Global Information Assurance Certification Paper

Meeting the information security requirements between client and contractor on a mega-construction project

A case study

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b Option 2

Submitted by Jon Truan
Thursday, October 14, 2004

Abstract

Whenever a project under construction exceeds 1 billion dollars, it definitely qualifies as a “mega-construction” project. It is also requires a large support staff, engineering from various disciplines, and other vital personnel. A job of this size may be on a 3- 5 year path, so the office that will be set up to run and support it is like any other office in terms of IT needs. To support such a project, the construction management firm must be well diversified. It is very common in the construction industry for two leading firms to form a joint venture company to bid on a project off this size to be able to scale up to meet the needs that a mega-job demands.

How then, do you secure systems in a joint venture company’s network space, while maintaining connectivity to each company’s corporate networks? To add to the problem, all of the IT equipment is furnished by the client, including switches, routers, desktops and servers. How do you maintain administrative control of your section of the network, while meeting the information security requirements of the client? What happens when the client asks you to make a major change to your architecture, which will require a new solution in order for your employees to connect back to their home networks?

Before Snapshot

The original solution was to be found in granting the joint venture firm their own subnet on the client network, and implementing a DMZ network configuration.

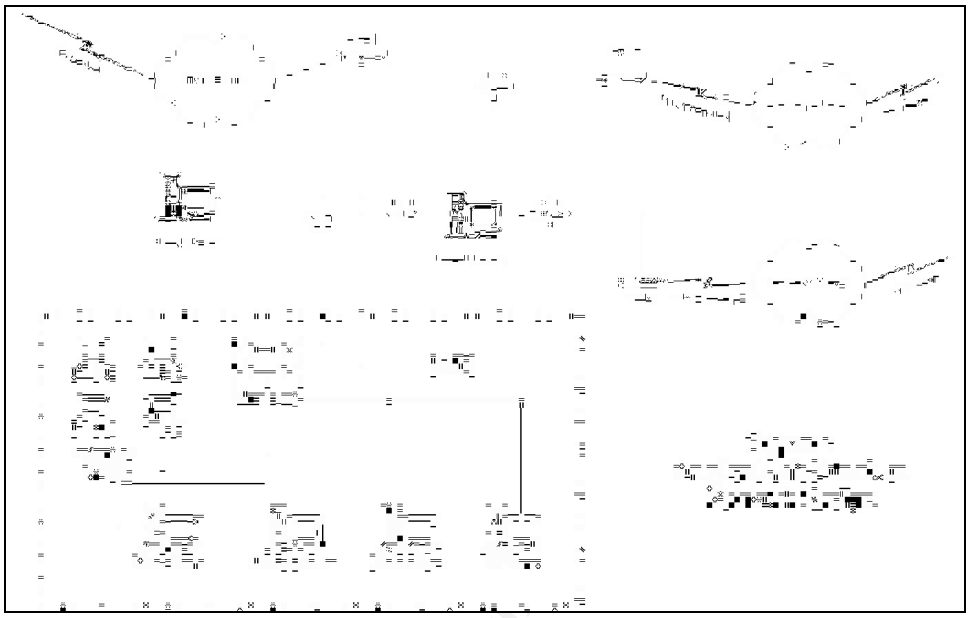
A DMZ is defined as:

“Short for demilitarized zone, a computer or small sub network that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. The term comes from military use, meaning a buffer area between two enemies[1].”

The DMZ would be formed using two firewall servers one serving as an endpoint to the T1 lines connecting back to each side of the newly formed joint venture’s home networks and one protecting the joint venture’s data from the client network.

[1] http://www.webopedia.com/TERM/D/DMZ.html

The initial network architecture can be seen in figure 1.



In order to support construction activities on the project, the joint venture needed to have access to their offices in different cities. In addition, these offices needed to be able to send files back to the joint venture on the construction site. CAD drawing revisions, request for information, and other items were critical in maintaining workflow of construction activities to keep the project on schedule and on budget. Add to this that client involvement is also required in each step of the process for approval and concurrence.

The original idea of a DMZ architecture met the needs of all parties, but was agreed upon reluctantly by the client because of the un-trusted nature of servers that they did not control, and T1 lines leading back to networks that they did not trust. In the end, the client did agree to allow this solution to be implemented. All was well until SQL Slammer…

Enter SQL Slammer worm and an article about subcontractor networks

The client reached the breaking point when the SQL Slammer worm was unleashed. Meetings about the DMZ were scheduled with the client in the wake of an article [2] about the SQL Slammer worm bringing down portions of a power plant. The worm entered through a subcontractor network. Although, neither the joint venture nor the client was affected by the worm due to good perimeter defenses, it opened a Pandora's Box about vulnerabilities from outside networks. This Pandora's Box would not be closed until a

[2] http://www.securityfocus.com/news/6767

major re-architecture took place on the joint venture network. The external T1 lines would have to go. How will the company connect back to their respective home offices? How will this affect day to day operations for the joint venture?

The DMZ had been a point of contention since the inception of the project. The client was somewhat unwilling from the onset to setup the architecture desired by the joint venture that would be overseeing the project. Eventually, the client agreed to the DMZ, but yearly internal security audits would bring this network architecture into focus each year, and each year the joint venture would try to stave off attacks from the clients' IT security staff to get rid of the DMZ. This led to strained relations with the joint venture and the client's IT staff. It seemed that a stalemate to this issue was at hand.

The SQL Slammer worm generated a new sense of urgency on the part of the client to make some changes to the DMZ that would be acceptable to the IT security staff. In addition, a new spirit of cooperation was being fostered, with the joint venture's previous network administrator leaving and a new one coming onboard in the form of this author. I had been briefed on the relations strain that had existed before my arrival. I saw my entry as a chance to turn the relationship back to what had been originally intended by my firm: one of cooperation and mutual respect. To say that we have to work hand in hand with our client is an understatement. On a project that exceeds multiple years of construction and over 1 billion dollars, the lines are sometimes blurred between client and contractor. Thus is the nature of collaborative work in this type of environment.

I felt that it would benefit me to get to know the management and IT staff of our client and see if I could put a "fresh face" on an old problem. In the months leading up to the SQL Slammer incident, this would serve me well when discussion about what to do with my network came up. It was clear to our client that their IT security team was no longer willing to tolerate our current network. It was equally clear to me that something was going to have to be done. The question was how painful would it be?

The initial meeting

The first meeting that took place in the process was a meeting with a consultant on our staff, me, and the client's IT management and security representative. Our consultant was our previous network administrator, who had been retained on a short term contract to ensure a smooth transition to me. This presented a potentially volatile situation since his past history with our client's IT management had strained the relationship with the joint venture with regard to IT matters. Ultimately, the decision was mine to recommend a solution to my management, but his input would be weighed by my boss. I needed to carefully balance the needs of my organization, while also meeting the needs of our client.

In our first meeting a wide range of options were discussed. One plan was to completely eliminate our entire subnet and roll my servers and clients into their network space. Our consultant felt it was important to have a separate address space for the joint venture network. There was also the concern of assigning the servers with new IP addresses and what effect this might have on a proprietary database product that was currently in use by the joint venture. Another plan was discussed that would allow the joint venture to keep the address space we were currently using but drop our DMZ. This would satisfy the needs of our client, but we would then lose connectivity to both sides of the joint venture joint venture's home networks. A solution somewhere in the middle was needed, and it was needed fast as we had just four weeks to design the new network and implement it.

The new solution to an old problem

A new plan was formed and I assigned a timeline of what events needed to be done, by whom, and when. Since my firm was paying for the services of the consultant I decided to leverage his existing knowledge of the current network architecture, in particular I placed him in charge of decommissioning the Netware server and firewalls since he had deep knowledge of these products. I was tasked with setting up remote connections back to both sides of the joint venture network, installing the VPN clients, and building out a new Windows 2000 server that would replace the roles that the Novell server currently performed.

I chose to use the model that both firms in the joint venture used for all of their other mobile workers, a Virtual Private Network connection back to the home network.

As listed on the www.vpnc.org website a VPN is:

"A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The main purpose of a VPN is to give the company the same capabilities as private leased lines at much lower cost by using the shared public infrastructure." [3]

I was able to convince my management that a VPN solution would meet our security needs in terms of encrypting[4] the data on the wire and insuring confidentiality of data transmission on our client's network. In fact, in many ways it was now more secure as the encrypted data was much less susceptible to sniffing from inside the client's enterprise network.

[3] http://www.vpnc.org/vpn-technologies.html

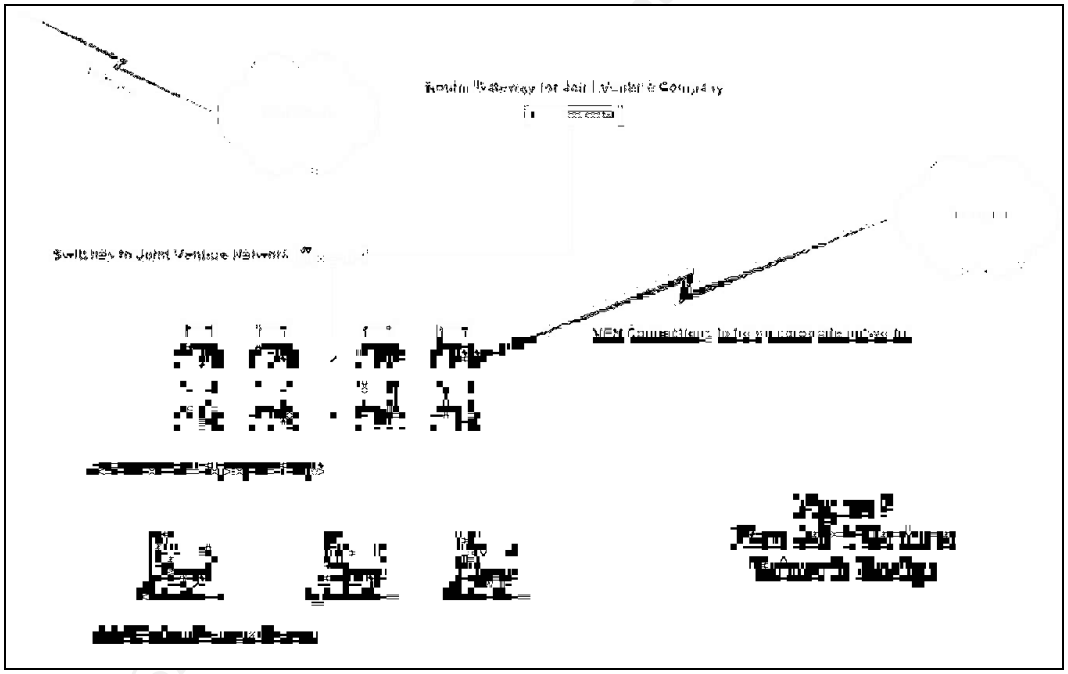
[4] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html

This solution would not be nearly as convenient as before for my users, but it was tolerable since 99% of the activity on the joint venture network happened on the client network in the form of email and internal apps and web pages. The joint venture staff has a few major apps that they use in day to day activity; a web based portal that serves as the main point of information within the company and a web based application for timekeeping. I felt that making a VPN connection to connect to these apps would not be major hindrance to daily workflow. Our joint venture servers would remain in place in their own domain just as they had always been. I presented the plan to my management and it was agreed upon. It was now time to act on the plan with the goal of transparency to my users and no downtime.

During Snapshot

The new joint venture network architecture can be seen in Figure 2

.



Not only did the new network design simplify my administrative load, it also opened up all of the joint venture workstations and servers to security scanning; a goal that had been long sought by our client. After the plan that I developed was reviewed, my consultant and I decided that the best way to make the changes that were needed would be to “rip off the band-aid”, that is to do all the major tasks in one weekend. We could not turn off the T1 lines without each workstation having the VPN client installed and an account created for each user to reach back to the joint venture corporate networks. We could also not drop the firewalls with the T1 still active. Since the joint venture network was Novell based, the Netware file and print server had to be re-

provisioned at this time too, and the firewalls relied on the Novell NDS tree. This meant that the Netware client would need to be removed from each desktop this same weekend as well. The Novell Netware 5 server had the duties of a personal file server, print server and NDS main tree server. We would need to recreate these roles as well. It was going to be a long weekend!

In the week leading up to the major rebuild of the network, I had all of the accounts created for each user to VPN back to their corporate networks. I also installed and configured each machine with the needed VPN client. In addition I scheduled and taught a training session on how to use the new system so that everyone would know how to connect back to their home networks and do their activities.

On the weekend of the re-configuration, the T1 lines were disconnected from their routers and the firewall servers were turned off. The server that was previously a Netware server was rebuilt to a Windows 2000 server and the needed print ques were created. A personal user storage share for each user in the joint venture was also created on this server. The joint venture also had an FTP server that was used to transmit large files. After reviewing this server's usage, I determined that we could totally de-commission the joint venture FTP server under the new network architecture. This proved not to be a problem at all, since large files could still be sent to our client's FTP server or via FedEx on CD.

I visited each machine and removed the NetWare client. I also took this opportunity to review each machines service pack and patch level and apply what was needed accordingly. Since the users were already logging into the client's Windows 2000 domain, no additional interaction would be required on my part when they returned to work on Monday, except to visit each user and set up the new network mappings to the newly created printer ques and personal network shares. This was accomplished in one day, and everyone tolerated it well. I was happy to have Novell off of my network since I had to create a Novell account on our Novell server that was identical to the primary Windows domain account assigned to each of my users by the client. I would not have to maintain these duplicate accounts anymore!

I tested everything out on Sunday and insured that everything worked. As expected, I could now log in to the Windows domain of my client, and the response was much faster since it was no longer passing though the Novell layer. There were a few features of the Novell environment that I was sad to see go, but it was worth it to make our client happy!

Securing the servers "without a fence"

Despite the fact that our servers and all of the software we used was owned by the client, there was still data that the client should not be able to see, at least until the project was complete, and possibly after. This data revealed the cost structure of my company, as well as company proprietary secrets about how we ran projects. How can

we ensure that only the proper individuals accessed this data under the new network model?

With the firewalls now a thing of the past, we had to look more closely at access controls to our joint venture company server's data and shares. Groups were already in place on the existing file server, and membership had been established, so it was determined that the existing access control lists[5] set up under windows would continue to be appropriate to keep our data private.

Despite the fact that the client's security team could now "look over the fence" we were confident in the ACL's that were defined on the company servers and shares. I convinced my management that the ACL's were a sufficient means of protecting the sensitive data that we did not want our client to see.

After all, we were on the client's network, using their domain accounts for our day to day work. I argued that if someone from our client breached the ACL's and "hacked" into our data, then that was a much larger issue itself, and would be dealt with at higher levels such as HR. Auditing attempts to gain access to our protected network share points was turned on as a reporting measure. All in all, my management seemed satisfied that our data was still protected from prying eyes.

After Snapshot

I faced several issues in the days and weeks after all of the work was competed. The biggest issue was and still is to have my users understand when they need to initiate a VPN connection and when to terminate it. Despite initial training sessions and one on one time with me, many of my users have been confused about why when they connect to the VPN; they cannot access their outlook mail, or internal web pages on our client's intranet. In addition to that, the VPN software used by my company is a customized version of the client, and changes the DNS settings of the machines to comply with their network. Of course, when my users disconnect from the VPN, the DNS settings do not get changed back, and sometimes even a re-boot will not clear the problem (for those users who are configured with static IP addresses). This usually requires a visit from me in person or remotely, and it is a huge headache.

There were a few surprises that surfaced after this project was completed, such as when my users complete their timesheet via an internal web application, printing did not work to network printers while they were connected to the company network via VPN. Many of these issues were minor annoyances, and presented an acceptable trade off in

[5] http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prdd_sec_tzxs.asp

terms of what was gained by decommissioning the DMZ and moving behind the client firewall.

Positives of the project

A major goal was accomplished by changing our network structure to the new system seen in figure 2. Chief among these was that the client no longer had points of ingress to their network that bypassed their firewall. This in itself represented a huge win in re-establishing good will between my firm and the security staff of our client.

A second important goal that was realized was that now that my systems and servers were no longer blocking internal scans by our client's security team, I now had the advantage of getting vulnerability data on my systems via internal reports compiled by my client. This made my job much easier. I could now respond to threats more quickly patching systems as needed. In addition, my users internal traffic could now be scrutinized more closely than before, alerting me to problems such as inappropriate use and other issues before they would be allowed to get too far out of hand.

Our client utilizes a myriad of both proprietary and off the shelf systems to secure the enterprise network and has a long track record in guarding their enterprise. By getting rid of the DMZ, I am now able to leverage these systems and their deep skills to provide a layered "defense in depth" [6]approach to protecting my section of the network in a much more robust manner than was previously possible.

Impact

The state of security for my firm's network segment has been greatly improved by the redesign to get rid of the DMZ configuration. At first, many in my firm were skeptical that we could do this and still "keep the client out" of the protected areas. But in a short time, my users saw that aside from connecting up with the VPN client every once in a while, nothing had really changed for them. Quietly, behind the scenes though, we were now being subject to scanning for known vulnerabilities on our network, malicious activity, website filtering, and other defensive measures that improved the overall state of security for my firm.

Additionally, now that the data originating from within our client's network going to their respective home offices is now encrypted, it is much more secure and protected from man-in-the-middle and sniffing based attacks. This was a side benefit that I don't think that anyone had really considered until we implemented the VPN connections back to each of the joint venture's home offices. On top of that, we were able to save our client $10,000 – $15,000 a year as a result of no longer needing to pay monthly fees on the

[6] Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz,

separate T1 lines. An additional cost savings was also realized in my time as my administrative load has eased quite a bit, saving me 2-3 hours per week in troubleshooting remote connection issues, firewall problems, and so on.

In conclusion, after implementing what at first seemed like a huge headache, I cannot help but wonder “Why didn’t someone do this sooner?” Not only is my network more secure than it ever was before, but it is also much easier to manage. We were able to satisfy the needs of our client and meet the needs of my users in the joint venture, while saving money, time, and improving our security posture. I think that by most any measurement that is a win-win for all parties involved. In the IT world, we must learn to embrace new ideas and changes, rather than fight them if we want to stay current and at the same time protect the intellectual capital of our enterprises. It is in our nature as IT professionals to be cautious, I think, but I have learned from this experience that change can be a good thing if done right. Above all, communication to our end-users (customers) and obtaining management buy-in for any major initiative is vital for it to be successful. Of course, when you have no other option but to change what you are currently doing, that helps too.

List of references

www.webopedia.com "Definition of a DMZ" March 26, 2004URL: http://www.webopedia.com/TERM/D/DMZ.html

Poulsen, Kevin "Slammer worm crashed Ohio nuke plant network" August 19, 2003 URL: http://www.securityfocus.com/news/6767

VPN Consortium "VPN Technologies: Definitions and Requirements" January 2004 URL: http://www.vpnc.org/vpn-technologies.html

Robert Bauchle, Fred Hazen, John Lund, Gabe Oakley, and Frank Rundatz "Encryption defined" October 27, 2003 URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html

Microsoft Windows XP Professional Resource Kit Documentation Online 2004 "Working with Access Control Lists" URL: http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prdd_sec_tzxs.asp

Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS Security Essentials and the CISSP 10 Domains "Defense in Depth" Version 2.2 SANS Press, January 2004 11-15