threats to assets; what the vulnerabilities with the existing systems were or how these risks could be mitigated.

Security Architecture and Design - For a company as large as the Enterprise, site wide security architecture should have been in place. Instead, a patchwork of solutions existed and few, if any, layers of security. There was no redundant remote access solution within any of the divisions (other than that within other divisions). There was insufficient capacity in a number of the existing systems– i.e. One division with several hundred personnel had a Shiva LAN Rover with only four modems for dial in access.

User Issues - There was almost no user accountability – users saw security as an IT issue, not something everyone has responsibility for. Enforcement of user access and removal was ad-hoc and poorly co-ordinated. Minimal user IT security education existed and few understood the reason why "remember my password" should not be selected on their laptop. End user vulnerability was also an issue as there was no common standard for remote user systems to be configured to. As Tim Redhead points out "… many end-point computers are often poorly maintained due to shortages in time, skills or other qualities …. Vulnerabilities at remote access end points lead to risks of application level attacks"[viii]

System & Network Management – As previously mentioned, there was no centralised management (or view) of remote access. In some parts of the organisation perimeter access was very strong (i.e. multiple firewalls at an email gateway) while in other parts very weak (i.e. network computers that dialled out to access the internet). Remote user's computers had no standardised configuration; often where there was logging it was rarely audited and undisciplined change control existed.

Authentication and Authorisation – From a management perspective the myriad of methods that the enterprise employed to support remote access, meant that the confidence that the person connecting remotely was an authorised employee could not be high. The absence of a clear policy or guidelines on providing remote access for third parties (vendors, clients, etc) meant that providing access to one part of the business may have inadvertently given them access to other parts of the business.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Monitor & Audit – No network monitoring tools were in place and auditing of systems that were capable of being accessed remotely was rarely conducted. Risk awareness amongst some system administrators was low and in others too much confidence placed either in their ability to 'detect' incidents or in the capability of the existing technology to keep intruders 'out'.

Physical Security – Control of the physical systems in place to manage remote access varied among the divisions. One division had a server room secured by a swipe card, while another had a server room with no lock, two floors from where the IT staff worked.

Continuity Planning & Recovery - There was no plan to provide redundant remote access within any of the divisions and in the event a business site had to be evacuated, there was no policy, or guidelines on which members of staff would have priority access to remote services.

Overall, the environment to support remote access was one in which a large number of security vulnerabilities existed – the solution would need to address the twin issues of accessibility for the remote user and security for the enterprise network.

Undertaking the Project

On being assigned the project, a plan was developed which consisted of five phases:

1. Determine the requirements of the business and identify the risk;
2. Select the solution;
3. Implementation – infrastructure, training, policy; and
4. 'Go live' & progressively migrate users from old system to new.

The implementation itself would require support of existing systems during all phases of the project to support any 'roll back', in the event unforseen issues arose with the chosen solution.

1. Determining the Requirements

In undertaking a requirements analysis, this author lost count of the number of times they were told "My requirements for remote access are quite unique." As such a culture of 'making exceptions' and allowing deviation from what most of the system administrators acknowledged as 'sound' security practices. By looking at the <u>what, when & how</u> of each <u>who</u>, we could begin to determine what services they required outside the Enterprise network. This was essential, as once we understood the users we could, from a security perspective, ensure the Enterprise remote access architecture was properly configured.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The results from the investigation were encouraging; most users had more in common than they realised (or were prepared to admit!). The key findings were that: most users connected remotely to the network from home using a business provided computer; that within each division were between 5-20 users who worked during business hours from a remote site (no WAN connection to the Enterprise) and each divisions' management travelled inter-state or overseas on a regular basis.

The majority of employees required access to just email, the internet and their home directory (to work on documents, spreadsheets etc). The remainder were system administrators and system developers who required access to diagnose and remotely manage network services. Both types of users typically accessed the network after office hours for one or two hours, with demand peaking between 6:00 – 10:00pm. The remote office users typically wanted to remain on all day, primarily to check email.

As already detailed previously, how they achieved remote access was also captured. Access logs (where available) were examined and where possible, a week or so worth of data was captured from existing systems. Where high risk means of access (such as modems on desktops) were identified during this phase, these were removed and users moved onto a system that reduced the vulnerability of the Enterprise to attack.

Overall we found users wanted to connect "from anywhere at any time, as if they were in the office."

2. Identify and assess the solutions available to the business

Overall business expenditure on IT security within the Enterprise was low – the META Group, pre Sept 11 2001 identified 82% of their business survey respondents spent less than 5% of their IT budget on security[ix] and the business required a solution that provided low cost remote access, with security as a secondary consideration. The system would have to support a range of different connection speeds (from analogue modems through to ISDN). Ideally the solution would support a central accounting and auditing system.

Options: Due to the size of the organisation, there were two solutions that seemed to best suit - either remote access using an ISP and the internet (secured by a VPN); or a private dial up service connected to the Enterprise. Deploying additional modems to other states was considered but discounted early due to the cost of equipment (especially when factoring the need to provide for peak periods), the need purchase and rent additional in-dial lines and the overhead such an installation would place on administrators (both in set up and maintenance).

It was also agreed early in the project that a central authentication and accounting server was vital if proper enterprise management and auditing were to be possible. The RADIUS (Remote Authentication Dial In User Service) protocol, due to its wide

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

use, open design, functionality and security features was chosen to provide this. The means by which users would connect to the RADIUS and then the Enterprise network, having been authenticated and a record of their session start logged.

VPN's: "A VPN (virtual private network) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network."[x] Tunnelling technologies (PPTP[1], L2F[2], L2TP[3]) are used to establish a secure connection through which can pass data between two authenticated users. The advantages of an internet VPN solution are that by employing the internet to connect remote users, the cost to connect users from anywhere in the world is substantially reduced.

Other benefits include the access speeds by which users operating from their home can take advantage of high speed internet connectivity, the ubiquity of internet access in most parts of Australia and overseas. Remote users install VPN clients and the business (Enterprise network) establishes a VPN server "on" the internet. One downside to adopting a particular VPN solution is that many of them are proprietary based and many VPN products only support specific types of VPN connectivity[xi]

Dial Up Service: The alternative to VPN's is maintenance / management of direct dial in service with a central NAS providing access into the organisation. For a small to medium business, the majority of dial up services can be resolved with a modem bank and in-house RAS. The problems with this solution in large national businesses are the expense in installing large numbers of modem banks – however this is just the start - "*Studies show that equipment costs are only 20% of total remote access costs: the rest is for support of remote users and managing the equipment.*"[xii] This management and support overhead on top of costs such as paying monthly rental on either a free call (1800) or local call (13) number for users, or toll rates for international users, can be significant.

3. Selecting the solution

Kaeo identifies five areas that an enterprise security architecture must cover are Identity, Integrity, Confidentiality, Availability and Audit[xiii] Both solutions, if properly implemented and configured would satisfy these areas.

Knowing which users on the Enterprise network are authorised and which are intruders is critical! Identity protection is a combination of sound user practices (have hard to guess passwords, no "remembering passwords") and an architecture that protects the more sensitive areas of the network from others. Integrity ensures that the selected architecture provides security both at the perimeter and in depth. This is particularly important when considering remote access, as one key area of security

[1] PPTP = Point to Point Tunneling Protocol
[2] L2F = Layer 2 Forwarding
[3] L2TP = Layer 2 Tunnelling Protocol

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(physical security) cannot be always be assured. In this instance, logical mechanisms such as how users are authenticated and authorised must be in place. Both VPN and Dial Up solutions support just such protocols (i.e. RADIUS) and so are equally acceptable for remote access. Confidentiality is about protecting the data, both technically and by business policy and enforcement. Remote access is all about availability. Ensuring authorised users can get to the data they need to, while denying that availability to intruders or malicious code. Finally auditing, so the business can see what is occurring with remote access. Compliance to policy should able to be assessed from audited records and security incidents capable of being investigated from information on hand from the system. Importantly, and in addition to these, the solution should be simple for the user to employ and for system administrators to manage; as complex procedures will put-off users and complex systems are a drain on an administrator's time.

Whilst VPN was a promising option – several issues worked against it. Firstly was the need to set each remote user up with an account by which they could access the internet. Each user during connection establishment and while 'online' was vulnerable to hacker exploits. A user for example, may have established a VPN to the Enterprise and while connected, surf to their personal email account (i.e. hotmail) and open an email containing malicious code – if their system was not well maintained, not only is their machine now infected, but the code could propagate into the Enterprise network via the VPN. It was decided by the project team that it was preferable for users to access the internet only via the businesses internet POP with several layers of perimeter security (which includes blocks to web-mail sites like hotmail). Not only would this be more secure, remote user "surfing" could be monitored and audited like any other user.

While the cost for per individual for internet access could be considered relatively low (one example quotes US$25 per month[xiv]), the Enterprise had experienced problems managing the individual ISP accounts – as they were paid for by the business but "owned" by the individual, when these users departed the company the accounts proved difficult to cancel. Hours were taken up by IT staff trying to manage and administer such accounts. Additionally, each VPN connection consumes bandwidth at the internet POP. While the enterprise had adequate internet access, management raised concerns over the possible impact on their e-commerce systems and possible problems with Quality of Service during peak periods.

There are also the problems faced in installing, configuring and managing VPN clients – As highlighted in a recent InternetWeek.com article "The market is now realising there is a great amount of difficulty, and often hidden costs, associated with VPN client offerings."[xv] Lucent also note "Implementation of VPNs is a complex process … organizational and managerial issues are as significant a challenge as technological issues."[xvi] The cost and time to distribute encryption keys and digital certificates are two factors, as is the overhead such support places on the system administrator (software conflicts, help installing etc). This overhead on administrators was given considerable weight during the assessment.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The decision to select Telstra's Dial IP (Dial Up) solution was made in light of the problems with VPN and for the advantages Dial IP offered over the standard Dial Up solution:

- A single (unique) number that could be employed Australia wide (a 019 number) – This meant users couldn't mix numbers up, or select the wrong inter-state number.
- Support for multiple frame access into the Enterprise network – The project had funds allocated for two POP from the Dial IP "cloud" into the network. This was important in providing a level of redundancy (such as loss of power at one of the POPs). The POP's could be scaled accordingly.
- Global POP – While there were multiple numbers for global roaming & limited countries (at the time), there was no need to support a second array of POP's for international users.
- 24 x 7 Monitoring – The system was maintained by personnel whose sole role was maintenance and management of the Dial IP system and who had a much greater technical management system than the Enterprise would had ever considered developing.
- 34 x 7 Fault management – Again dedicated technical staff could alert Enterprise system administrators in the event of problems with the RADIUS server(s), access at a Dial In POP, or the connection(s) between Dial IP and the Enterprise network.
- Supported dial up from analogue 33.6 kbps to ISDN 128 kbps – This covered all our users and all conceivable connection types. In addition, the Service Level Agreement with Telstra ensured there was excess capacity for users to call in on.
- Passwords never transmitted over internet – The connection is established between the remote caller and the enterprise POP through Telstra's private network.[xvii]

Another key argument that came out favouring the direct dial in service was that users, if they required access to the internet, could (and should) access it via the Enterprise Internet POP where security measures were stronger than if they dialled up onto the internet from their laptop.

4. Implementation – Infrastructure, Training & Policy

Having decided to proceed with Telstra Dial IP in early July, implementation was split into two within the project team. Infrastructure preparation would be assigned to the technical staff and Policy development and training with management.

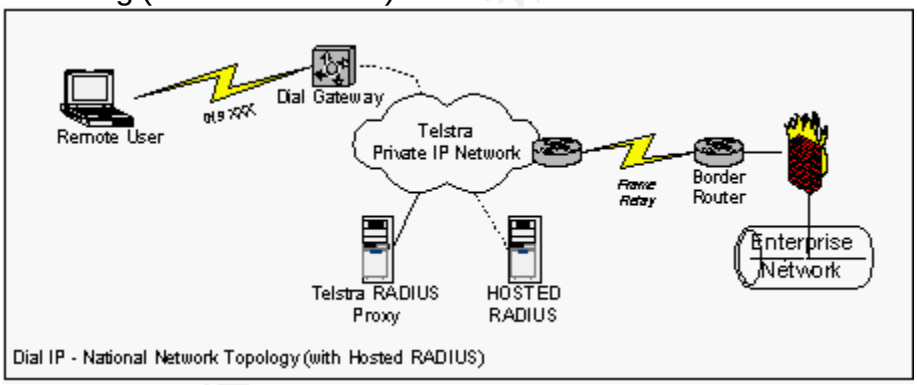
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Topology: The overall network topology for Dial IP at the Enterprise site is quite simple. Telstra provide a central RADIUS Proxy which shares a 'secret' with each customer's RADIUS (of which there can be up to three per customer[xviii]). Once the RADIUS has authenticated the remote user and allocated configuration information material according to its database, the remote machine has a connection established with their network, typically over a frame relay link.

To provide a level of redundancy and load share bandwidth, two frame relay connections from the Dial IP network into the Enterprise were made. This particularly suited the divisions whose mobile workforce was divided between the two largest Australian states of New South Wales and Victoria. It also provided geographic diversity so as to limit the impact of any disaster on remote access in one of these two states. This was in-line with Telstra's own redundancy arrangements[xix]

The project team, in discussion with management agreed that management of a RADIUS server was not an effective use of neither system administrator's time, nor a skill set that was required by the businesses. It was decided that a RADIUS server hosting and management option would be adopted. While there were some concerns over having the RADIUS outside of the Enterprise network, it was believed that the system could be managed more effectively, cheaply and securely by Telstra rather than by purchasing, configuring and internally maintaining two RADIUS servers (at least two would be required for redundancy).

The diagram below illustrates the topology used by the Enterprise for Australia wide Roaming (one POP shown).

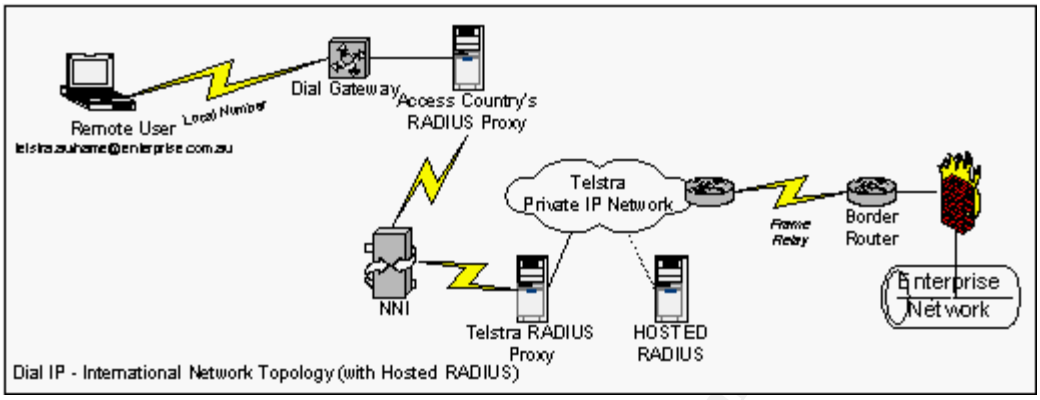


For International users, there are two options – either call the 019 number using an international call (i.e. *+61 19 xxx*) or use the *Global Roaming* option. This option makes use of the agreements Telstra has with other countries carriers or ISPs. An international pool of users can be supported on the same RADIUS as domestic users. International users (of Dial IP) are distinguished by the domain header (telstra.au) in the user name. When overseas a user dialling into a local or national POP is connected to the nearest RADIUS Proxy (or similar Network Access Server device). The domain header tells that proxy that information about the user should be located on the Telstra RADIUS Proxy in Australia. Via a Network to Network

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Interface (NNI) an encrypted connection is made between the proxies. From here connection establishment is treated much like a domestic connection.

The diagram on the next page illustrates the topology used by the Enterprise for International Roaming (one POP shown).



The technical team ordered and configured the border routers. These routers even though connecting a private (Enterprise) to private network (Telstra Dial IP) were configured to provide the first layer of security within the Enterprise network. Access Control Lists (ACL's) were established to deny certain types of traffic, such as "obvious" spoofed traffic (traffic outside the allocated IP range). Each border router was then interfaced directly into an internal Enterprise firewall. These firewalls were already in use within the network to keep parts of the business networks isolated from other areas. Rule sets were added to allow the Dial IP ranges through with varying levels of access, depending on the purpose that range had been allocated for (i.e. One range allowed for access to the internet thorough the while another did not). This provided further security in-depth and provided another mechanism by which activity could be accounted, monitored and audited. While both the router and firewall were being configured, data was being compiled for loading onto the RADIUS servers. The RADIUS protocol is highly configurable and supports a wide range of services. As well as user name & password, the type of transport or network protocol, IP address (or address range), allocated domain name services, and session lengths can all be defined and assigned to the user on successful authentication.

While not all the features were adopted, the project implemented several of them. IP ranges were allocated (*10.x.x.x*) and split into six different subnets- three for each of the two POPs. The first and smallest range was for system administrators and certain business application "super users"; the second range (and the largest) for users requiring access to most of the network applications and internet access. While the last IP range was for users who required remote email access only. An Idle limit (the maximum time the connection can remain inactive) and a Maximum Session Length were established to ensure users couldn't login and "walk away" from their machine for extended periods of time.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

For the management team, the focus was on putting processes in place that would ensure the system continued to provide secure remote access once the project was complete. Work commenced on a Remote Access Policy for users, a training and instruction manual, a document for system administrators on configuration requirements and importantly, procedures for obtaining remote access. It was important that the policy mitigate the risk of remote access. The approval process was structured so that each application required an 'endorsee', usually a senior manager or the CIO. Once approved and the user had acknowledged they had read the policy; remote access had to be configured by an authorised administrator according to the documented procedures (SOP[4]) attached to the policy.

The policy also made users aware that their use of the system was monitored and regularly audited. A strong password policy was introduced – enforcing the use characters and numbers. User education was undertaken, being was a combination of material released on the company intranet, slide presentations to business divisions and emails to users as they were added to the RADIUS database. Procedures for auditing and accounting for user activity were developed and worked through with management.

5. 'Go live' & user migration

In mid October 2000, the service went 'live' with some 50 users trialing the system. By November the number had grown to 150 and the first reports to management were produced. The overall response was positive and very encouraging for the project team. As users were migrated over from their old system to the new one, the team was able to decommission modem banks, close internet accounts and stop automatic re-direction of email. November was the first month in which international roaming was used. As is usually the case, everything went well during user testing and training in the office - once 10,000 miles from the closest system administrator, problems began! Fortunately the business was better able to diagnose the problem with Dial IP than it had been able to previously and connectivity was eventually restored, with the problem identified as the user attempting to dial from a hotel network (rather than phone) port.

One area of concern was managing adds/deletions/changes to user information in the RADIUS database. At the time the system went live it required human interaction between the Enterprise administrators and Telstra Dial IP services. An online management system initially proposed for delivery late 2000, (now scheduled for mid 2003) would have enabled Enterprise administrators to make amendments themselves, without human intervention. However this was expected to be resolved relatively quickly, and so in the interim a list of Enterprise personal authorised to make additions or alterations was sent to Telstra to ensure users couldn't simply ring up and make changes to their own log-in or password.

[4] Standard Operating Procedure

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Validating the Impact of the Project

Validating the new environment with ISA's Practices, demonstrates how the implementation of the Telstra IP solution, in conjunction with other activity lead to an improved security environment:

General Management - Remote access was centrally co-ordinated. As the majority of technical support was outsourced to an organisation with dedicated remote access resources, the Enterprises system administrators could dedicate their efforts into other, equally important areas such as standardised builds & configuration. With management involved from the very start of the project they 'bought into' the solution and became enthusiastic supporters and adopters of the solution. A mechanism for approval and revocation now existed - no longer could a user approach a system administrator to gain remote access – the user's manager became the 'owner'.

Policy - The Enterprise now had a Remote Access policy – issued to all users before their access was activated. The policy was published on the company intranet and users had to acknowledge they read and understood what the policy was. System administrators could now enforce user behaviour and were aware of their own responsibilities to the users.

Risk Management - Having undertaken a review of the remote access environment, management and system administrators had a greatly improved understanding of the vulnerabilities that existed on their network. In undertaking the remote access project, a number of other security related projects spawned from it such as development of an enterprise IT security policy.

Security Architecture and Design - The Enterprise now has a single remote access architecture; layers of security were provided through the RADIUS and Firewalls; multiple POP's mitigated the risk of losing all remote access should one site have a power failure (or similar such incident).

User Issues - User accountability – with a clear policy and visible enforcement of it though the User Access Application process and reports to divisional management, users began to take steps towards thinking of security as 'their problem as well'. By outsourcing the technical support and management, the enterprise's system administrators were free to concentrate on proper user setup and auditing.

System & Network Management – Remote access was now better controlled; 'perimeter' security was no longer compromised with users needing to install modems on the desktop; logging of remote user activity was improved and change control (adding and removing users) was better as it was all centrally coordinated. There was also "defence in depth" – connection to a hosted RADUIS server (monitored 24 x 7) then once authenticated and authorised connected to one of two POPs, through a border router and firewall onto the network.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Authentication and Authorisation – The RADIUS protocol provides strong mechanisms for user authentication and authorisation and as the process is conducted from within a private, rather than public network, there is a greatly reduced threat from "hackers" monitoring or capturing activity.

Monitor & Audit – Remote access is continually monitored by Telstra and the enterprise receives log reports each month (or more frequently if required); Management have better visibility and oversight over their remote users than had previously been the case. Documented and practised 'incident response' plans were put in place, and despite being 'outsourced' the ability of the Enterprise system administrators to obtain timely access to RADIUS logs from Telstra for auditing has proven to be achievable. The table below provides an example of the amount of information recorded and available for audit if required.

	Attribute	Attribute Number	Example Value	Explanation
START RECORD DATA	Time		Tues Oct 1 9:30:11 1997	Time Record received by RADIUS
	User-Name	1	"jsmith"	Name user logged in with
	NAS-Identifier	4	144.130.4.5	IP Address of Radius Proxy
	Acct-Status-Type	40	Start	Type of accounting record - start or stop
	Acct-Delay-Time	41	10	Seconds delay before record was forwarded
	Acct-Session-Id	44	"C0030EE702F6"	Accounting Record Identifier
	Framed-Protocol	7	PPP	Framing protocol used
	Called-Station-Id	30	"4321"	Last 4 digits of number called by user.
	Calling-Station-Id	31	"0396403xxx"	Telephone number the user dialed from.
	Rating Advice	249	"A1"	Real time call zone advice
	Framed-IP-Address	8	145.200.200.20	IP Address allocated to user
STOP RECORD DATA	Stop Time		Tue Oct 1 11:56:57 1996	Stop time of session. Calculated from time received and delay time.
	User-Name	1	"jsmith"	Name user logged in with
	NAS-Identifier	4	144.130.4.5	IP Address of RADIUS Proxy
	Acct-Status-Type	40	Stop	Type of accounting records
	Acct-Input-Octets	42	121980	Octets sent to the network
	Acct-Output-Octets	43	616916	Octets received from the network
	Acct-Input-Packets	47	4736	packets sent to the network
	Acct-Output-Packets	48	3917	packets received from the network
	Acct-Delay-Time	41	10	seconds delay before record was forwarded
	Acct-session-time	46	8813	length of session in seconds
	Acct-Session-Id	44	"C0030EE702F6"	Accounting Record Identifier
	Disconnect-Cause	195	45	Reason for disconnection
	Data-Rate	197	28800	Speed of connection (bps)
	Called-Station-Id	30	"4321"	Last 4 digits of number called by user.
	Calling-Station-Id	31	"0396403xxx"	Telephone number the user dialed from.
	Framed-IP-Address	8	145.200.200.20	IP Address allocated to user
	Framed-Protocol	7	PPP	Framing protocol used
	Rating Advice	249	"A1"	Real time call zone advice

Table: Provided by Telstra[xx].

Physical Security – Enforcing a password discipline on remote users and ensuring they backed up critical information onto the network were the steps taken to ensure improved physical security. Server rooms that housed the Dial IP routers were secured (locked or swipe cards access installed).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Continuity Planning & Recovery - Redundant remote access through multiple POP's provides a continuity of service to the divisions. While not planned for, some 12 months following implementation, some 60 users were unable to get to their offices on-site, but were able to work remotely using Dial IP for several days until they could return to their desks.

Ongoing Initiatives

Like any system, a continual cycle of review and improvement was undertaken to ensure serviceability and security are maintained. The team identified several issues shortly after 'go live'. One of these was the disclosure of one of the divisions that a business client required access to an Enterprise mainframe, which was currently supported by a direct dial-up into the mainframe. The solution was to have them connect via Dial IP with a login ID on the RADIUS and have allocated a static IP address. A revised ACL on one of the border routers and rule change on an internal firewall and each remote session between the client and mainframe was enabled via Dial IP.

One issue that did arise from having the RADIUS outsourced was the use of social engineering by some system administrators to add users or make changes without following the proper procedure (particularly if in a hurry). Despite several attempts at reducing this vulnerability which have proved to be partially (but not completely) successful; until the release of the online management system it is likely the existing arrangement will remain a weakness in the current system.

Post implementation, further developments were taken such as rolling out the solution in New Zealand and using the Australian based RADIUS server. This further improved security as the New Zealand network, linked to the Australian network had similar problems with remote access. It also gave Australian based management improved visibility of the activity of their remote users overseas.

Conclusion

In conclusion, the implementation of a centrally managed remote access solution effectively enhanced the security within the Enterprise. It removed a number of vulnerabilities, which given the present (and ever growing) threat of intrusion from external sources was critical.

The option of an internet based, VPN solution or the 'traditional' dial up solution ended up being a compromise, comprising both technologies through Telstra's Dial IP product. Dial IP met the key security criteria, in addition to meeting business needs. As important as the technology, was establishing a process that everyone could comply with. The process for adding and approving users, monitoring use, a standard for configuring laptops / PC's for remote access, training of users; the issuing of a policy, regularly conducting audits and the reporting of user activity to management all greatly improved the security within the organisation.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As the Enterprise workforce becomes even more mobile, it is important that in the rush to provide the access the user wants, that security is not forgotten or compromised. The selection of a remote access solution that is secure and in line with the ISA's ten practices will save a business, its managers and system administrators problems further down the track.

References

Allen, J; Mikoski, E; Nixon, K & Skillman, D; Common Sense Guide for Senior Managers; 1st Ed; Internet Security Alliance; USA; 2002. URL: http://www.isalliance.org (26 Oct 2002)

Allen, J; Alberts, C; Behrens, S; Laswell, B; Wilson, W; "Improving the Security of Network Systems"; Cross Talk: The Journal of Defence Software Engineering; Oct 2000. URL: http://www.stsc.hill.af.mil/crosstalk/2000/10/allen.html (15 Oct 2002)

Cole, E; Kolde, J & Northcutt, S; SANS Security Essentials II: Network Security, SANS Institute; USA; 2001

Derfler, F; Using Networks; Macmillian Computer Publishing; Indiana, USA; 1998.

Dial IP Technology Group; RADIUS Information Document; Telstra Corporation; Australia; 1998

Dial IP Technology Group; Telstra Private IP Solutions: Security Framework Overview; Issue 1.0; Telstra Corporation; Australia; 2000

Dial IP Technology Group; Dial IP Homepage. URL: http://www.telstra.com.au/dialip/index.htm

Giunta, P; "Virtual Private Networks: An Overview"; 2000. URL: http://lucent.com/livelink/162065_whitepaper.pdf (26 Oct 2002)

Kaeo, M; Designing Network Security; Cisco Press; USA; 1999

Mitchell, B; "Introduction to VPN"; Computer Networking; Jan 2001; URL: http://compnetworking.about.com/library/weekly/aa010701c.htm

Redhead, T; "Making the Risks Remote"; SEA; April 2002. URL: http://www.seanational.com.au/journals/journal-6/pdfs/se006_73-80.PDF (26 Oct 2002)

Salamone, S; "Keep An Eye Out For the Hidden Costs"; Internet Week; March 1999, URL: http://internetwk.com/VPN/supplement329-2.htm (26 Oct 2002)

Stephenson, P; "Securing Remote Access"; Network Computing; Jun 2002; URL: http://www.networkcomputing.com/602/602work2.html

Wright, J; "Bullish on VPNS"' Information Security Magazine; Jun 2002; URL: http://www.infosecuritymag.com/2002/jun/bullish.shtml (14 Nov 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"2003 Worldwide IT Benchmark Report"; META Group; USA; 2002; URL: http://www.metagroup.com/cgi-bin/inetcgi/commerce/productDetails.jsp?oid=33569 (10 Nov 2002) *NOTE: This is the free summary, not the complete report*

"Cyber crime bleeds US Corporations"; Computer Security Institute; 7 April 2002. URL: http://www.gocsi.com/press/20020407.html (26 Oct 2002)

"Designing a Remote Access VPN"; CMP Asia; 2000. URL: http://www.cmpnetasia.com/tech_guide/vpn/viewArt.cfm?aid=18&pid=1 (26 Oct 2002)

"Security and the Mobile Office"; GRIC Communications; 9 April 2002; URL: http://www.gric.com/pdfs/whitepaper_reps.pdf (10 Nov 2002)

"Security Risks in Telecommuting"; F-Secure; April 2000; URL: http://www.f-secure.com/products/white-papers/telecom_risks.pdf (26 Oct 2002)

---

[i] Allen, J et al; Common Sense Guide for Senior Managers; URL: http://www.isalliance.org
[ii] Product material on Telstra Dial IP (also known as Telstra Dial Connect) can be viewed at the Telstra Dial IP homepage at http://www.telstra.com.au/dialip/index.htm
[iii] Allen, J et al; op cit; p.iii
[iv] Cole, E, et al; SANS Security Essentials II: Network Security; 2001, p 1-7.
[v] "Cyber crime bleeds US Corporations"; URL: http://www.gocsi.com/press/20020407.html
[vi] Allen, J et al; op cit; p.16
[vii] GRIC, p.1 URL: http://www.gric.com/pdfs/whitepaper_reps.pdf
[viii] Redhead, T; "Managing the Remote Risks"; p76
[ix] 2003 Worldwide IT Benchmark Report. URL: http://www.metagroup.com
[x] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213324,00.html
[xi] http://www.cmpnetasia.com/tech_guide/vpn/viewArt.cfm?aid=18&pid=1
[xii] Giunta, P; "Virtual Private Networks: An Overview"; p.3
[xiii] Kaeo, M; Designing Network Security; p158
[xiv] Wright, J; "Bullish on VPNS"; URL: http://www.infosecuritymag.com/2002/jun/bullish.shtml
[xv] Salamone, S; "Keep An Eye Out For the Hidden Costs". URL: http://internetwk.com/VPN/supplement329-2.htm
[xvi] Giunta, P; op cit; p.11
[xvii] This information collected from various Dial IP documentation.
[xviii] Dial IP Technology Group; RADIUS Information Document; p 3.
[xix] Dial IP – Frequently Asked Questions. URL: http://www.telstra.com.au/dialip/faqs.htm
[xx] Dial IP Technology Group; op cit; p 9

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced